



Hvordan norske banker responderer på ny teknologi og nye aktører

En kvalitativ utforskende analyse om hvordan norske banker tilpasser seg endringene som oppstår når nye aktører og blokkjedeteknologi truer deres markedsposisjon.

Eilev Haukaas & Nicolai Herman Grann Greve

Veileder: Tommy Stamland

Master i Finansiell økonomi og Økonomisk styring

NORGES HANDELSHØYSKOLE

Dette selvstendige arbeidet er gjennomført som ledd i masterstudiet i økonomi- og administrasjon ved Norges Handelshøyskole og godkjent som sådan. Godkjenningen innebærer ikke at Høyskolen eller sensorer innestår for de metoder som er anvendt, resultater som er fremkommet eller konklusjoner som er trukket i arbeidet.

Sammendrag

Vi har gjennom en kvalitativ analyse med induktiv tilnærming, gjennomført dybdeintervjuer med nøkkelpersoner i norske banker og finansforetak, for å få en dypere forståelse av bransjen og de utfordringene den møter. Basert på analyse av primærdata og en gjennomgang av tilgjengelig litteratur, ble det dannet et grunnlag for å diskutere hvordan norske banker tilpasser seg endringene som oppstår når nye aktører og blokkjedeteknologi truer deres markedsposisjon.

På kort sikt finner utredningen ingen tegn på at blokkjeder vil true markedsposisjonen til bankene, da teknologien fortsatt krever tredjeparter som kontrollerer informasjonen som legges på kjeden. Teknologien kan imidlertid bidra til å effektivisere bankene som tredjepartsaktører, såfremt en finner løsninger på de regulatoriske, organisatoriske og teknologiske hindringene. Blokkjedeteknologi er vanskelig å skalere, og det er utfordrende å integrere teknologien i bankenes eksisterende systemer og prosesser. Teknologien har på den annen side potensialet til å skape nye produkter og tjenester i bransjen ved å effektivisere generell forretningsvirksomhet og administrasjon, som for eksempel dokumenthåndtering.

Bankenes markedsposisjon trues derimot av selskaper som Google, Amazon, Facebook og Apple (GAFA), samt FinTech-aktører, som alle er på vei inn i bransjen. De store teknologiske selskapene har sterke merkevarer i Norge, og tilbyr allerede brukervennlige betalingsløsninger til sine kunder. Det er uenighet blant de norske bankene om hvor stor trussel aktørene representerer på kort sikt, men de tar alle høyde for at utradisjonelle bankaktører er en reell utfordrer på lang sikt. Det er utviklet ulike strategier for å imøtekomme konkurransen i markedet, hvor tilnærmingen i stor grad varierer blant de etablerte aktørene. Blant annet velger både Nordea og Sbanken å muliggjøre bruk av Apple Pay for sine kunder, i motsetning til DNB og de øvrige norske bankene som velger å sperre tjenesten for å fremme sine egne tilbud.

De norske bankene er, uavhengig av respons, tvunget til å utvikle brukervennlige og konkurransedyktige produkter og tjenester for å ivareta tillitsforholdet til sine kunder. Et tillitsforhold som kan avgjøre hvilken aktør fremtidens bankkunder velger når de skal ta opp et lån eller sette penger på konto.

Forord

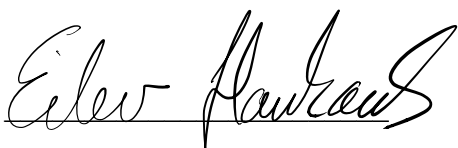
Masterutredningen er en del av vår mastergrad i økonomi og administrasjon ved Norges Handelshøyskole (NHH). Utredningen tar for seg strukturelle og finansielle aspekter i norske banker, og inneholder elementer fra begge profilene Finansiell økonomi og Økonomisk styring.

Vi vil rette en stor takk til ekspertene vi har intervjuet for dyp forståelse og gode refleksjoner om utviklingen innen bank og finans. Alle intervjuobjektene er sitert ved navn, og presentert i Appendiks C.

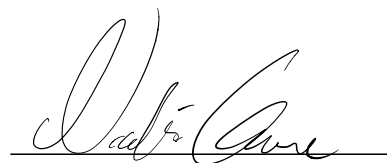
Vi vil også takke Finance Innovation for innspill og hjelp til å komme i kontakt med relevante aktører og personer i næringslivet.

Til slutt, en stor takk til vår veileder, Tommy Stamland, for hans innsikt og konstruktive tilbakemeldinger i løpet av prosessen.

Bergen, Desember 2018



Eilev Haukaas



Nicolai Herman Grann Greve

Innholdsfortegnelse

SAMMENDRAG	2
FORORD	3
INNHOLDSFORTEGNELSE	4
1. INNLEDNING	7
1.1 PROBLEMSTILLING	7
1.2 AVGRENSNINGER	8
2. METODE	9
2.1 FORSKNINGSDSIGN	9
2.1.1 <i>Valg av tilnærming</i>	9
2.1.2 <i>Valg av metode</i>	10
2.2 DATAINNSAMLING	10
2.2.1 <i>Primær- og sekundærdata</i>	10
2.2.2 <i>Intervjutype</i>	11
2.2.3 <i>Intervjuguide</i>	12
2.2.4 <i>Valg av intervjuobjekter</i>	12
2.2.5 <i>Anonymitet og personvern</i>	13
2.3 ANALYSE AV PRIMÆRDATA.....	13
2.4 EVALUERING AV RESULTATER.....	14
2.4.1 <i>Validitet</i>	14
2.4.2 <i>Reliabilitet</i>	15
2.4.3 <i>Svakheter i analysen</i>	15
3. BAKGRUNN	17
3.1 TEKNOLOGISK BAKGRUNN	17
3.1.1 <i>Blokkjeder</i>	19

3.1.2	<i>Permissioned-og Permissonless-nettverk</i>	23
3.1.3	<i>Smartkontrakter</i>	26
3.2	VERDIEN AV TILLIT - EN OBJEKTIV TREDJEPART.....	27
4.	TRUSSELEN FRA BLOKKJEDER OG NYE AKTØRER	29
4.1	AUTENTISERING – EN BÆREBJELKE I BANK OG FINANS.....	30
4.1.1	<i>Systemets infrastruktur</i>	30
4.1.2	<i>Utfordringer</i>	33
4.1.3	<i>Komplekse og kostbare prosesser</i>	36
4.1.4	<i>Revisjonens rolle</i>	39
4.2	TRANSAKSJONER OG FLYTTING AV VERDIER	42
4.2.1	<i>Infrastrukturen i bransjen</i>	42
4.2.2	<i>Produkter som trues</i>	46
4.2.3	<i>Lightning Network</i>	54
4.3	HVORDAN NYE MARKEDER HAR ÅPNET SEG	57
4.3.1	<i>FinTech og GAFa</i>	57
4.3.2	<i>I bresjen for utvikling</i>	64
5.	OPPSUMMERING OG KONKLUSJON	75
	BIBLIOGRAFI	77
	APENDIKS A - INTERVJUFORESPØRSEL	89
	APENDIKS B - INTERVJUGUIDE	90
	APENDIKS C - INTERVJULISTE	92

Figurer

Figur 1 En blokk i blokkjede.....	Feil! Bokmerke er ikke definert.
Figur 2 Blokkjede.....	21
Figur 3 Blokkjedetrilemmaet	24
Figur 4 Blokkjede-Matrise	26
Figur 5 Oversikt over store dataangrep på sentrale databaser.....	34
Figur 6 Bitcoin-transaksjon.....	48
Figur 7 Transaksjonstid for Bitcoin	55
Figur 8 Hvilke aktører nordmenn har tillit til som leverandør av aggregeringstjenester	62

Tabeller

Tabell 1 Samfunnsøkonomiske kostnader av transaksjoner	44
--	----

1. Innledning

1.1 Problemstilling

Blokkjedeteknologi har de siste årene fått stor oppmerksomhet for evnen til å utfordre bankenes rolle som en tillitsskapende tredjepartsaktør (McKinsey, 2016). Teknologien sikrer integriteten til hovedboken gjennom matematiske regler og ugjennomtrengelig kryptografi, og gjør det mulig å redusere kostnadene til mange av de tjenestene bankene leverer (Gupta, 2018). Bankene har historisk investert store summer for å effektivisere eksisterende systemene, og har de siste årene fått øynene opp for at blokkjeder kan være en viktig brikke i deres fremtidige forretningsmodell (Edwards, 2018). Paradoksalt nok kan teknologien som ble laget for å fjerne tredjepartsleddet gjøre at bankene blir vesentlig bedre.

Alle banker, også små sparebanker, er opptatt av blokkjedeteknologi. Alle ser at det kommer til å endre mye av det vi gjør fremover.

Lasse Meholm – DNB

I et marked med stadig økende konkurranse, kan det å implementere blokkjeder være utfordrende. Teknologien krever betydelig investering på et tidspunkt hvor bankene bruker majoriteten av sine investeringer på å holde vedlike gamle IT-systemer (Røise, 2016). Investeringer i de gamle systemene har spesielt ett problem: Kapitalsterke aktører kan vie betydelige ressurser i å utvikle helt nye systemer, som kan sette bankenes eksisterende systemer på sidelinjen (Fox, 2016). Selskaper som Facebook, Amazon, Google og Apple (GAFA) har, med sin kjernekompetanse på teknologi, allerede etablert seg i bank- og finanssektoren. De teknologibaserte selskapene har to dimensjoner å spille på; verdien av å selge banktjenester og verdien av data som tjenestene genererer. Ved å tilby tjenester som for eksempel revisjon og transaksjoner, billig, til både privatpersoner og bedrifter, kan de bygge opp et tillits- og kundeforhold som historisk har vært forbeholdt finansinstitusjonene. Formålet er å kombinere transaksjonsdata og banktjenester med data aktørene allerede besitter. Slik kan de blant annet predikere når og hvorvidt kunder trenger lån, samt gjøre bedre risikovurderinger.

Markedsposisjonen til bankene blir utfordret fra flere hold. Ny teknologi truer deres relevans og nye aktører utfordrer deres markedsposisjon. Ved litteratursøk og empirisk forskning gjort

gjennom intervjuer av eksperter og andre interessenter innen bank og finans, har vi kartlagt de ulike truslene næringen møter, og søker av den grunn å belyse;

Hvordan norske banker tilpasser seg endringene som oppstår når nye aktører og blokkjedeteknologi truer deres markedsposisjon.

1.2 Avgrensninger

Oppgavens omfang er begrenset av både tid og emne, og vi har av den grunn valgt å utelukke andre effektiviserende teknologier som blant annet kunstig intelligens og robotisering. Basert på primærdata begrenser vi begrepet «nye aktører» til å omhandle store teknologiske selskaper som Google, Amazon, Facebook og Apple (GAFA), samt FinTech-selskaper. Nye aktører som Bank Norwegian og Komplet Bank vil også kunne true bankenes markedsposisjon, men vil ikke analyseres i denne utredningen.

2. Metode

Kapittelet beskriver valg av metodisk tilnærming til problemstillingen. Det presenteres først valg av forskningsdesign, deretter prosessen som helhet med innsamling og strukturering av data. Videre vil metodens validitet og reliabilitet vurderes opp mot alternativ metode, og hvorvidt valg av metode begrenser analysen.

2.1 Forskningsdesign

Valg av metode avhenger av tilnærmingen til innsamling av data. Metoden gjenspeiler informasjonsbehovet som trengs for å kunne svare på oppgavens problemstilling. I den anledning er det to tilnærminger til analyse.

Den første og mest brukte metoden i dypere studier er kvantitativ metode, hvor statistikk i stor grad danner grunnlag for analyse (Befring, 2015). Med andre ord veies statistiske konklusjoner opp mot hverandre for å finne sammenhenger.

Den andre metoden til datainnsamling er kvalitativ metode. Metoden baserer seg i stor grad på intuisjon og rasjonalitet, og ønsker å svare på det overordnede spørsmålet med en tilnærming om hva, hvorfor og hvordan (Befring, 2015). Kvalitativ forskning er spesielt effektiv for å skaffe spesifikk informasjon om verdier, meninger, atferd og sosiale sammenhenger av bestemte populasjoner.

2.1.1 Valg av tilnærming

For å besvare oppgavens overordnede spørsmål kan det gjennomføres en induktiv eller en deduktiv tilnærming (Saunders M. N., 2015). Induktiv tilnærming søker å danne ny teori basert på empirisk analyse. Logikk brukes i stor grad for å trekke paralleller mellom utsagn, påstander og data, slik at det kan lages generelle prinsipper og teorier. Induktiv tilnærming vil for eksempel konkludere med at alle svaner er hvite, fordi de observerte svanene i et eksperiment er hvite. I motsetning er et deduktivt design en metode hvor en empirisk avkrefter

eller bekrefter teori. Deduktiv tilnærming vil for eksempel teste påstanden om at alle svaner er hvite, og enten avkrefte eller bekrefte dette.

Oppgavens formål er å svare på hvordan bankene tilpasser seg den stadig økende konkurransen, fra både ny teknologi og nye aktører. Et induktivt design er derfor valgt, da en mer eksplorerende tilnærming til forskningsspørsmålet fremstår mer konstruktivt og resultatskapende. Press fra blokkjedeteknologi og nye teknologiske aktører er et relativt nytt fenomen for banker, og det eksisterer få konkrete eksempler på hva dette vil bety for næringen.

2.1.2 Valg av metode

Utredningen beskriver hvordan banker er tradisjonelle institusjoner, som i liten grad har vært utsatt for et internasjonalt og teknologisk press. Det er med andre ord få tall som kan belyse problemstillingen i et historisk perspektiv, og vi valgte av den grunn å gjennomføre en kvalitativ analyse. Oppgaven ønsker å belyse og strukturere den eksisterende informasjonen som finnes, samt bidra med nye empiriske data i form av intervjuer med sentrale aktører innen blokkjeder, teknologiutvikling og finanssektoren som sådan.

2.2 Datainnsamling

2.2.1 Primær- og sekundærdata

Datagrunnlag for en analyse kan deles inn i primær- og sekundærdata. Primærdata vil si data som samles inn med formål om å analysere og belyse konkrete problemstillinger, og kan være svar på spørreundersøkelser, intervjuer og eksperimenter (Creswell J. W., 2014). Sekundærdata er i motsetning til primærdata, informasjon som allerede eksisterer. Det vil si at resultater av oppgavens intervjuer er primærdata for denne oppgaven, men det kan for en annen analyse fremstå som sekundærdata. Sekundærdata kan også være bøker, rapporter og markedsundersøkelser, og regnes som et viktig supplement for å bygge opp under funnene i primærdata.

Oppgaven bruker i stor grad primærdata til å danne grunnlag for analysen. Data er samlet inn gjennom dybdeintervjuer med sentrale personer i bank og finanssektoren, samt eksperter på blokkjedeteknologi og autentisering.

I kombinasjon med primærdata, er sekundærdata brukt for å supplere. Spesielt knyttet til blokkjedeteknologi, et felt hvor diskusjonen i stor grad preges av synsing og udokumenterte påstander. Kombinasjonen av sekundær- og primærdata var derfor helt essensielt for å sikre kvalitet i analysen.

2.2.2 Intervjutype

Strukturert intervju

Strukturert intervju baserer seg på at hvert enkelt intervjuobjekt blir stilt helt like spørsmål i det samme formatet (Befring, 2015). Metoden gir data som samles inn relativt lik kodeks, og gjør at det i større grad dannes et grunnlag for kvantitativ analyse.

Semistrukturert intervju

Semistrukturert intervju baserer seg på en intervjuguide med en overordnet problemstilling som ønskes diskutert (Befring, 2015). Det er ingen krav til streng struktur, men intervjuguiden brukes som en retningsgivende plan for å dreie intervjuet i en hensiktsmessig retning. Semistrukturerte intervjuer gir mer naturlig flyt i intervjuet, og kan ende med helt ulike diskusjoner fra intervjuobjekt til intervjuobjekt. På den annen side kan slik tilnærming gjøre innsamlet data vanskelig å sammenligne.

Ustrukturert intervju

Et ustrukturert intervju sikter i større grad mot en dialog, sammenliknet med de to andre alternativene. Tanken er å kunne gå dypt inn i tematikker, uten å være bundet av et rammeverk (Befring, 2015). Intervjuene baserer seg ikke på en intervjuguide, men samtalen styrer retningen på diskusjonen. Intervjuformen gjør at intervjuobjektet lettere deler det som fremstår relevant og interessant å diskutere. Ulempen med et slikt format er at en i liten grad får sammenlignbar data, og en kan ende opp med å diskutere tematikker som ikke er relevante for å svare på oppgavens problemstilling.

Valg av intervjumetode

Oppgavens forskningsspørsmål er lite belyst i tilgjengelig sekundærdata. Det taler i stor grad for en mer eksplorativ tilnærming til intervjuene, og semistrukturerte intervjuer ble av den grunn valgt som oppgavens hovedform.

Ved bruk av mer strukturerte intervjumetoder er det fare for at intervjuerne legger føringer som begrenser diskusjonene og datagrunnlaget. De semistrukturerte intervjuene ble derfor supplert med et fåtall ustrukturerte intervjuer om tematikker hvor vi ønsket nye vinklinger på spesifikke problemstillinger, som for eksempel blokkjedeteknologi.

2.2.3 Intervjuguide

I henhold til bruk av semistrukturert intervju ble det utviklet en intervjuguide for å sikre en viss grad for likhet mellom intervjuene, og at datagrunnlaget dannes i tråd med behovene for å besvare oppgavens problemstilling. En godt forankret intervjuguide var derfor essensielt for sluttresultatet.

Intervjuguiden ble utformet basert på våre ønsker til diskusjon. Det ble først utformet et utkast for to pilotintervjuer med hensikt å se hvorvidt vårt forskningsspørsmål lot seg besvare. Resultatene av de to pilotintervjuene førte til at intervjuguiden, og oppgavens overordnede spørsmål ble revidert. Den reviderte intervjuguiden ble brukt på de resterende semistrukturerte intervjuene.

Revidert intervjuguide ligger vedlagt i Appendiks B.

2.2.4 Valg av intervjuobjekter

Det finnes flere tilnærminger til valg av intervjuobjekter, avhengig av hva slags resultat en er på jakt etter (Jacobsen, 2005). Vi valgte i oppgaven å tilnærme oss intervjuobjektene på flere måter. Den overordnede metoden var en strategisk utvelgelse, hvor vi valgte de personene vi fant mest relevante for å belyse oppgavens tematikk. Mangfold i analysen ble sikret ved å kombinere metoden med variasjonsutvelgelse, med den hensikt å fange opp ulike erfaringer,

praksiser og meninger. I løpet av intervjuprosessen fikk vi tips om relevante personer å snakke med, anbefalinger vi valgte å benytte oss av i de tilfellene det var relevant for oppgaven.

Alle intervjuobjektene fikk en skriftlig henvendelse, med en formell invitasjon til intervju. I brevet ble oppgavens formål beskrevet, samt en oppsummering av de tematikkene vi ønsket å gjennomgå i intervjuet. De praktiske opplysningene om intervjuets lengde, form og på hvilken plattform det ville foregå, ble også formidlet i den skriftlige henvendelsen.

Intervjuforspørsel er vedlagt i Appendiks A.

2.2.5 Anonymitet og personvern

For å sikre at intervjuprosessen har fulgt lover og regler om personvern, ble intervjuene gjennomført i henhold til retningslinjer fra «Norsk senter for forskningsdata». Prosjektet er også meldt inn som et forskningsprosjekt, med de krav det medfølger. Etter innlevert avhandling vil all lagret informasjon om intervjuobjektene slettes.

Det ble gitt samtykke av samtlige intervjuobjekter om bruk av lydopptak under intervju, en forespørsel alle personene fikk i den formelle invitasjonen. Synspunkter og meninger ytret av intervjuobjektene reflekteres nødvendigvis ikke av deres respektive selskaper. Før innleveringen av oppgaven har alle sitater blitt godkjent av de respektive intervjuobjektene med mulighet for korrigerende eller tilbaketrekking av utsagnet.

2.3 Analyse av primærdata

Tematisk analyse er i oppgaven brukt som tilnærming til den kvalitative metoden, og egner seg godt til å se mønstre mellom ulike intervjuer (Saunders, Lewis, & Thornhill, 2016). Ulike temaer og ord i primærdata ble kodet med en referansekode, for å sikre systematikk og finne mønstre i datasettet. Dette ga et godt grunnlag for å sette argumenter mellom intervjuobjektene opp mot hverandre.

For å sikre korrekthet ble alle intervjuer tatt opp med båndopptaker, for så å bli transkribert ved første anledning etter endt intervju. Transkribering var essensielt for effektivt

sammenligne, referere tilbake til, og ikke minst bruke primærdata som oppslagsverk i tiden etter intervjuene (Saunders et al., 2016).

Etter endt intervjuopprosess ble samtlige transkriberingsdokumenter kodet slik at relevante tematikker og spesifikke ord ble samlet i mindre databaser. Ordet autentisering ble for eksempel kodet med en kode og lagret i en felles database for autentisering, sammen med andre ord som for eksempel verifisering. Metoden sørget for et mangfoldig bilde av de ulike tematikkene uten å risikere at vi overså intervjuobjekter.

Databasen var et viktig verktøy når vi kombinerte vår primærdata med sekundærdata. Slik kunne vi kontrollere påstander fra alle intervjuobjektene og se etter likheter.

2.4 Evaluering av resultater

2.4.1 Validitet

Validitet skal reflektere i hvilken grad resultatene i et studie er gyldig, og det skilles mellom intern, ekstern og begrepsvaliditet (Saunders et al., 2016).

Begrepsvaliditet forklarer i hvor stor grad empiriske data måler hva en ønsker å måle, og er spesielt relevant i kvantitative studier (Creswell J. W., 2014). I motsetning er det i kvalitative studier ikke like lett å operasjonalisere begreper, og av den grunn ikke like relevant å evaluere begrepsvaliditeten.

Intern validitet forklarer i hvilken grad oppfattelsen av primærdata samsvarer mellom forskeren og det fenomenet eller utvalget som er undersøkt (Saunders et al., 2016). Det vil si at vår oppfattelse av en mening er lik intervjuobjektets mening. Overenstemmelse ble sikret ved at vi brukte god tid i innledningen av intervjuet til å sette intervjuobjektet godt inn i problemstillingen vi ønsket å diskutere, i tillegg til den formelle invitasjonen som ble sendt ut på forhånd. Svar på spørsmål ble underveis i intervjuet kontrollert med oppfølgingsspørsmål, for å sikre at begge parter var samstemte.

Ekstern validitet sier noe om resultatene i analysen kan generaliseres og brukes på tvers av bransjer, eller til å forklare andre situasjoner (Saunders et al., 2016). Vårt utvalg av intervjuobjekter er relativt sett lite og med strategisk utvelgelse av intervjuobjektene, kan

generalisering være utfordrende. På den annen side vil mange av utfordringene knyttet til blokkjedeteknologi og teknologiens muligheter være likt på tvers av bransjer og situasjoner. Det vil si at vår analyse muligens vil kunne benyttes av andre finansinstitusjoner som står ovenfor samme krav til blant annet autentisering og press fra teknologiske selskaper. Likevel skal en være forsiktig med å trekke generaliserende slutninger basert på analysen, da de fleste av intervjuobjektene jobber eller har jobbet i store nasjonale banker, og kan være farget av dette.

2.4.2 Reliabilitet

Reliabiliteten til oppgaven sier noe om påliteligheten til analysen og konklusjonen (Saunders et al., 2016). Det kan være utfordrende i kvalitative studier, spesielt med en induktiv tilnærming, hvor en leter etter svarene på samme måte som en leter etter de gode spørsmålene. Mangel på standardisert struktur i datainnsamlingen, og situasjonsbetingede svar fra respondentene, kan gjøre det vanskelig å gjenta studiet i et annet tidsrom.

Det ble av flere intervjuobjekter trukket frem at svarene gitt i intervjuet ikke nødvendigvis vil være like om ett år, på grunn av en enorm fart i bransjen, og ikke minst innen blokkjedeteknologi. Ved bruk av semistrukturert intervjuform vil sannsynligvis diskusjonen variere fra tid til annen, avhengig av relevans og interessen til intervjuobjektet på det aktuelle tidspunktet, som igjen påvirker reliabiliteten til analysen.

For å ivareta reliabiliteten så godt som mulig sørger vi derfor for transparens i metode og utvalg av intervjuobjekter. Intervjuguide og liste over intervjuobjektene er vedlagt i henholdsvis Appendiks B og C. At primærdata er supplert av sekundærdata sørger også for en viss konsistens mellom faktagrunnlaget i oppgaven og andre rapporter eller utredninger.

2.4.3 Svakheter i analysen

Den største utfordringen med analysen er at utvalget for innsamlingen av primærdata er begrenset. Det er få ressurser med ekspertise på blokkjeder i Norge generelt, noe som begrenset utvalgsmulighetene. Likevel sitter vi igjen med et inntrykk av at datagrunnlaget danner et godt bilde av dagens situasjonen. Vi har snakket med de to største bankene i Norge,

DNB og Nordea, som begge har sine egne ekspertteam på blokkjedeteknologi. Deres utsagn om generelle utfordringer hos norske banker er kryssjekket med to andre banker av betydelig størrelse, Sparebanken Vest og Sbanken. Videre er alle uttalelser om blokkjeder kryssjekket med både eksperter og sekundærdata. Denne metoden har gjort det mulig å danne et bilde av hva som er udokumenterte påstander, og hva som er reelle utfordringer og beskrivelser. Samme personer ble anbefalt av flere av intervjuobjektene på tvers av fagfelt, noe som impliserer at utvalget reflekterer godt kunnskapsbehovet som trengs for en presis analyse.

I analysen om de store teknologiske aktørenes trussel på bank og finans skulle vi gjerne hatt intervjuer med flere av disse selskapene. Det er forsøkt å oppnå kontakt med GAFA-selskapene¹ med hensikt å innhente informasjon om deres tilnærming til det norske bankmarkedet. Mangel på primærdata fra begge sider kan potensielt danne et skjevt bilde av den reelle trusselen, men vi ser det likevel ikke som en kritisk svakhet da oppgaven ønsker å se på hvordan de norske bankene responderer på trusselen, uavhengig av hva de nye aktørene faktisk velger å gjøre.

¹ Google, Amazon, Facebook, Apple

3. Bakgrunn

Kapittelet 3, skal ta for seg noen av de strukturelle og teknologiske trekkene som gjør blokkjeder unike fra dagens system, og se på noen forskjeller mellom de ulike blokkjedeteknologiene. Videre skal vi vurdere hvilken rolle tillit spiller i dagens system, og hvordan bankene har opparbeidet seg den.

3.1 Teknologisk bakgrunn

Lagring av kontrakter og transaksjoner er med på å definerende strukturene i våre økonomiske, lovgivende og politiske systemer (Lakhani & Iansiti, 2017). Systemet beskytter både individers og organisasjoners verdier, og samspillet mellom dem. Uavhengig av den sentrale rollen systemene spiller i vårt samfunn, og de byråkratiske retningslinjer som er satt opp for å styre dem, har de ikke klart å holde tritt med den digitale transformasjonen samfunnet har gjennomgått.

På 1990-tallet ble verden introdusert for internett (Castelles, 2013). Det var trolig få som kunne forestille seg hvilken revolusjon som var startet, og hvor mye det ville komme til å påvirke våre liv. Teknologien endret en rekke industrier, og hverdagen til utallige mennesker. Verden ble kontinuerlig mer digitalisert og globalisert, hvor en rekke selskaper hadde eksponentiell vekst på en bølge av ny teknologisk innovasjon.

Banker over hele verden var, som mange andre selskaper, en del av denne enestående og diskuterbare usunne veksten. I 2008 var verden i den største resesjon i verdensøkonomien siden den store depresjonen på 1930-tallet (Singh, 2018). En rekke selskaper gikk konkurs, hvor det mest omtalte eksemplet er Lehman Brothers, en av verdens største banker på det tidspunktet (Havemann, 2018).

Krisen i 2008 illustrerer en av ulempene ved å stole på sentraliserte aktører, med deres maktkonsentrasjon og manglende transparens. En ukjent enkeltperson, eller gruppe, under pseudonymet Satoshi Nakamoto ønsket å finne et bedre alternativ til det eksisterende systemet, og introduserte i 2008 verden for Bitcoin gjennom whitepaperet² «*Bitcoin: A Peer-to-Peer*

² Whitepaper er et informasjonsdokument utstedt av et firma for å fremme, eller fremheve funksjonene til en løsning, et produkt eller en tjeneste (Businessdictionary, 2018)

Electronic Cash System», kun to måneder etter at Lehman Brothers gikk konkurs (Nakamoto, 2008).

Hensikten med Bitcoin var blant annet å hoppe over tredjepartsleddet, og heller drive med handel og transaksjoner mellom enkeltpersoner (Nakamoto, 2008). Satoshi ønsket å fjerne innsynet og kontrollen som banker og myndigheter hadde over transaksjoner med et betalingsmiddel like anonymt som kontanter. Systemet skulle sørge for at alle aktørene var fullstendig ærlige og til å stole på når det gjaldt penger.

“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution”

Satoshi Nakamoto, 2008³

Satoshi fant en revolusjonerende måte å praktisk gjennomføre slike transaksjoner, ved hjelp av blokkjeder, teknologien som ligger bak Bitcoin og andre kryptovalutaer. En åpen, digitalt distribuert transaksjonshovedbok⁴, som kan lagre alle transaksjoner mellom to parter på en effektiv og permanent måte (Lakhani & Iansiti, 2017). Transaksjoner som foregår på nettverket vil være sporbare, men hvor sendere og mottakere er anonyme. Ved bruk av blokkjedeteknologi kan det eksistere en verden hvor alle transaksjoner og kontrakter er lagret i transparente, og distribuerte databaser, beskyttet mot redigering og sletting. Enhver avtale, prosess og betaling vil ha et digitalt fotspor og signatur som kan bli identifisert, validert, lagret og delt.

Konseptet som ble utviklet av Satoshi er imidlertid ikke nytt. Ideen ble først presentert i journalen om kryptografi av Stuart Haber og W. Scott Stornetta kalt «*How to time stamp a Digital Document*» (Harber & Stornetta, 1991). Haber og Stornetta møtte imidlertid et fundamentalt problem. Dokumenter tilgjengelig for flere kan være upålitelige, fordi de til enhver tid kan endres, hvor et resultat av dette er kjent som «double spending» eller «The Byzantine Generals Problem» (Nakamoto, 2008). Det beskriver i hovedsak et problem om

³ Nakamoto, 2008, Bitcoin: A Peer-to-Peer Electronic Cash System s 1

⁴ Kjent på engelsk som «ledger»

konsensusdannelse i et system der kommunikasjonskanaler ikke kan stole på hverandre, og det behøves en tredjepart for å validere at informasjonen er korrekt.

I dag skjer de fleste transaksjoner gjennom tredjepartsaktører som banker, meglere og clearinghus (Tapscott & Tapscott, 2018). Tredjepartene sørger for at kjøpere og selgere kan møtes, og spiller en fundamental rolle for å flytte informasjon, penger og andre ressurser i markedet. I modellen har interaksjonen mellom mellomledd, og behovet for kontinuerlig verifisering, skapt et fragmentert system med en rekke forsinkelser, risikoer og kostnader for både kjøpere og selgere. Det er her blokkjeder gjør seg aktuell, en sikker, kryptert og distribuert teknologi, som teoretisk fjerner mange av de problemene bransjen møter. Teknologien skal kunne muliggjøre kommunikasjon mellom computere ved å lagre og sende informasjon trygt og effektivt uten behov for tredjeparter, som en slags revolusjonerende tillitsmaskin.

Blokkjeder har blitt referert til som det største teknologiske gjennombruddet siden internett på 1990-tallet (Rawson, 2017). Det sås lite tvil om at potensialet er stort, men interessen de siste årene har bidratt til en enorm «hype»⁵ rundt blokkjeder. Det er mange barrierer teknologien må igjennom før den fullt ut kan implementeres i næringslivet. Blant annet teknologiske, regulatoriske og organisatoriske hindringer som er kompliserte og krevende å løse.

Blokkjeder er en fundamental plattform som kan skape helt nye økonomiske og sosiale systemer, men det er en økonomisk- og tidskrevende prosess (Gupta, 2018). Flere av intervjuobjektene trakk frem at storhetstiden til blokkjeder er mange år frem i tid, og at det av den grunn er viktig å ha et rasjonelt syn på teknologiens muligheter og begrensninger. På bakgrunn av dette vil vi i det neste delkapittelet gå igjennom hva blokkjeder kan, og ikke kan bli bruk til, og de begrensninger som ligger i teknologien.

3.1.1 Blokkjeder

Blokkjeder kan defineres som en distribuert hovedbok basert på kryptografiske protokoller (Sinrod, 2018). Teknologien er motstandsdyktig mot manipulering, noe som kan gi høy tillit

⁵ Hype er en betegnelse på en opphausende og eventuelt manipulerende omtale eller markedsføring; reklame som skaper store forventninger til et produkt eller et fenomen ved hjelp av overdrivelser (SNL, 2018)

til informasjonen som finnes på den. Nettverket er drevet av en nettverkskonsensus, og tillater at data blir lagret og overført i et person til person-nettverk. Det muliggjør flytting og lagring av informasjon, verdier og data mellom to personer, uten behovet for en tredjepart.

Blokkjeden er kun den datastrukturen hvor en lagrer ny informasjon uten å slette den gamle (Tapscott & Tapscott, 2018). Nye blokker blir registrert, og lagt i kronologisk rekkefølge med en kryptografisk link tilbake til den forrige blokken, som gjør at en ikke kan endre gammel data uten at kjeden brytes. Strukturen kan beskrives som en loggføring av transaksjoner, og er på ingen måte en revolusjon. Loggføring har eksistert i århundrer, og praktiseres i stor grad i de fleste virksomheter i dag. Med andre ord er det ikke den grunnleggende strukturen som ble funnet opp av Satoshi Nakamoto, men bruk av kryptovaluta som et verdiobjekt til å insentivere arbeidere i et nettverk.

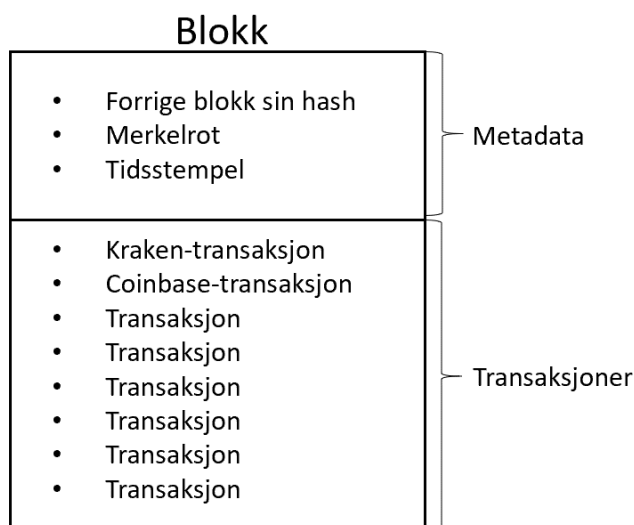
En blokk i systemet er en datastruktur med formål om å samle opp transaksjoner og distribuere det til alle nodene⁶ på nettverket, og kan deles i to deler (Nakamoto, 2008). Den ene delen er metadata, som validerer gyldigheten av en blokk ved hjelp av blant annet et merkleltre⁷ og hash-koding⁸. Den andre delen kan i prinsippet representere alt, slik som veksling av penger eller instruksjoner om kjøp og salg av aksjer (Goldman Sachs, 2018). Gitt et tilfelle med transaksjoner, vil blokken inneholde den informasjonen minere⁹ har valgt å inkludere i den aktuelle blokken. Brukere gjennomfører transaksjoner som sendes til nettverket hvor de venter på at minere skal inkludere transaksjonen i en ny blokk.

⁶ En node er en enhet på nettverket

⁷ Merkleltre, er en kryptografisk hash av alle transaksjonene som inngår i denne blokken.

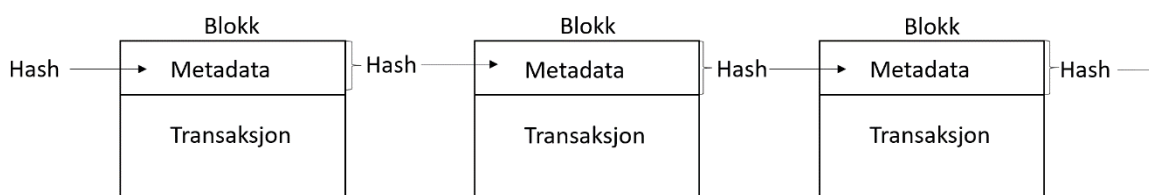
⁸ Se side 22 for nærmere forklaring av hash

⁹ En eller flere noder på nettverket som leverer datakraft for å validere transaksjoner og lagrer de i hovedboken (Pokrandt, 2018).



Figur 1 En blokk i blokkjede

Minerene tar ventende transaksjoner, verifiser at de er kryptografisk nøyaktige, og pakker informasjonen inn i blokker, som lagres på blokkjeden (Gupta, 2018). Deretter får blokken en unik kode, en hash, som legges i enden av blokkjeden på minerens node. Den distribueres så til nettverket og oppdateres av alle andre noder. Oppdatering av loggen gjøres ved å løse et vanskelig verifiseringsproblem. I et Proof of Work-nettverk er en slik mekanisme bevisst utformet som ressursintensiv, slik at antall blokker produsert hver dag forblir stabilt. Individuelle blokker må inneholde et bevis på at utført arbeid skal vurderes som gyldig. Beviset på at arbeid er utført verifiseres av andre noder på nettverket hver gang de mottar en ny blokk.



Figur 2 Blokkjede

Alle i nettverket kan enkelt kontrollere om verifiseringsprosessen er riktig eller ikke. Det kan tenkes på som en Sudoku – den er vanskelig å løse, men det er lett å verifisere at den er løst (Tapscott & Tapscott, 2018). Eksempelvis tar det for en Bitcoin-transaksjon gjennomsnittlig 10 minutter å løse koden for å lage en ny blokk, og det er matematisk umulig å ta noen snarveier. Når nettverket ser den korrekte løsningen, har deltakerne på forhånd blitt enig om at den som først klarer å løse koden, kan lage den nye blokken.

Når en for eksempel sender Bitcoin, må en avgift betales for å insentivere minerene til å inkludere transaksjonen i en blokk (Browne, 2017). Det er en budkrig om å få transaksjonen til blokken, hvor den som byr mest blir behandlet først. En bivirkning av høy aktivitet er av den grunn høyere transaksjonsavgifter.

En åpen¹⁰ blokkjede er sikret gjennom mekanismen om utslettelige og ikke-redigerbare poster (Tapscott & Tapscott, 2018). Informasjonen valideres gjennom en avstemming i nettverket, fremfor en sentralisert myndighet. I et Proof of Work nettverk er en miners stemmевe begrenset av deres beregningsressurser, slik at systemet forblir demokratisk. Hvordan en slik mekanisme fungerer avhenger av hvilken blokkjede en bruker, hvor den vanligste valideringsprosessen er en flertallsavgjørelse. Prinsippet kan illustreres på følgende måte: Hvis Per og Pål mener de begge er fedre til Kari, og Kari mener hun er barnet til Per, så er det den kombinasjonen med flest stemmer som vinner og blir plassert i blokkjeden, altså kombinasjonen med Per og Kari. Selve verifiseringsprosessen kan bygges på mange måter, hvor blant annet Proof of Stake¹¹ og Proof of Assignment¹² er andre alternativer.

Det andre sikkerhetsmomentet er at hver blokk er kryptert, noe som skaper en unik hash-kode (Nakamoto, 2008). Krypteringen gjør at informasjonen om blokken er meningsløs frem til den er dekryptert og satt i riktig rekkefølge, gjennom en mekanisme med offentlige og private nøkler. De offentlige nøklene er tilgjengelig for alle i nettverket i motsetning til de private nøklene som er konfidensielle, og kun tilgjengelig for sine respektive eiere. Nøkkelparet er

¹⁰ En åpen blokkjede er i oppgaven en Offentlig-Permissionless blokkjede

¹¹ En valideringsprosess der en person kan validere blokktransaksjoner i henhold til hvor stor innsats de har i nettverket, for eksempel hvor stor andel Bitcoin de har. (Blockgeeks, 2018)

¹² Enkelte noder bestemmer over nettverket (Iotw, 2018)

matematisk generert, som betyr at alt som krypteres med en offentlig nøkkel, kun kan dekrypteres med den tilhørende private nøkkelen, og omvendt.

Skulle noe av den krypterte informasjonen bli forandret, endrer den aktuelle hashen til blokken seg (Nakamoto, 2008). Ettersom hash-koden av den siste blokken er inkludert i forrige blokk, endres også den forrige blokken. Slik fortsetter det til alle de underordnede blokkene er endret. En skal trekke frem at det er teknisk mulig å ta kontroll over et slikt nettverket, som alle andre nettverk, det er bare svært utfordrende. Noder i et åpent Proof of Work-basert blokkjedenettverk distribueres, der hver node har en kopi av hovedboken. Endring i blokkjeden kan ikke skje før 51% av datakraften i nettverket godkjenner endringen. Det matematiske puslespillet, og datakraften som kreves for å ta kontroll over nettverket er stor, og praktisk umulig for enkeltpersoner å tilegne seg.

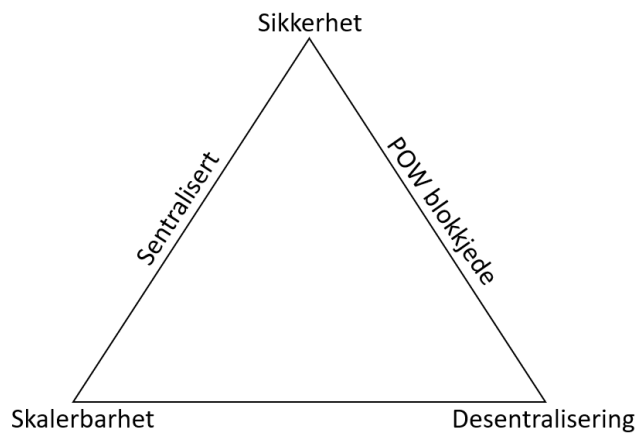
3.1.2 Permissioned-og Permisjonless-nettverk

Systemer som brukes av banker i dag er bygget opp av databaser, som skiller seg fra blokkjeder, ved at det er en organisert samling av informasjon som lett kan nås, administreres og oppdateres (BBC, 2018a). Databaser er organisert i rader, kolonner og tabeller, og det er indeksert for å gjøre det lettere å finne relevant informasjon. Databaser eies og drives av en overordnet part som fastsetter vilkårene for de som ønsker tilgang. Data kan bli oppdatert, utvidet og slettet avhengig av ønskene til eieren av databasen eller nettverket. Tradisjonelt har sentraliserte enheter styrt og eid databasene (Thake, 2018). En av de største ulempene til et slikt system er risikoen for dataangrep, noe en har sett en rekke tilfeller av de siste årene (Holm-Nilsen & Mjaaland, 2018).

Blokkjeder er en bestemt type Distributed Ledger Technology, ofte skrevet av desentraliserte og vanligvis anonyme agenter, fremfor kjente sentraliserte parter. Distributed Ledger Technology er et paraplybegrep som brukes for å beskrive teknologier som distribuerer poster eller informasjon blant alle de som bruker teknologien, enten privat eller offentlig (Worldbank, 2018). En slik hovedbok bør ideelt være:

- sikker,
- skalerbar
- desentralisert for å unngå kraftkonsentrasjon.

Distributed Ledger Technology har som all annen ny teknologi noen grunnleggende utfordringer, som gjør at prioritering av enkelte egenskaper går på bekostning av andre. Dette er illustrert som blokkjedens trilemma i figur 3 (Margaritoff, 2018). Ønskes et desentralisert nettverk med høy sikkerhet, vil det gå på bekostning av skalerbarheten. På samme måte vil økt fokus på skalerbarhet og sikkerhet føre til mer sentralisert struktur. Det er umulig for en aktør å oppnå alle de tre egenskapene ved hjelp av dagens blokkjedeteknologi. Blokkjeditrilemmaet fremmer de viktige økonomiske valgene en må ta ved utformingen av transaksjonshovedbøker.



Figur 3 Blokkjeditrilemmaet (Margaritoff, 2018)

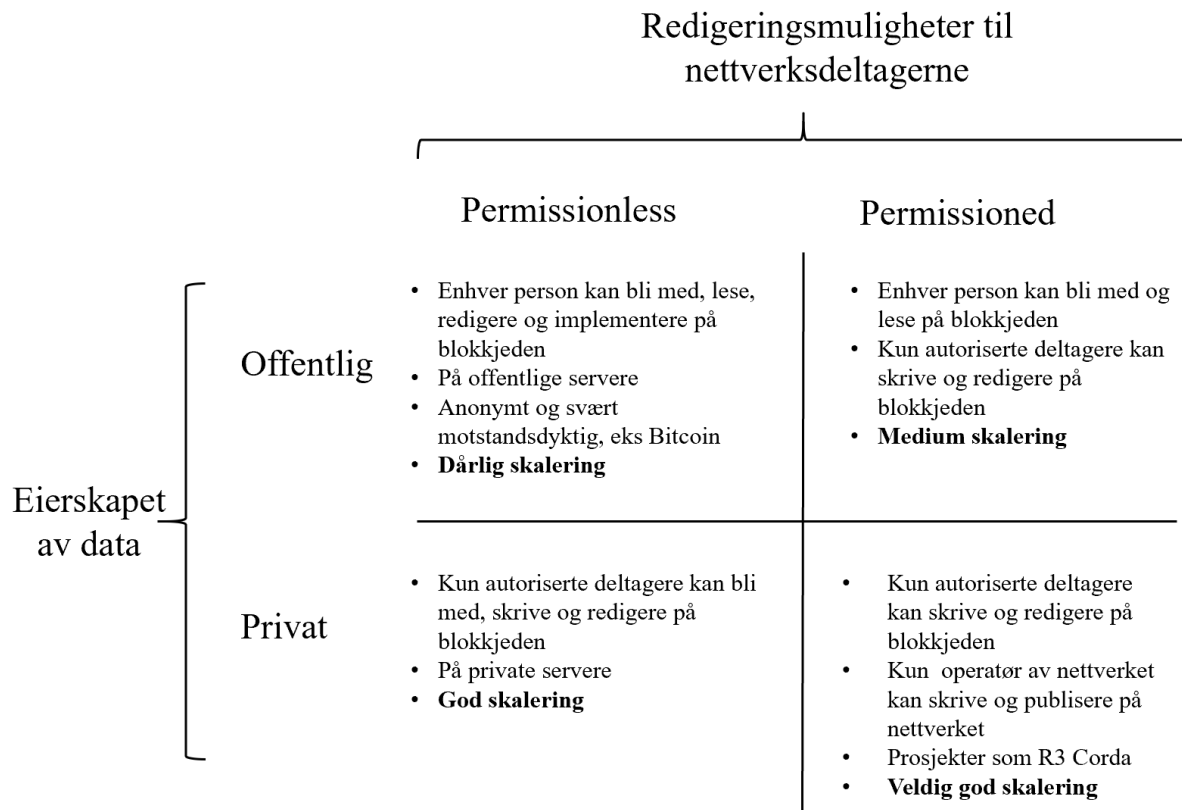
For å forstå blokkjede-trilemmaet, er det nødvendig å forstå hvorfor desentraliserte og anonyme blokkjeder er ressursintensive. Gitt at alle kan redigere en offentlig blokkjede, er en konsensusalgoritme nødvendig for å bekrefte den sanne historien blant mulige inkompatible eller falske rapporter (Goldman Sachs, 2018). Slik systemet fungerer i dag vil sentraliserte mellommenn insentiveres til ikke å begå svindel, fordi de risikerer å miste lisensen dersom de jukser. En sentralisert mellommann har et insitament til å jukse hvis fordelene ved en engangsforvringning av hovedboken kompenserer for kostnadene ved å miste sin fremtidige fortjeneste.

Bruken av Proof of Work-verifiseringer løser det overnevnte problemet ved at minere veier fordelene av et engangsangrep opp mot kostnadene ved å legge til nye blokker på en blokkjede (Faridi, 2017). Det vil si strømmen av avgifter betalt til ærlige blokkjedeforfattere.

Eksempelvis vil en kryptominer sammenligne kostnaden for å gjennomføre et «double-spending»-angrep med det beløpet som kan brukes dobbelt.

Ved bruk av et lukket oppsett, for eksempel gjennom et bankkonsortium, trengs ikke denne formen for Proof of Work (Hyperledger, 2018b). Avstemming kan i stedet brukes, hvor for eksempel flertallet i nettverket er enige om den riktige versjonen, eller et system der en sentral aktør bestemmer. En slik metode vil ikke fungere i et åpent system, fordi det vil ved bruk av en konsensusalgoritme være mulig å lage flere nye brukerkontoer med stemmerett. Det vil for eksempel for en aktør være mulig å opprette 100 nye brukerkontoer, og dermed stemme som 100 «forskjellige» personer.

Utfordringene i verifiseringsprosessene har ført til to hovedformer for blokkjeder som brukes i markedet, Permissioned og Permissionless, der eierskapet av data enten er privat eller offentlig fordelt (McKinsey, 2018). Permissioned-blokkjeder hindrer ulovlige modifikasjoner ved at kun bestemte aktører er autorisert til å gjøre endringer i nettverket. Permissioned-blokkjeder observeres oftest i blokkjedeprojektene til banker og andre store aktører, som utnytter nettverkets kraft til egen intern virksomhet (Cecchetti & Schoenholtz, 2018). Et slikt oppsett gjør det mulig å teste pilotprosjekter i liten skala, og undersøke potensialet før det rulles ut i produksjon. I en åpen blokkjede er ideen å gjøre identitet irrelevant, der hvem som helst kan bli med og forlate nettverket, hvor det mest kjente eksemplet er Bitcoin. Vi har under laget en matrise basert på en rapport av McKinsey for å illustrere noen av de egenskapene og problemene hvert av alternativene har.



Figur 4 Blokkjede-Matrise (McKinsey, 2018)

3.1.3 Smartkontrakter

Smartkontrakter vil i utredningen være programmer som sikrer, håndhever og gjennomfører overføringer av digitale eiendeler i henhold til forhåndsdefinerte kontraktsvilkår (Szabo, 1996). Den mest utbredte plattformen for bruk av smartkontrakter går via Ethereum-blokkjeden (Ethereum, 2018b). I whitepaperet til Ethereum forklares det hvordan blokkjeden kan brukes til transaksjoner og datalagring av mange slag. Det angis en omfattende liste over potensielle bruksområder som for eksempel lånesystemer, stemmegivningssystemer, finansielle derivater og forsikring (Buterin, 2015).

3.2 Verdien av tillit - en objektiv tredjepart

Behovet for banker kan spores helt tilbake til mer enn 2000 år før vår tidsregning, hvor handelsmenn på vegne av bønder handlet og solgte varer i byene mot en liten andel av inntekten (Hoggson, 2007). Bankene har siden den tid operert som en tredjepartsaktør slik at folk kunne beskytte sine eiendeler og handle med sine verdier. Grunnen til at en historisk sett har valgt, og at man i dag også velger å benytte seg av en tredjepart, beror på flere faktorer som blant annet kompetanse, alternativkostnader, reguleringer og tillit (Ticoll & Tapscott, 2012).

Tillit er en av de viktigste forutsetningene for et funksjonelt samfunn (Leite, 2015). Man legger rutinemessig sine liv i hendene på totalt fremmede, fordi man stoler på at de skal gjøre det rette. Eksempelvis kapteiner som flyr mennesker over havet, taxisjåfører som kjører folk fra sted til sted, og samspill mellom bilister på veien. I disse og andre tilfeller i livet, fungerer tillitssamspillet godt. Det er imidlertid noen tilfeller hvor en er avhengige av objektive tredjeparter for å opprettholde tilliten til systemet.

Tillit i en forretningsammenheng bygges ved at en aktør er ærlig, hensynsfull, transparent, ansvarlig og opptrer med integritet (Ticoll & Tapscott, 2012). Ettersom mennesker ikke alltid er til å stole på når det kommer til verdier, som for eksempel penger, er det i noen settinger behov for objektive og tillitsskapende tredjeparter, en rolle som bankene i dag besitter. Banker sikrer blant annet folks penger, gir en oversikt over deres verdier, muliggjør og sikrer overføringer (Olsen Ø. , Norges Bank, 2014). I dag sitter banker på komplekse og avanserte systemer med millioner av databaser som inneholder all slags informasjon (Tapscott & Tapscott, 2018). Bankene har klart å opprettholde sin markedsposisjon på grunn av sin gode evne til å holde på hemmeligheter og verne om sine kunders data.

Banker har i lang tid hatt informasjon om stort sett alt vi bruker penger på, men de har ikke brukt denne informasjonen til målrettet produktutvikling og markedsføring utover det som faller naturlig innenfor bank, eller delt data videre til tredjeparter. De har vernet om privatpersoners forbruksvaner, noe som har gjort at de over lang tid har opparbeidet respekt og tillitt ovenfor sine kunder.

Med røtter flere tusen år tilbake i tid har det utviklet seg noen strukturelle trekk hos bankene. De har blitt mer komplekse, utvidet produktporteføljen, og de har med tiden blitt tildelt en rolle som myndighetenes kontrollorgan, for å hindre blant annet økonomisk kriminalitet (Røise, 2016). Mer komplekse prosesser og lange tradisjoner byr også på noen strukturelle utfordringer. Dagens system er krevende å videreutvikle, hvor risikoen og kostnaden ved å bytte ut systemet i flere tiår har blitt regnet som for stor (Hidas, 2016). Bankene slik vi kjenner de i dag driftes på et teknologisk kjernesystem som ble utviklet på 70-tallet.

På tross av sin kompleksitet, har det finansielle systemet tjent kundene bra. Det eksisterer et globalt økonomisk marked, hvor det daglig rutinemessig behandles flere milliarder transaksjoner (Norges Bank, 2018b). Likevel er vårt nåværende system på ingen måte perfekt. Det er avhengig av et stort antall private og offentlige aktører, hver med sine proprietære IT-systemer. Dagens metoder for autentisering og transaksjoner er kostbare med både forsoning og motpartsrisiko. Finanskrisen i 2008 er et av mange eksempler på en lang historie om risiko tilknyttet finanssektoren og tilliten viet til den (Britannica, 2018).

Tillitt i næringslivet er viktig på flere plan. Næringslivet handler om et samspill mellom mange parter, ofte med divergerende interesser. Dersom en investor skal investere i et selskap, er en avhengig av å kunne stole på regnskapstallene til selskapet det skal investeres i. Regnskapstallene kan være utarbeidet av et eksternt regnskapsbyrå med tillitt fra ledelsen og eierne i selskapet. Interessene til regnskapsbyrået og investoren er ulike, men de er begge avhengig av å ha tro til systemet, og de ulike partene (Lazanis, 2015). Noen av utfordringene i et tillitsbasert system, med mange avhengige og uavhengige parter, er sannsynligheten for at feil oppstår. Feil som enten er gjort bevisst for å fremme egne interesser, eller ubevisst. Det er i næringslivet etablert mange lover og regler for å sikre seg mot slike feil (Regjeringen, 2014). Et eksempel er revisjonsselskap som reviderer regnskapet til uavhengige bedrifter, og på den måten sikrer at informasjonen som både går til eiere av selskapet, myndighetene og andre interessenter er korrekt og i henhold til de gjeldene lover og regler. Reguleringene skaper en infrastruktur som det kan bygges virksomheter på, blant annet banker.

4. Trusselen fra blokkjeder og nye aktører

Bruk av blokkjedeteknologi i finansielle tjenester, som beskrevet i kapittel 3, kan potensielt endre den eksisterende infrastrukturen i bank og finans. Det er to egenskaper ved blokkjeder som våre intervjuobjekter trakk frem som spesielt interessante. Det første er at teknologien med sin desentraliserte og kryptografiske struktur er tilnærmet immun mot angrep. I en verden hvor nettverkssikkerhet har blitt et sentralt tema for personers, bedrifters og nasjonal sikkerhet, er blokkjeder trukket frem som en potensielt revolusjonerende teknologi (McKinsey, 2016).

Den andre funksjonen som ble trukket frem er hvordan systemets desentraliserte struktur kan skape et samfunn uten behov for sentraliserte aktører (McKinsey, 2016). Tilliten vil avhenge av matematikken som ligger bak algoritmen, fremfor mennesker og institusjoner. Teknologien kan fjerne behovet for mellomledd, og dermed gjøre prosesser mer effektive. Kravene for å tilfredsstille kundene øker stadig, og det vil være essensielt å tilby de mest brukervennlige produktene og tjenestene, for å unngå å miste kunder.

Kundens adferdstrender har vist at når det kommer til praktiske løsninger og vaner, er de villige til å se på ikke-tradisjonelle finansielle aktører som leverandør av finansielle tjenester (Burns & Toit, 2017). Når kundene åpner opp for banktjenester levert av ikke-finansielle institusjoner, trues markedsposisjonen til bankene i flere dimensjoner. Vi har snakket med flere aktører og eksperter i det aktuelle markedet for å analysere hvilke aspekter som truer markedsposisjonen til bankene, og hvordan de tilpasser seg deretter.

Det er tre gjentakende punkter som intervjuene våre belyste som potensielle trusler mot den markedsposisjonen bankene har i dag:

1. Autentisering
2. Internasjonale transaksjoner
3. Nye og utradisjonelle aktører på vei inn i bank og finans

Dette kapittelet skal ta for seg konkrete utfordringer knyttet til de tre punktene. Først vil vi se på utfordringene knyttet til autentisering og flytting av verdier, for så å vurdere hvordan blokkjedeteknologi potensielt kan løse utfordringene tjenestene møter. Videre skal vi se på hvordan nye aktører søker seg inn i bransjen ved å tilby brukervennlige og billigere løsninger, for så å se på hvordan bankene respondere på denne trusselen.

4.1 Autentisering – en bærebjelke i bank og finans

Bank- og finansnæringen er en strengt regulert bransje, både av hensyn til personvern, og for å hindre kriminalitet. En viktig del i forebygging av blant annet hvitvasking er å ha tilstrekkelig informasjon om kundene (Kunz & Schirmer, 2015). Banker og andre finansinstitusjoner har et stort ansvar når det gjelder innhenting og etterprøving av informasjon, og kan av myndighetene få sanksjoner dersom de tilsynelatende burde oppdaget at noe var galt (Ekroll, 2018).

Vårt økonomiske system kunne blitt truet dersom en kunne gått til banken og lånt penger i en annen persons navn, eller om en hadde hatt flere lån med pant i samme hus eller hytte. Bank- og finansinstitusjoner har med andre ord både egeninteresse og stort ansvar når det gjelder autentisering av identitet og verdi.

Blokkjedeteknologi utfordrer bankenes posisjon som en tillitsskapende tredjepartsaktør (Tapscott & Tapscott, 2018). Dersom hver enkelt person og bedrift kan verifisere sin egen identitet elektronisk, distribuert i et desentralisert nettverk, kan det bidra til et mer effektivt og sikkert system. Denne delen av oppgaven skal ta for seg i hvor stor grad blokkjedeteknologi kan endre behovet for en autentiserende tredjepart.

4.1.1 Systemets infrastruktur

Autentisering kan sees på som en prosess hvor det bekreftes at Ola Nordmann er Ola Nordmann, at huset han eier både eksisterer og er hans, og at han ivaretar avtaler i henhold til hans lovnader. Det eksisterer flere aktører som jobber med autentisering, blant annet finansinstitusjonene selv, og uavhengige tredjeparter, slik som kredittvurderingsbyråer og BankID (Evry, 2018b). Autentisering kan primært skilles i to former, autentisering av verdi og autentisering av identitet.

Autentisering av identitet

Autentisering av identitet handler om å identifisere og kontrollere de involverte partene i handler og transaksjoner (Tapscott & Tapscott, 2018). En aktør som autentiserer

enkelpersoners identitet er BankID, en flerfaktor-autentiseringsløsning¹³, hvor alle personer over 15 år kan opprette et elektronisk sertifikat av sin ID via banken (BankID, 2018a). Sertifikatet kan genereres av en hvilken som helst norsk bank, og krever at banken har verifisert et identitetsbevis av kunden, for eksempel et pass. Den tilhørende personen får så tilgang til et elektronisk sertifikat, som styres av BankID (BankID, 2018b).

BankID er en integrert autentiseringsløsning i alle norske banker og offentlige register, og kan brukes som signeringsverktøy for å verifisere identitet i de fleste elektroniske prosessene i Norge (BankID, 2018c). Blant annet når det skal gjennomføres betalinger i nettbank og godkjenne endringer i Altinn. Systemet er særegent i verden, og trekkes frem i flere av intervjuene som en av de største teknologiske suksessene i Norge.

I Norge har vi jo BankID som fungerer veldig bra, og som mange andre land er veldig misunnelig på. Dette fungerer fordi vi har tillitt til den sentrale parten som utvikler dette.

Svein Ove Langeland – Sparebanken Vest

BankID-sertifikatet er linket opp til en rekke register, og gir autentiseringsaktørene automatisk tilgang til informasjon (BankID, 2018d). Informasjon de er lovpålagt å innhente og rapportere, og som er bundet opp i en rekke kostnader og tungroddede prosesser. Blant annet prosedyren som kalles Know Your Customer (KYC), som må gjennomføres av alle aktører som selger finansielle tjenester i Norge, og resten av EØS (Finans Norge, 2018b). Prosessen innebærer at banker og finansinstitusjoner må tilegne seg informasjon om kundeidentitet, bostedsadresse, overvåking av transaksjoner, hvilke tjenester og produkter de benytter og omfanget av kundeforholdet. Basert på informasjonen kan institusjonene danne en risikoprofil for å hindre kriminalitet, og i større grad sikre seg mot ugunstige salg av finansielle tjenester.

Know Your Customer er en av flere prosesser bankene må gjennomføre før de kan opprette et kundeforhold (Nordea, 2018). En kunde som eksempelvis ønsker et boliglån må oppfylle en rekke krav, knyttet til blant annet betalingsevne og sikkerhet. Når bankene utsteder boliglån med pant i boligen, må de blant annet forsikre seg om at boligen ikke er pantsatt i andre lån,

¹³ Flerfaktor-autentisering er autentisering hvor man i tillegg til noe man vet (for eksempel et passord og en innloggings-ID) må kombinere dette med noe man har (for eksempel en kodebrikke eller en mobil)

gjennom et realregister (Statens innkrevingssentral, 2012). Personer blir også sjekket for betalingsanmerkninger av betydning gjennom en kredittsjekk utført av en uavhengig tredjepart (Datatilsynet, 2018).

Autentisering er med andre ord ikke utelukkende en konsekvens av reguleringer, men også til for å sikre lavere risiko forbundet med banktjenester. Høyere risiko kan gi en direkte konsekvens i høyere priser for forbrukerne. Et eksempel kan være kredittkorttjenester som har en langt høyere rente enn et boliglån, fordi boliglånet utstedes med sikkerhet i pant, i motsetning til et kredittkort som primært knyttes til finansiering av forbruk (Olsen Ø. , 2018). Forbruk kan ikke kapitaliseres tilbake til penger, som gjør at risikoen banken har knyttet til tilbakebetaling av forbrukslån er høyere, som igjen gjør renten høyere.

Autentisering av verdi

I autentisering av verdi fastsettes verdien på et objekt som inngår i en transaksjon. Dette kan være verdien av en bolig som skal pantsettes eller en klokke som skal forsikres. Verdien av en bolig kan settes av en takstmann, og verdien av en klokke kan bekreftes gjennom en verdivurdering gjort av en urmaker.

Man kan si at i sluttproduktet som forsikring leverer trenger man fysisk tilstedeværelse. En form for assistanse som leveres som en ytelse. Det er i veldig liten grad økonomisk hjelp, men veihjelp, hjelp til å bygge opp huset, reparere bilen eller sykehusopphold. Da krever det en betydelig infrastruktur som aldri vil digitaliseres.

Rune Smådal – If

Fysisk tilstedeværelse er viktig i mange tilfeller når motytelsen skal ytes, slik som Rune Smådal beskriver, men i like stor grad vil fysisk tilstedeværelse være avgjørende når verdien av et objekt skal settes. Eksempelvis når det søkes om boliglån i en bank utenfor Norges grenser. En bank som primært opererer i USA vil vanskelig kunne vurdere hvorvidt takstmann Peder Aas er godkjent som en takstmann, og følgelig hvorvidt verdivurderingen av boligen stemmer overens med markedsverdien. Med andre ord er graden av direkte informasjon noe som verdsettes av bankene, fordi informasjonen lettere kan valideres, og kan tenkes å være en av årsakene til at små lokalbanker fremdeles eksisterer (Waupsh, 2016).

4.1.2 utfordringer

Det er viet stor tillitt til bankene som institusjoner. De sitter på enorme mengder informasjon som vernes om, og forblir mellom bankens fire vegger (Ticoll & Tapscott, 2012). BankID er et eksempel på dette, som i 2018 står registrert med 3,9 millioner elektroniske sertifikater med tilhørende dokumentasjon, lagret i en sentral database (BankID, 2018a).

Inntoget av teknologi i autentiseringsprosesser har skapt utfordringer av nye dimensjoner. Risikoen for ID-tyveri er større en noen gang, og det å validere personer over internett kan være krevende (Datatilsynet, 2017). Kriminelle utnytter dette til stadighet, hvor et nærliggende eksempel er personer som hevder de er nigerianske prinser som tilbyr gull og grønne skoger for å få tilgang til sensitiv informasjon (Eriksen, 2018). Kriminelle henvender seg til millioner av mennesker via falske annonser og e-poster, med håp om at personer skal respondere. Med andre ord er persondata og bankinformasjon et attraktivt mål for kriminelle. Så attraktivt at det brukes millioner av kroner på å forsvare og sikre de sentraliserte databasene, mot dataangrep (Digranes, 2017).

Et attraktivt bytte for hackere og kriminelle

Sentraliserte databaser er i langt større grad utsatt for dataangrep enn de desentraliserte (Cisco, 2018). Jo større databasen er, desto mer attraktivt er det for hackere å angripe, fordi data har en verdi (Thirani & Gupta, 2017).

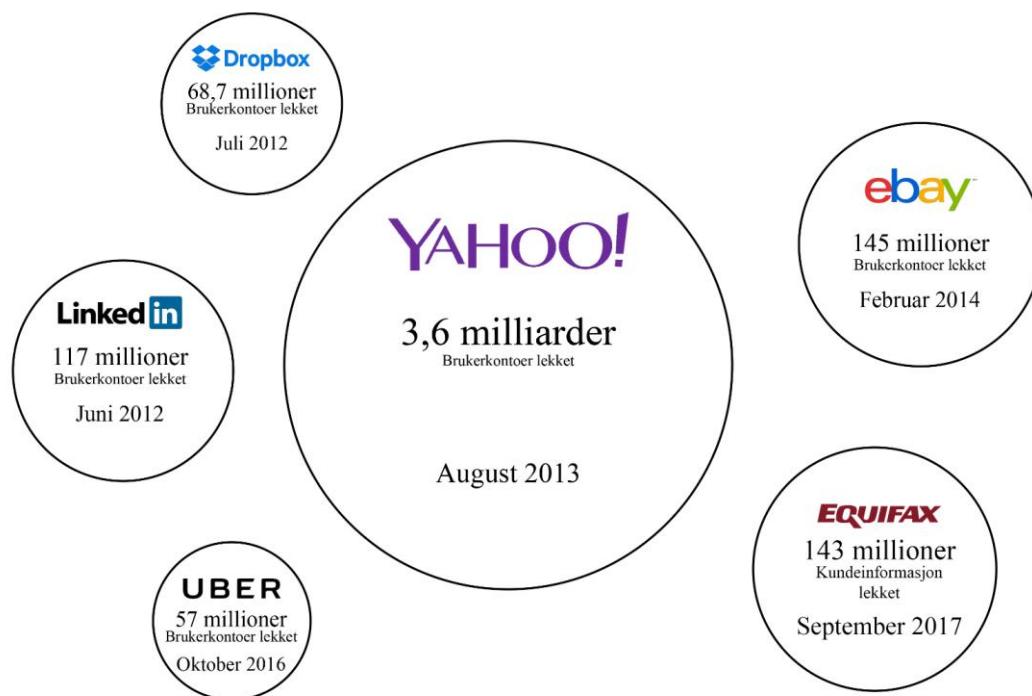
Centralized options are always the cheapest and fastest to get into market, but you will run into problems in the long term.

Ville Sointu – Nordea

Det finnes flere eksempler på store databaser som har blitt hacket (Santander Consumer Bank, 2018). Blant annet databasene tilhørende de store teknologiselskapene, med informasjon som nærmest kan beskrive personligheten til milliarder av mennesker verden over. En av de store skandalene er da Yahoo! i 2013 ble hacket, og brukerkontoen til 3,6 milliarder mennesker ble lekket ut (Perloth, 2017). Apple ble også i 2017 anklaget for å ha lekket informasjon om 559 millioner iCloud-brukere, noe de kontant avviste (Hackett, 2017). En annen stor skandale var da 143 millioner amerikanere ble rammet av et dataangrep på det amerikanske ratingbyrået

Equifax (Timberg, Dwoskin, & Fung, 2017). Betalingshistorikk, personopplysninger og bankopplysninger ble lekket ut og endret. Angrepet førte til at amerikanere med plettfri betalingshistorikk plutselig hadde fått anmerkninger og flagg på sin konto, og krevende kunder¹⁴ hadde fått ren historikk. Konsekvensene kunne potensielt vært at lån hadde blitt utstedt til mennesker som aldri skulle hatt det, eller at personer som var flagget for hvitvasking plutselig fikk nye muligheter.

Oversikt over store dataangrep på sentrale databaser fra 2012 til 2016



Figur 5 Oversikt over store dataangrep på sentrale databaser mellom 2012 og 2016
(Santander Consumer Bank, 2018)

Det er ikke utenkelig at det har vært utallige forsøk på å hacke den sentrale databasen til BankID. Det finnes flere eksempler på såkalte phishing-angrep¹⁵, men den sentrale databasen har ikke blitt utsatt for et vellykket angrep, så lenge en skal stole på at slik informasjon ville kommet ut i media (Norsk senter for informasjonssikring, 2014). Den eneste måten å unngå dataangrep på sentraliserte databaser, er å utvikle en avansert brannmur (Cisco, 2018).

¹⁴ Kunder med betalingsanmerkninger og andre kriminelle merknader

¹⁵ Phishing-angrep er angrep hvor man forsøker å stjele innloggingsinformasjon ved å sette opp en nettside som kloner for eksempel DNB sin nettside.

Utviklingen av slik forsvarsteknologi er ressurskrevende, fordi jo mer verdifull informasjonen i databasen er, desto flere hackere ønsker å angripe. Facebook vil eksempelvis i løpet av 2018 ha nærmere 60% av sine 30 000 ansatte til å sikre og beskytte data, og planlegger å ansette ytterligere i årene som kommer (Balakrishnan, 2017).

Desentralisert data kan være løsningen

Krav satt av myndighetene for å hindre blant annet hvitvasking krever store mengder informasjon fra bankene om sine kunder (DNB, 2018). Slik systemet er bygget opp i dag, må hver enkelt bank ivareta informasjon om kundene, noe som gjør at det bygges opp store datasiloer tilhørende hver enkelt bank.

En av de egenskapene som har gjort blokkjeder til en verdensomspennende teknologi, er som nevnt tidligere, den desentraliserte oppbygningen som gjør informasjonen på systemet svært vanskelig å endre. Teknologien sørger for anonymitet på nettverket, ved å sikre data om personene, gjennom unike kryptografiske nøkler.

Så lenge ingen andre har tilgang til en persons private nøkkel, har personen et sikkert pseudonym som lar den utføre anonyme transaksjoner i nettverket. Slik anonymitet kan misbrukes, og det er her to sentrale problemer med blokkjeder dukker opp. Den private nøkkelen må forbli privat. Hvis noen andre får tilgang til en privatnøkkel, kan de få tilgang til enhver fil eller enhet som er kryptert med nøkkelen. Det andre problemet er at en ikke kan være sikker på at riktig informasjon er blitt godkjent og plassert på blokkjeden. En aktør kan for eksempel godkjenne falske KYC-dokumenter¹⁶ og opprette en blokkjede som andre aktører godkjenner over tid, noe som kan gi inntrykk av at de falske KYC-dokumentene er gyldige. En har derfor et behov for å validere at informasjonen som blir puttet på blokkjeden er korrekt, og igjen møter man på behovet for pålitelige tredjepartsaktører.

Man har ikke kontroll på at informasjonen som puttes på stemmer, med mindre man har konkrete bevis

Bjørn Bjercke – Bitgate

¹⁶ Know Your Customer

Bankenes beslutning om hvorvidt de skal bruke det eksisterende systemet, eller implementere blokkjeder, vil være en avveining mellom funksjonalitet og kostnad, i bytte mot sikkerhet. Desentraliserte blokkjeder som for eksempel Bitcoin og Ethereum, er som nevnt tidligere tilnærmet umulig å hacke, men systemene er komplekse, krever enorme mengder datakraft, og er kostbare å implementere. Systemet kan fremlegges slik: Jo mer penger som legges i desentralisering, desto mindre funksjonelt blir systemet. Et mindre funksjonelt system vil resultere i høyere utviklingskostnader av løsninger som kan integrere blokkjedeteknologi i bankenes eksisterende systemer.

Bitcoin har valgt å strippe ned funksjonaliteten i programmeringsspråket sitt, og generelt være så strippet ned som overhodet mulig for å være mest mulig robust og sikkert. Ethereum har innført et programmeringsspråk for å øke kompleksiteten som gir mer fleksibilitet. Det gjør det også mer sårbart.

Torbjørn Bull Jensen – Arcane Crypto

Spørsmålet er om kostnaden ved å sikre den sentrale databasen er mindre enn å desentralisere den, og ikke minst om det er sikkert nok. Vi finner ingen omfattende tilfeller i Norge hvor det har skjedd vellykkede angrep på bankenes og BankID sin database. Det kan tyde på at systemet vi har i dag er godt tilpasset infrastrukturen og risikoen i Norge. Norge er tross alt et lite land med stort fokus på sikkerhet, med et velfungerende rettsvesen¹⁷, så sannsynligheten for at hackere søker andre land kan tenkes å være stor.

4.1.3 Komplekse og kostbare prosesser

Opprettelse av kundeforhold som privatperson i en norsk bank kan enkelt gjøres ved å autentisere seg selv med BankID (BankID, 2018d). På bedriftssiden er det en helt annen prosess knyttet til autentisering ved opprettelse av kundeforhold og kjøp av finansielle tjenester. Denne delen av oppgaven skal først ta for seg kompleksiteten som kreves for å

¹⁷ (World Justice Project, 2018)

opprette et kundeforhold som bedrift, for så å se på hvordan blokkjeder kan bidra til å effektivisere autentiseringsprosessen.

Autentisering – mange aktører og alle må gjøre det

Dersom en ønsker å opprette¹⁸ en bedriftskonto, kreves det utfylling av en rekke opplysninger, blant annet gjennom en Know Your Customer-prosess. Hvilket land personen som oppretter kundeforholdet er skattepliktig til, formålet med kundeforholdet, om det skal mottas eller betales over 100 000 kroner til utlandet, og om personen skal administrere penger for andre. Det må også opplyses om personen som oppretter kundeforholdet er politisk eksponert¹⁹, hvilken adresse personen som oppretter selskapet bor på, hvilken rolle personen har, samt generell kontaktinformasjon for både personen og bedriften. I tillegg må bedriftens virksomhet beskrives: eierforholdet, egenkapital, og hvor mye og hva slags lån som eksisteres i selskapet.

I motsetning til autentisering av personer hvor det ikke er like strenge krav til beskrivelser av kundeforholdet på grunn av BankID sin rolle, er autentisering av bedrifter krevende for både kunde og bank. En stor grad av manuell inntasting fra kunden krever på motsatt side et større kontrolleringsbehov, noe som er både tids- og kostnadskrevende for bankene (Callahan, 2018).

Hvis en bedrift i dag ønsker flere bankforbindelser, en regnskapsfører, en revisor eller forsikring, må hver enkelt institusjon gjennomføre en KYC-prosess før et kundeforhold kan etableres (Callahan, 2018). I tillegg til å være ressurskrevende for bankene, vil det være krevende og frustrerende for nye kunder, ettersom samme dokumentasjon må sendes inn til hver enkelt aktør.

Flere av autentiseringsprosessene er definert av myndighetene. Blant annet har kredittvurderingsbyråer en egen lov som definerer minstekrav for aktørene og praksis for drift (Lov om kredittvurderingsbyrå, 2016). KYC-prosesser er på sin side kun en standard – ikke en lov (Finans Norge, 2018b). Det betyr at ulike banker kan ha ulik praksis knyttet til blant

¹⁸ Det er i denne prosessen opprettet et fiktivt kundeforhold som både person og bedrift i DNB for å kunne gjenspeile prosessen så korrekt som mulig.

¹⁹ Politisk eksponerte personer vil i henhold til Hvitvaskingsloven § 2. f) si personer som innehar rolle som for eksempel statsoverhode, medlem av styrende organ i politisk parti og direktør eller styremedlem i en internasjonal organisasjon, eller som har nære relasjoner til personer som fyller slike roller. (Hvitvaskingsloven, 2018)

annet etablering av kundeforhold. Potensielle kriminelle kan eksempelvis oppsøke uendelig antall banker frem til de omsider blir godkjent. Bare i Norge er det langt over 100 sparebanker, og sannsynligheten for at minst en av de ikke er like oppmerksom kan tenkes å være tilstedeværende (Sparebankforeningen, 2018).

En løsning på problemet beskrevet over kan være å ha en sentralisert enhet som gjennomfører Know Your Customer-prosesser på vegne av institusjonene. En selvstendig aktør med en egen database om hver enkelt bedrift, som distribueres på forespørsel. utfordringene med en slik aktør, er at den vil være utsatt for dataangrep, da det vil være allment kjent at aktøren sitter på store mengder sensitive data.

Et helt konkret område hvor det finnes muligheter for blokkjedeteknologi i norske banker og finansforetak er ved autentisering av bedrifter (Tapscott & Tapscott, 2018). En kan se for seg en løsning hvor kunden logger inn på en KYC-klient²⁰ med sin KYC-ID, utstedt av en hvilken som helst bank. Kunden velger hvilken bank de ønsker å gi sin KYC-informasjon til, det kan være all påkrevd informasjon i en autentiseringsprosess for bedrifter. Informasjonen kan være skrevet inn i et standardisert grensesnitt, hvor det lastes opp nødvendig dokumentasjon på de nødvendige punktene. Så snart kunden har gitt banken tilgang, vil de etter nødvendig due diligence kunne verifisere den innsendte informasjonen som lagres på blokkjeden. Det vil si at hvert enkelt element i verifiseringen lagres på blokkjeden i en unik kode som ikke kan endres.

Videre kan en se for seg at kunden ønsker å opprette en bankkonto hos en annen bank. I henhold til Hvitvaskingsloven må denne banken også gjennomføre en KYC-prosess (Hvitvaskingsloven, 2018). Forskjellen mellom et slikt system kontra dagens, er at den nye banken kan hente informasjon som er verifisert på den eksisterende blokkjeden. Når en kunde har tatt kontakt med den nye banken og oppgitt sin KYC-ID, vil banken kunne søke opp personen i KYC-klienten og be om tilgang til den forrige verifiseringen. Forespørselen kan så godkjennes av kunden uten ytterligere arbeid, fordi blokkjeden sørger for at den oppgitte informasjonen er uendret.

²⁰ Know Your Customer

Prosesen beskrevet over vil kunne bidra til et mer sømløst system rundt KYC-prosesser, som er den største kostnadsdriveren i autentiseringsarbeidet for banker (Callahan, 2018). På den annen side vil en blokkjedebasert løsning ha noen strukturelle utfordringer knyttet til hvordan teknologien er bygget opp. I en åpen blokkjede vil en hvilken som helst kunde kunne opprette et uendelig antall KYC-IDer. Det betyr at dersom en kunde har blitt flagget eller fått avslag på et autentiseringsforsøk som vil spores på blokkjeden, vil det enkelt kunne opprettes en ny ID uten spor tilbake til avslaget. Et slikt system vil kunne fungere godt for å håndtere de kundene som følger regelverket, og mindre godt for de som har noe å skjule. Dersom en antar at kunder som har noe å skjule er de som i størst grad forbindes med risiko for bankene, og derav de som krever mest ressurser, kan et system som her beskrevet virke mot sin hensikt.

Noen av de strukturelle utfordringene ved åpne blokkjeder kan løses ved å samle autentiseringsaktørene i et nettverk som baserer seg på en Permissioned-blokkjede. Systemet kan bygges opp slik at hver enkelt kunde kun kan opprette én ID ved å knytte sin KYC-ID til for eksempel organisasjonsnummeret. Utfordringen med et slikt system er at alle aktørene må enes om et felles grensesnitt, noe som kan være krevende²¹.

4.1.4 Revisjonens rolle

En aktør som er helt sentral for bankenes risikovurdering av bedrifter er revisjonsselskapene. Dersom en bedrift ønsker å ta opp et lån, må banken ha en eller annen form for kompensasjon for risikoen de utsettes for (Bernhardsen & Larsen, 2002). I et boliglån kan kompensasjonen være sikkerheten i selve boligen, i motsetning til investeringer knyttet til drift og fremtidig inntekt i et selskap, som er vanskelig å pantsette. Bankene er derfor avhengig av å få fremlagt dokumentasjon som argumenterer for at de skal utsette seg selv for risiko. Regnskap er en slik type dokumentasjon, et standardisert format som alle selskaper er pliktig til å føre (Regnskapsloven, 1999).

En av utfordringene tilknyttet regnskapets pålitelighet er at bedriftene selv kan føre og utarbeide regnskapet internt, hvor det i visse sammenhenger kan være fristende for bedrifter å pynte på regnskapstallene. Feil i regnskapet kan for eksempel føre til at staten betaler tilbake

²¹ Forklares nærmere i delkapittel 4.2 og 4.3

for mye skatter og avgifter, eller at bankene vurderer driften som bedre enn den tilsynelatende er. Jo større selskapene er, desto større betydning får eventuelle feil, både for samfunnet og bankene. Det er derfor innført en lov om revisjon som blant annet sier at alle virksomheter med en omsetning over 5 millioner kroner skal kontrolleres av en revisor (Revisorloven, 2017, Kapittel 2. Revisjonsplikt m.v.§2-1).

Revisorens oppgave er å autentisere verdiene og postene i regnskapet, for å sikre at samfunnet og aktørene som baserer seg på regnskapet har riktige og tilsynelatende like forutsetninger for å vurdere driften (Lazanis, 2015). Det at samfunnet har tillit til revisoren kan imidlertid i visse sammenhenger skape problemer. En revisors inntektskilde er bedriftene de skal revidere. Med andre ord vil det for en selskapsrevisor være viktig å tjenestegjøre kunden i så stor grad som mulig, uten at det er i strid med lovverket. Det er enkelte tilfeller hvor tilliten blir misbrukt, slik som i Enron-skandalen i 2002 (Hosseini & Dr. Mahesh, 2016). Uvanlige regnskapsprosedyrer som hadde foregått i løpet av hele 90-tallet grenset til bedrageri. Uvanlige prosedyrer i så stor grad at verdens femte største revisjonsselskap Arthur Andersen burde ha avdekket at noe var galt. Skandalen førte til konkurs av Enron, men også oppløsning av Arthur Andersen.

Blokkjedeteknologi kan fjerne behovet for tredjeparter som autentiserer verdi ved at alle transaksjoner umiddelbart lagres på en blokkjede (Holm & Frøystad, 2015). Dersom en datamaskin selges hos en elektronikkbutikk, vil transaksjonens innhold automatisk lagres i et regnskap. Blokkjedens oppbygning gjør at transaksjonen ikke kan endres i ettertid uten at det fanges opp i endringene av hash-koden. En kan derfor være sikker på at datamaskinen som handles ikke vil bokføres med en annen verdi enn den reelle verdien av den aktuelle datamaskinen. Umiddelbar oppdatering av blokkjeden, som igjen vil oppdatere regnskapet, vil til enhver tid kunne fremlegge sanntidsregnskap. Bankene kan dermed i større grad vurdere den sanne risikoen tilhørende salg av sine finansielle tjenester, fordi de ikke baserer deres analyse på fjorårets tall. Bankene kan også ved en blokkjedebasert regnskapsfremstilling være sikker på at tall ikke er sminket eller endret, som igjen kan bedre beslutningsgrunnlaget.

På den annen side har blokkjedens rolle i regnskap og revisjon et sentralt problem. I likhet med problematikken knyttet til en blokkjedebasert Know Your Customer-løsning kreves det også her tillit til at informasjonen som puttes på blokkjeden stemmer. Hvis datamaskinen som ble solgt i systemet faktisk ikke var den samme som ble levert til kunden, vil et slikt system falle sammen. Selv om det hadde eksistert et 100% distribusjonssystem hvor mennesker ikke

hadde vært direkte involvert, ville det fremdeles vært behov for tillit til de menneskene som programmerte systemet. Systemet vil ikke kunne fange opp om en flybillett betalt fra selskapets konto ble brukt til en privat tur eller til en bedriftsreise. Blokkjedeteknologi vil ikke kunne løse disse problemene slik teknologien fremstår i dag, og en vil være avhengig av å ha uavhengige tredjeparter som kan kontrollere og autentisere verdier i et selskap.

Blokkjedeteknologi kan imidlertid påvirke bransjen på andre måter. Flere av intervjuobjektene trekker frem at teknologien ikke vil endre bransjen fundamentalt, men at det på noen områder kan være hensiktsmessig å ta i bruk infrastrukturen.

Bank og revisjon kommer til å påvirkes av blokkjedeteknologi, men ikke på den måten journalister og konsulenter fremlegger det. Blokkjeder kommer ikke til å løse alle problemer, men teknologien kan bidra til å skape noen nye muligheter. Slik som hvordan vi reviderer selskaper som driver med krypto-bokføringen, noe vi definitivt blir påvirket av

Magnus Jones – EY

En anvendelse av blokkjedeteknologi som kan påvirke revisjonsbransjen, er ved bruk av smartkontrakter. Dersom et regnskapssystem er bygget opp av både smartkontrakter og blokkjedeteknologi kan det løse noen av utfordringene som er beskrevet over. Bokføring av en flybillett kan for eksempel avhenge av flere faktorer, definert av en smartkontrakt, som en betingelse for bokføring av flybilletter. Dersom en ansatt i Oslo skal fly til London, vil bokføringen først godkjennes når et møte er booket i London, eller en påmelding til en konferanse har skjedd, og overordnede leder har godkjent kjøpet. Når bokføringen først er gjennomført sikrer blokkjeden at den i ettertid ikke er endret.

Dersom et slikt system skal fungere i virkeligheten, må det designes smartkontrakter som sikrer at lover og regler blir fulgt. Det må derfor være personer som reviderer og kontrollerer disse kontraktene, noe som gjør at næringen fortsatt er avhengig av uavhengige tredjeparter.

Vi har hatt en del interessante diskusjoner om hva slags rolle revisorer har i fremtiden. Jeg tror revisjonsbransjen som sådan fortsatt vil være nødvendig, men at det vil endre seg fra å revidere transaksjoner og pengeflyt, til å handle mer om validiteten av smartkontrakter. Så en revisor vil kanskje i fremtiden i større grad være en jurist fremfor en økonom.

Hvorvidt et blokkjedebasert system er mer effektivt for både samfunnet og revisjonshusene er vanskelig å si på bakgrunn av begrenset tilgjengelig informasjon. Revisjonsbransjen vil uansett fortsatt være helt essensielt for samfunnet, og for bankene når de skal vurdere salg av finansielle tjenester (Psalia, 2017).

4.2 Transaksjoner og flytting av verdier

Det er gjort undersøkelser av blant annet Bain and Company²² og PWC²³, om hvilken påvirkning blokkjeder kan ha på det internasjonale finansmarkedet. De konkluderer med at aktørene i finansmarkedet kan spare mellom \$ 15-35 milliarder ved å implementere Distributed Ledger Technology (Olsen , Ford, Ott, & Zeng, 2017). Mer enn 80% av de spurte lederne mener at blokkjeder vil ha, og har en signifikant påvirkning på markedene (PWC, 2018c). En av de største besparelsene trukket frem i rapportene, og i våre intervjuer, er effektiviseringen av internasjonale transaksjoner. Vi vil videre studere hvordan dagens system er bygget opp slik at vi kan undersøke de tjenestene som trues og hvordan bankene har respondert på trusselen.

4.2.1 Infrastrukturen i bransjen

Hver dag overføres titalls milliarder kroner mellom kontoer i hele verden (U.S. Department of the Treasury, 2006). Det finansielle systemet sørger for at pengene ikke blir brukt flere ganger, ved å være en pålitelig tredjepartsaktør. Systemet er komplekst med et stort antall mellomledd. I Norge må bankene ha en banklisens eller lignende kostbare konsesjoner utstedt av Finanstilsynet for å kunne selge finansielle tjenester (Finanstilsynet, 2016). Bankene må også tilfredsstille en rekke krav beskrevet i både norsk lov og av EU, før konsesjonene kan tildeles.

²² (Olsen , Ford, Ott, & Zeng, 2017)

²³ (PWC, 2018a)

Det må i Norge blant annet foreligge en startkapital på minst fem millioner euro²⁴, personer i finansforetaket må egnethetsvurderes²⁵, og det må betales tilsynsavgift før en kan starte som en bank (Finans Norge, 2017b). Hele vårt monetære system er bygget på slike lover og regler, og det er med på å skape den sikkerheten som kreves for et pålitelig transaksjonssystem. Integriteten til systemet opprettholdes ved at det er et kontinuerlig innsyn fra Finanstilsynet, hvor endringer må gå gjennom tilsynet før det kan bli iverksatt.

DNB kan drive som bank fordi de har lisens. For alle beslutninger DNB gjør må de stille seg spørsmålet om hva som skjer med lisensene ved å ta de valgene de gjør. Skal de prøve et nytt produkt, hva skjer med lisensen? Det har vært svært vanskelig å få en slik lisens, derfor er det svært få og vanskelig å bli bank, og alle bankene ser like ut.

Fredrik Haga – Dune Analytics

En av utfordringene ved konsesjoner, er at de også kan trekkes tilbake om virksomhetene ikke driver i henhold til satte standarder, blant annet god forretningsskikk (Finanstilsynet, 2008). Det er flere eksempler på banker som har mistet konsesjonen sin på grunn av brudd på lovverket. Et slikt eksempel er Glitnir Privatøkonomi som i 2007 mistet sin konsesjon på grunn av ensidig salg av produkter med høy fortjeneste. Prosessen med kontinuerlig overvåking er både tidkrevende, komplisert og dyr, hvor hvert land har sitt individuelle system med lover og regler (Barth, Caprio, & Levine, 2013). Effekten er et fragmentert og ressurskrevde globalt betalingssystem, hvor det nå er raskere å sende en ambolt til Kina med posten enn å sende en person i Kina penger for å kjøpe den selv (Tapscott & Tapscott, 2018).

Når penger overføres fra en konto til en annen i samme bank, forlater pengene aldri banken (Brown, 2013). Banken oppdaterer sine egne poster, trekker beløpet fra kontoen til personen som overfører og legger til samme beløp til mottakers konto. I Norge går alle transaksjoner mellom banker gjennom NICS²⁶, et system hvor det daglig overføres over 200 milliarder kroner (SVEA, 2017). Transaksjonene gjøres i hverdager, 4 ganger om dagen på tidspunktene 05:40, 11:05, 13:35 og 15:35. Dette impliserer at overføringen som for eksempel ikke er gjort

²⁴ Krav som gjelder alle banker som operer innen EØS (Finans Norge, 2017b)

²⁵ Egnethetsvurdering utføres av Finanstilsynet på enkeltpersoner og sjekker blant annet om personen er forbundet med straffbare forhold, om utdanning og økonomisk adferd.

²⁶ Norwegian Interbank Clearing System

innen fredag kl 15:35 vil være i en likviditetsmessig limbo²⁷ frem til mandag morgen, 62 timer etter at pengene ble sendt.

De samfunnsøkonomiske kostnadene transaksjoner har i samfunnet, analyseres med jevne mellomrom, hvor den siste rapporten ble lagt frem i 2014 (Norges Bank, 2014). Ifølge Norges Bank utgjorde transaksjonskostnader 0,48 % av Norges BNP i 2013. Ved forrige måling, gjort i 2007, utgjorde kostnadene 0,49% av BNP. Ved å justere for tidsforskjellen kan en se at samfunnsøkonomiske kostnader for transaksjoner både nominelt og reelt har blitt redusert²⁸ (Norges Bank, 2009). En indikasjon på effektiv organisering og teknologi reflekteres av lave kostnader, hvor Norge er rangert som det tredje mest effektive betalingssystemet Europa (Menon Economics , 2017).

Samfunøkonomiske kostnader av transaksjoner (Prosent av BNP)	
Finland	0,34%
Nederland	0,42%
Norge	0,48%
Sverige	0,68%
Danmark	0,78%

*Tabell 1 Samfunnsøkonomiske kostnader av transaksjoner
(Menon Economics , 2017)*

Siden 2014 har mye skjedd innen transaksjonsprosessering i realtid, hvor betalinger nå skjer på sekunder, til lave kostnader, gjennom en nasjonal infrastruktur drevet av Bits (Bits, 2018a). De sikrer og styrker en effektiv betalingsformidling og infrastruktur i Norge, ved å tilby en felles plattform som brukes, driftes og eies av bankene. Formålet med et slikt system er å håndtere utfordringene og mulighetene fremtiden kan bringe i form av nye aktører, teknologi

²⁷ Limbo er en udefinerbar tilstand/ sted

²⁸ Ved å justere for tidsforskjellen, utgjorde kostnadene 0,42% av BNP (Norges Bank, 2014)

og reguleringer. Bits oppgave er å sikre en effektiv og sikker infrastruktur for det norske samfunnet (Bits, 2018b).

Man kan bruke eksempel fra jernbanenettet for å illustrere hva Bits er. Norge har 11 selskaper som har lov til å kjøre tog på linjene, men det er ingen som lager 11 jernbaneskinner mellom Bergen og Oslo – her kommer infrastruktur inn. Det selskapet som står for jernbane, strømføring til skinnene og signalene er Jernbaneverket. Det å kjøre toget gjør NSB og Flytoget. Bits er veldig forenklet Jernbaneverket til finansnæringen.

Eivind Gjerdal – Bits

Det norske intrabanksystemet er som sagt effektivt, og behovet for store reformer for å redusere kostnader og korte ned tiden på transaksjoner fremstår som lite. Imidlertid har det norske betalingssystemet sett på muligheten til å effektivisere systemene ytterligere ved bruk av blokkjedeteknologi, uten å ha funnet noen konkrete bruksområder.

Det vi har brukt en del tid på å finne ut er hvor blokkjeder faktisk er mer effektivt enn det systemet vi har i dag. Svaret på det er ingen. Vi ser ingen aktuelle scenarioer hvor blokkjeder og Distributed Ledger Technology per nå er mer effektivt enn slik vi driver i dag.

Eivind Gjerdal – Bits

Internasjonale pengeoverføringer fungerer i utgangspunktet likt som nasjonale bankoverføringer, men flere land involvert fører til mer kompleksitet. I Brussel er det mest utbredte systemet for internasjonale overføringer lokalisert – SWIFT²⁹ (SWIFT, 2018b). SWIFT er et meldingssystem med 11 000 kunder i over 200 forskjellige land og territorium, brukt til å overføre informasjon og instruksjoner sikkert gjennom en standardisert kodeks. Det lar banker sende penger til hverandre, nesten hvor som helst i verden, og i mange ulike valutaer (Seth, 2017).

Digitale verdiobjekter kan sees på som en form for fordring på en motpart, hvor SWIFT-systemet kan illustreres med et fiktivt eksempel (SWIFT, 2018b): Ved å ha penger i banken,

²⁹ Society for Worldwide Interbank Financial Telecommunications

så har man banken sitt gjeldsbevis. Ved å for eksempel selge tekstiler i Portugal får man penger lokalt, og har dermed en fordring på en bank i Portugal, et bankinnskudd. Pengene kan ikke sendes direkte til Norge, ettersom det er en gjeld på en portugisisk bank, som ingen norske banker har en relasjon til. Pengene kommer ikke til Norge før det finnes en kjede med banker som suksessivt stoler på hverandre, og som kan bytte gjelden i en kjede bortover. Bankene bytter fordringene på hverandre, helt til de avslutningsvis ender opp som et innskudd i en norsk bank, for eksempel Nordea.

SWIFT er med andre ord et sikkert meldingssystem der banker deler fordringer på hverandre (Seth, 2017). Av slike grunner må mer menneskelig intervensjon brukes for å overføre de faktiske midlene, samt reguleringer i de enkelte landene som transaksjonene sendes gjennom. Bankene forplikter seg også til å utføre visse kontroller for å hindre blant annet hvitvasking, før betalinger kan gjennomføres. Slike variabler gjør at en transaksjon internasjonalt kan ta alt fra en dag til et par måneder. Systemet for overføring av verdier ble utviklet tidlig på 70-tallet, og går ofte tregt med høye tilknyttede kostnader, men har til nå vært den mest effektive måten å overføre verdier over landegrensene (Tapscott & Tapscott, 2018).

Bankene over hele verden ser på clearance-funksjonen, hvor de ønsker en effektivisering av prosesser som i dag tar altfor lang tid og koster for mye penger.

Magnus Jones – EY

4.2.2 Produkter som trues

Blokkjedeteknologi har med mekanismene forklart i kapittel 3, teoretisk kapasitet til å utfordre verdi- og dataoverføringer som er lagret og registrert i en hovedbok. Blokkjeder og andre distribuerte hovedbøker skiller seg fra eksisterende databaser primært på grunn av den distribuerte arkitekturen og bruk av konsensusmekanismer. Teknologien unngår behovet for tillit til sentraliserte og pålitelige mellommenn, hvor en av de mer omtalte mulighetene blokkjedeteknologien har, er den som ble introdusert av Satoshi Nakamoto i 2008, betalingssystemer (Nakamoto, 2008).

Ved bruk av blokkjeder til transaksjoner vil ting bli mye lettere. Prisen vil komme opp med en gang og det vil være rask betaling, samtidig som det kontinuerlig vil være verifisering om at for eksempel pengene er på vei.

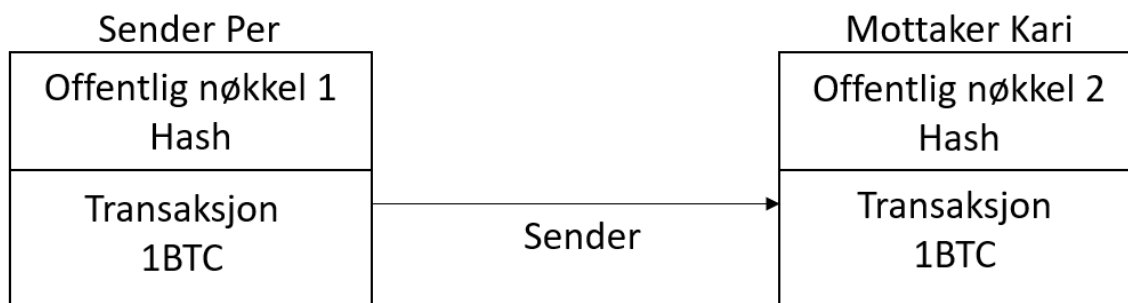
Blokkjedens store fordel, og det som gjør teknologien relevant for mange, er uavhengigheten teknologien kan skape. Dagens system er bygget opp av sentraliserte databaser, kontrollert og styrt av hver enkelt bank (Stigsen, 2017). En åpen plattform skaper grobunn for innovasjon, der hvem som helst kan komme med nye tjenester som utnytter sikkerheten eller infrastrukturen i åpne blokkjeder (McKinsey, 2016). Teknologien har de siste årene vokst i popularitet blant bankene og deres konkurrenter, fordi den kan effektivisere dagens drift.

I dagens system går 6,95% av alle pengeoverføringer internasjonalt til transaksjonskostnader (The World Bank, 2018). Dette er enorme summer, der det er et stort potensial for å redusere kostnader. Interbankbetalingssystemer som SWIFT er gamle, langsomme og i økende grad utsatt for cyberangrep, på et tidspunkt hvor banker er under et enormt press for å redusere kostnader og beskytte kundedata fra hackere (Sharma, 2017).

Desentraliserte, distribuerte løsninger har mulighet til å løse flere av de overnevnte problemene (Marr, 2016). Teknologien kan redusere kostnader i formidling, sikring og verifisering av transaksjoner. Videre kan slike løsninger redusere operasjonell- og motpartsrisiko, og en vil så snart transaksjonen er lagt til i blokken se om motparten faktisk har betalt eller ikke. Fordelene slike systemer gir må veies opp mot flere ulemper, hvor de største utfordringene til nå har vært kapasitetsbegrensninger, skalerbarhet og personvern ved transaksjoner på blokkjeden (Back, 2018). Vitalik Buterin, grunnleggeren av Ethereum, har antydnet at eksisterende åpne blokkjeder, ikke kan oppnå den skalerbarheten som trengs for å gjennomføre transaksjoner, uten at det går på bekostning av sikkerhet og desentralisering (Tomaino, 2018).

Et sentralt problem ligger i verifiseringsprosessen til åpne blokkjeder. Transaksjoner verifiseres ved at enhver node i nettverket må ha tilgang til informasjonen som ligger i blokkjeden. (McKinsey, 2016). Åpne blokkjeder er dermed fundamentalt forskjellig fra sentraliserte databaser, der transaksjoner kun er synlige for databasens skapere og administratorer. Ved å tildele nodene på nettverket en unik ID, vil alle transaksjoner over nettverket være anonyme. Problemet ligger i at selv om adressen er anonym, kan mye læres av å analysere atferden og informasjonen som blir sendt i nettverket. I en åpen blokkjede publiseres alle transaksjoner offentlig, og de er tilgjengelige for alle deltakende noder i systemet, som illustrert i figur 6. Dette er et eksempel på en transaksjon av én Bitcoin, fra

avsenderen Per, til mottakeren Kari. Her sender Per detaljer om transaksjonen offentlig og hver node på nettverket kan se detaljene i transaksjonen samtidig som mottaker Kari.



Figur 6 Bitcoin-transaksjon

Ved å analysere informasjonen i transaksjoner fra én adresse til en annen, kan en over tid potensielt identifisere hvem Kari eller Per er, eller hvilket selskap som står bak de unike offentlige nøklene. I et forretningsperspektiv er dette lite ønskelig, ettersom alle transaksjoner registreres i en global offentlig hovedbok, som potensielt kan skape både konkurransemessige- og juridiske problemer (Accenture, 2016). Et eksempel på dette er når DNB og Storebrand flytter verdier mellom hverandre, da vil de trolig ikke at konkurrenter som Nordea og Sbanken skal tilegne seg all informasjonen om transaksjonen. Et annet problem er hvis enkelte transaksjoner blir gjennomført på vegne av en banks kunder, det kan da, basert på dagens regulatoriske system, være ulovlig å avsløre informasjonen om kundene på denne måten (NOU, 2011). Det er med andre ord et behov for konfidensialitet ved flytting av verdier som åpne blokkjeder per dags dato ikke kan tilfredsstille. En alternativ versjon av blokkjedeteknologi, såkalte Permissioned-blokkjeder, har en mulig løsning på konfidensialitetsbehovet bransjen krever.

Permissioned-blokkjeder

Permissioned-blokkjeder fungerer gjennom mekanismene forklart i kapittel 3, som lukkede økosystemer. Brukere er ikke fritt i stand til å bli med i nettverket, se registrert historie eller utstede egne transaksjoner. Permissioned-blokkjeder har betydelig ulike egenskaper fra desentraliserte systemer, og fungerer på mange måter likt som dagens system (IBM, 2018b). Ved å flytte informasjonen til en felles hovedbok er det muligheter for å digitalisere og

effektivisere prosesser som i dag i stor grad er manuelle. To store prosjekter på Permissioned-blokkjeder er Corda av R3-konsortiet³⁰, og Hyperledger³¹ av Linux-stiftelsen. De har som formål å undersøke mulighetene blokkjeder har, gjennom Distributed Ledger Technology.

R3-bankkonsortiet ble inspirert av offentlige blokkjeder til å bygge tjenester ønsket av deres medlemmer (R3, 2018). Prosjektet Corda er en plattform med formål å fjerne friksjon i transaksjoner mellom bedrifter, der informasjon om avtaler og andre transaksjonsdetaljer kun er tilgjengelige for de involverte partene. Selv om Corda er basert på blokkjedeteknologi, er ikke infrastrukturen bygget opp av blokker i en blokkjede, men gjennom Distributed Ledger Technology.

Corda is a good example of how banks would like to see how decentralization is happening in the financial sector/ services infrastructure. That is the way we control and get to see who sees what, in context of any transaction, our customers data is controlled by party's that they trust, and not leaked to any third party without their permission, we get settlement finality and proper scalability on the network.

Ville Sointu – Nordea

Et annet prosjekt som baserer seg på Corda-systemet, er Marco Polo-prosjektet som DNB er en del av. Formålet til prosjektet er å effektivisere betalinger i et lukket nettverk hvor konsortiets medlemmer kan overføre verdier mellom hverandre (Marcopolo, 2018).

Prosjektet kan hele tiden ha oversikt over hvem som skylder penger. Dette er et eksempel på en veldig spesifikk løsning som tar for seg et problem i «Trade Finance», handel på tvers av landegrenser.

Lasse Meholm – DNB

En annen løsning på konfidensialitetsproblemet er ved hjelp av Hyperledger Fabric (Hyperledger, 2018a). Hyperledger tar sikte på å skape et miljø, der programvareutviklere og

³⁰ (R3, 2018)

³¹ (Hyperledger, 2018a)

selskaper kan møtes for å koordinere et blokkjederammeverk. Systemet er delt inn i forskjellige kanaler med ulike nettverk, der en kanals transaksjoner fungerer som en separat blokkjede, uleselig for alle andre enn de involverte partene. Eiendeler kan ikke flyttes fra en kanal til en annen uten hjelp av en betrodd mellommann som er aktiv på begge kanalene.

Vi har et annet prosjekt som er utviklet sammen med BitSpace i Oslo, det handler om måten å dele forslag til avtaler med eksterne parter, eksempelvis i Danmark eller England. Den funker slik at når vi sender et forslag til avtale, så kan alle parter gjøre endringer i forslaget, hvor blokkjeden sikrer at vi har kontroll på alle endringer. Tidligere sendte vi bare rundt et Word-dokument, uten kontroll på hvem som hadde gjort hvilke endringer. Så blokkjeder er en glimrende teknologi for å sikre denne kontrollen og oversikten.

Lasse Meholm – DNB

Den finansielle sektoren velger altså konfidensialitet og skalerbarhet over de fordelene en får av å ha et desentralisert nettverk. Dette betyr at det fortsatt er behov for tillit til en tredjepartsaktør for å kunne verifisere transaksjoner, med de kostnadene det medfører. Flere av våre intervjuobjekter trekker frem at inntil problemene rundt skalerbarhet, personvern og sikkerhet er fikset, samt at klare regulatoriske retningslinjer er lagt, vil trolig Permissioned-blokkjeder være den eneste fungerende løsningen i den finansielle sektoren. Behovet for disse kvalitetene er fundamentale for at dagens system skal fungere, og fokuset bankene har rundt teknologien ligger deretter.

We stop talking about Blockchain in general but tend to talk about Distributed Ledger Technology. We want to control the governance of this networks and we need to be able to know who is trading on this network and who is liable for what and in what state of the transaction. We need to have things like clear rulebooks and clear contractual applications where we connect to these networks.

Ville Sointu – Nordea

Bruk av Permissioned-blokkjeder gjør at bankene kan gjøre mye av det samme som de gjør i dag, ved å stå sentralt som en tredjepart samfunnet fortsatt må stole på. Ved å bruke Distribuert Ledger Technology kan prosessen potensielt effektiviseres.

Hindringer

I en optimal verden ville alle banker umiddelbart blitt med i en global blokkjede dagen en slik tjeneste ble levert. I virkeligheten, som illustrert gjennom de forskjellige konsortiene, vil flere blokkjeder bli vedtatt av ulike grupper med banker. Dette skaper en av hovedutfordringene til implementeringen av teknologien – samarbeid.

Mange ulike blokkjeder resulterer i mange ulike interne systemer mellom aktørene som benytter seg av teknologien, som igjen kan ødelegge en av de store fordelene til blokkjeder, nettverkseffekten (Swanson, 2018). Hvert prosjekt må utvikle en strategisk utformet arkitektur og et åpent kildekode-rammeverk som dekker de grunnleggende funksjonalitetene for alle aktørene. Det må eksisterer et samtykke i styringsbeslutninger om hvordan systemet, data og investeringer vil bli ledet og administrert mellom bankene, både nasjonalt og internasjonalt (McKinsey, 2018).

Et problem er at det er mange banker med i prosjektet, og at vi må bli enige om hvordan det skal være. Det å skrive en kontrakt i Norge er ikke det samme som i Spania eller Hong Kong, så vi bruker mye tid på å bli enige. Da må dette systemet sys sammen med systemene som vi allerede har i banken.

Lasse Meholm – DNB

I et konsortiumoppsett må aktørene, som Lasse Meholm påpeker, eniges om systemets lover og regler. Dette kan illustreres gjennom et eksempel, loggføringen av en aksje: Når IT-systemene registrerer en gyldig aksje som er overført til en person på gyldig vis, må det finnes en organisatorisk enighet om hva som gjøres når det viser seg at verifiseringen eksempelvis skyldes en utro tjener. Rettslige prosesser og mekanismer må være på plass, slik at en kan reversere uriktige transaksjoner i nettverket. Det å bli enig om felles regler har vist seg å være det vanskeligste elementet å løse for å få Permissioned-blokkjeder fra et pilotprosjekt til fullskala (McKinsey, 2018). Det er ingen elementer i Distributed Ledger Technology som gjør det lettere å løse slike uenigheter. Prosjekter som blant annet Corda, jobber aktivt for å etablere slike standarder. Ved å ta sikte på å følge satte industristandarder og overholdelse av eksisterende finansregulering, kan det bli enklere å lage et felles system aktørene kan eniges om (Brown, Carlyle, Grigg, & Hearn, 2016).

Grunnen til at man ikke har oppdatert disse systemene som er ineffektive og utdaterte, er ikke fordi man ikke har teknologien til det. Det er så utrolig vanskelig å finne sammen for å lage et alternativ som alle kan være enige om.

Torbjørn Bull Jensen – Arcane Crypto

Usikkerheten rundt hva som blir de etablerte markedsstandardene, samt kostnadene ved å bli med på et tidlig stadium, gjør at flere av våre intervjuobjekter har en avventende holdning til implementeringen av Permissioned-blokkjeder. Til gjengjeld følger de kontinuerlig med i markedet, og vil raskt være klare til å hoppe på den, eller de plattformene som blir markedsstandard.

Vi har sett på noen globale initiativer, men de fleste krever ressursinnsats og investeringer, og det kan igjen bli vanskelig å velge hvilket initiativ man skal hoppe på. Så vi venter heller til noe er etterprøvd, for så å hoppe på dette med en litt høyere premie, men med langt lavere risiko. Vi har rigga oss for å følge med, men har hittil ikke sett noe som er åpenbare «go» til å bli med på. Vi evaluerer forløpende, men i og med at blokkjede ikke er en av de områdene hvor vi skal være først ute, så venter vi til vi har noe konkret å hoppe på.

Svein Ove Langeland – Sparebanken Vest

Hvorvidt en skal gå fra systemet vi har i dag, som tross alt fungerer, vil være en avveining mellom de fordelene og ulempene som blokkjedebasert teknologi skaper. Rakesh Sharma påpeker i artikkelen «*Does Blockchains popularity mean the end of SWIFT?*», at infrastrukturen i SWIFT utvikles stadig (Sharma, 2017). Selskapet møter konkurranse fra flere fronter, blant annet gjennom prosjektene Hyperledger og R3 Corda. Økt konkurranse har ført til at SWIFT har reagert med sitt eget initiativ for innovasjon i det globale betalingssystemet, for å unngå at nye aktører setter dem på sidelinjen (SWIFT, 2018a).

Løsningen heter SWIFT GPI³² som av de selv omtaltes som den nye standarden i globale betalinger (SWIFT, 2018a). Bankene vil med systemet kunne sende og motta fordringer raskt

³² GPI = Global Payment Innovation

og sikkert, hvor som helst i verden, med full åpenhet om hvor en betaling er til enhver tid. Formålet med teknologien er å forbedre internasjonale betalinger med fart, sikkerhet og stabilitet, og på så måte skal de forbedre elementene som per dags dato har vært flaskehals i systemet.

SWIFT har nå effektivisert sine prosesser på de områdene som blokkjeder kan forbedre

Thomas Tjøstheim – Sbanken

SWIFT har også sett på mulige blokkjedeløsninger for å løse systemets problemer. Selskapet uttalte etter et pilotprosjekt som baserte seg på en Distributed Ledger Technology-løsning at blokkjedeteknologi trenger å utvikles betydelig, før den kan behandle mengden transaksjoner som sendes over nettverket hver dag (Arnold, 2018a). SWIFT trekker også fram det faktumet at banker og långivere må revidere sine operasjoner og kjernesystemer betraktelig, før de kan bytte til et blokkjedebasert system. De 28 bankene som var med på pilotprosjektet til SWIFT, krevde opprettelse av til sammen 528 «sub-ledgers³³» for å unngå at konfidensiell informasjon ble overvåket av konkurrerende banker. Implementering av systemet i stor skala vil derfor kreve betydelige investeringer og store mengder datahåndtering.

Det gjenstår å se om noen av de virkelig klarer å høste frukter av Permissioned-blokkjeder. Det er høyst usikkert.

Torbjørn Bull jensen – Arcane Crypto

Det er klare likheter mellom aktørene som forsøker å implementere Permissioned-blokkjedeteknologi. Mulighetene for effektivisering av system er tilstedeværende, men usikkerheten knyttet til kostnader og overvåking fra konkurrenter er et reelt problem. SWIFT har tro på den underliggende teknologien, og at utfordringene som finnes i dag vil kunne løses (Arnold, 2018a). De teknologiske og organisatoriske utfordringene gjør imidlertid at implementeringen av teknologien ikke vil skje før den har utviklet seg betydelig. SWIFT uttalte, i likhet med flere av våre intervjuobjekter, at når det kommer en løsning som lar seg implementere i storskala vil de være klare for å ta den i bruk.

³³ Forskjellige konfidensielle kanaler på et Permissioned-nettverk

4.2.3 Lightning Network

Det er utviklet løsninger for problemene åpne blokkjeder har rundt kapasitetsbegrensninger, skalerbarhet og personvern, hvor en av de mest lovende er Lightning Network (Chester, 2018). Plattformen er bygget opp på Bitcoin-teknologien, og gjør det mulig å håndtere millioner av transaksjoner uten å være koblet til nettverket (Lightning Network, 2016). Teknologien skal kunne gjennomføre store mengder transaksjoner på nettverket uten å kontinuerlig måtte oppdatere blokkjeden. Gjennom Lightning Network vil en starttransaksjon registreres på Bitcoin sin blokkjede, og en kanal utenfor nettverket vil bli opprettet. Transaksjoner mellom aktørene vil her fritt kunne bli gjort utenfor blokkjeden. Dersom det for eksempel skulle oppstå uenighet mellom aktørene vil kanalen bli lukket, og den endelige balansen vil være det som registreres på blokkjeden som en sluttransaksjon. Det er da bare en start- og en sluttransaksjon som behøves på Bitcoin sin blokkjede, og det vil teoretisk kunne redusere antall transaksjoner som går igjennom nettverket betraktelig.

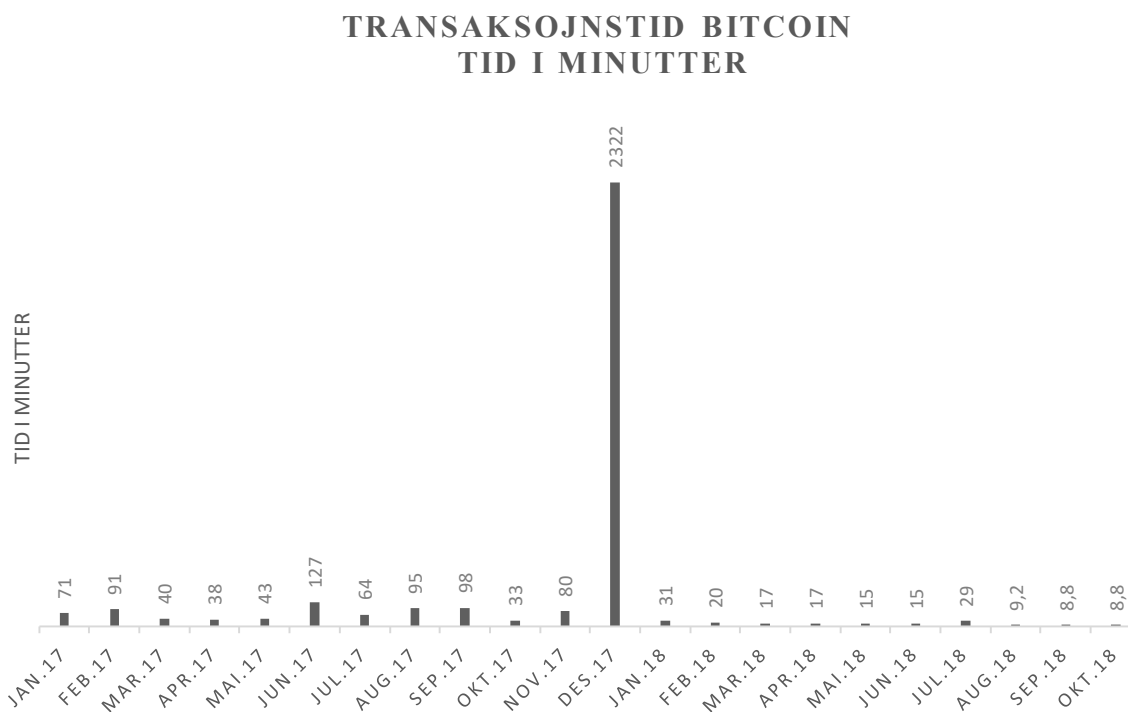
Tenk på en blokkjede med Lightning-nettverket som en høyesterett som er helt forutsigbar, med mange saker som folk kjenner til. Da kan man løse mange saker uten å ta saken til høyesterett, fordi begge parter vet hva som vil skje om man tar den til høyesterett. Den digitale versjonen er at man kan løse finansielle Bitcoin-transaksjoner uten å bruke blokkjeden, fordi man vet at om det skulle bli en uenighet kan man ta den siste versjonen av transaksjonen og gjøre opp med 100% forutsigbarhet med Bitcoin sin blokkjede.

Torbjørn Bull Jensen – Arcane Crypto

Skaleringsproblemer til åpne blokkjeder kom tydelig frem under den store interessebølgen for kryptovalutaer rundt juletid 2017 (Browne, 2017). Interessen for Bitcoin var så stor at kostnadene per transaksjon kom helt opp i \$ 55, og tiden det tok å gjennomføre en transaksjon var på nesten to døgn. Samme transaksjonen kostet i november 2018 under \$ 0,5 og tok i snitt åtte minutter å gjennomføre (BitInfoCharts, 2018).

I desember skulle alle inn på nettverket, noe som førte til kø på systemet. Transaksjonskostnadene og tiden føyk i været fordi alle bydde over seg selv for å få gjennomført transaksjonen så raskt som mulig.

Bjørn Bjercke – Bitgate



Figur 7 Transaksjonstid for Bitcoin (Statista, 2018)

Figur 7 illustrerer det store skalerbarhetsproblemet teknologien har, og som Lightning-nettverket ønsker å løse (Lightning Network, 2016). Bakgrunnen for at transaksjoner tar tid, kommer av størrelsen per blokk i Bitcoin-nettverket. Det betyr at transaksjoner som overskrider kapasiteten til en blokk, blir sittende fast i en kø, avventende på bekreftelse av minere. Driften og sikkerheten av slike nettverk opprettholdes, som forklart i kapittel 3, av minere. Det kreves dyr maskinvare for å kunne løse hash-koden, som danner grunnlaget for Proof of Work, og sikrer validiteten til transaksjonen. Dette er en ressurskrevende konkurranse om å løse meningsløse hash-koder, og der ny forskning viser at mining av Bitcoin krever mer strøm³⁴ enn hele verdens kobber, platina og gullproduksjon (Max.J.Krause & Tolaymat, 2018). Valideringsprosessen er derfor trolig ikke bærekraftig hverken økonomisk, eller miljømessig, men som forklart tidligere er det essensielt for nettverkets kredibilitet at Proof of Work fungerer slik som det gjør.

³⁴ Fra 1. januar 2016 til 30. juni 2018 anslår rapporten at Bitcoin mining gjennomsnittlig forbrukte 17 Mega joule per genererte dollar, i motsetning til kobber, platina og gull produksjon, som til sammen brukte 16 Mega joule per genererte dollar. Mining av de 4 kryptovalutaene Bitcoin, Ethereum, Litecoin and Monero stod i denne perioden for mellom 3-15 millioner tonn CO2-utslipp.

Det høye strømforbruket vedvarer selv ved bruk av et Lightning Network, ettersom det er minerene gjennom Proof of Work som forbruker energi, ikke nodene som validerer transaksjonene. En reduksjon av transaksjoner vil derfor ikke betraktelig redusere ressursbruken i valideringsprosessen.

Lightning-teknologien er i en utprøvningsfase, der det nylig ble lansert en betaversjon for å teste teknologien sine teoretiske muligheter (Lightning Labs, 2018). Kapasiteten og antall noder, samt kanaler øker jevnt, men påliteligheten for å betjene betalinger på Lightning Network er fortsatt lav, spesielt for store transaksjoner (Diar, 2018). I betaversjonen var suksessraten for en transaksjon på \$ 2 mellom tilfeldige noder på nettverket 70%, sammenlignet med beløper over \$ 50 hvor raten kun var 10%. Jo større transaksjonen var, desto lavere sannsynlighet var det for at transaksjonen ble validert. Dette er bare noen av de mange hindrene teknologien må løse før den kan implementeres og brukes som en betalingstjeneste (Chester, 2018).

Et sentralt aspekt ved bruken av blokkjeder vil også være i hvilken grad man kan sidestille behovet for tillit. Fremfor å stole på tredjepartsaktører som banker, vil en måtte stole på den kryptografien som ligger bak teknologien, maskinvaren som kjører den og arkitekturen på nettverket. Det må derfor tas en avgjørelse om hvorvidt det å outsource tillit til teknologi er en god idé. Det kan medføre komplikasjoner og bivirkninger som man enda ikke kan forestille seg, og en må være nøye med å forstå teknologien og dens innvirkning før den tas i bruk. På samme måte som Roma ikke ble bygget på en dag, ble hoveddrammesystemene i finansielle tjenester ikke utviklet over natten. Ny finansiell infrastruktur bygget på blokkjeder vil ta tid å implementere.

Blokkjeder kan bidra til at ting blir litt mer effektivt, men jeg tror ikke vi kommer til å se noe paradigmeskift i finansbransjen som et resultat av dette.

Martin Knutli – Blockchangers

4.3 Hvordan nye markeder har åpnet seg

I løpet av intervjuprosessen ble verdien av informasjon trukket frem av tilnærmet samtlige intervjuobjekter. Informasjon har alltid vært en viktig brikke i bankenes virke, og ved å sammenstille data er det nå i langt større grad mulig å predikere fremtiden (IBM, 2012). Dette delkapittel skal analysere hvordan norske banker skal klare å holde tritt med de store teknologiske selskapene. Videre skal vi se på hvordan utradisjonelle aktører utfordrer bankenes markedsposisjon ved å tilby både billigere og mer brukervennlige produkter og tjenester i bytte mot informasjon.

4.3.1 FinTech og GAFA

Store, tradisjonsrike selskaper etablerer seg stadig i nye markeder. Et eksempel på dette er Statoil, som har gått fra å være et oljeselskap til å bli et bredt energiselskap under det nye navnet Equinor (Equinor, 2018). Regnskap- og revisjonsbransjen går fra å være en bokføringsbransje til å bli en rådgivningsbransje, og bankbransjen har gått fra å være en filialbasert bransje til å i økende grad levere og selge sine produkter og tjenester på nett (Accenture, 2018).

Enhver næring blir stadig utfordret av nye aktører. Et eksempel er Sbanken som i år 2000 kom inn i det norske bankmarkedet uten en eneste filial (Sbanken, 2018). Banken var fullstendig nettbasert, og satte i gang enorme krefter i en tradisjonell bransje. De tradisjonelle aktørene måtte hive seg rundt og imøtekomme den nye aktøren som tilbydde de samme produktene, bare gjennom nye kanaler, og til en lavere pris.

Sbanken, som med deres digitalisering av bankbransjen kan klassifiseres som en FinTech, en aktør som bruker ny teknologi for å utvikle tradisjonelle, finansielle tjenester (IBM, 2018a). Et annet eksempel er DnB-prosjektet, Vipps, som jobber for å effektivisere person til person-betalinger via en mobilapp (Vipps, 2018). De siste årene har fokuset på FinTech økt betraktelig, og det er etablert store næringsklynger som utelukkende jobber med å utvikle teknologiske løsninger innen bank og finans. Den Bergen-lokaliserte klyngen Finance Innovation er en slik aktør, som samler nye og gamle krefter for å skape fremtidens løsninger (Finance Innovation, 2018).

På den andre enden av gründerskalaen eksisterer store etablerte aktører som ser potensiale utover egen bransje. Det finnes historisk utallig eksempler på selskaper som med tiden har entret nye markeder hvor det eksisterer en økonomisk oppside (Ageras, 2018). Fellestrekket for aktørene er at de anvender sin kompetanse på nye områder. Equinor er et eksempel på et slikt selskap, som brukte sin kompetanse på fossil energi og havet, til nå å utforske muligheten til å bruke bølgekraft og vindkraft som energikilde til oljeutvinning (Hole, 2018).

Fenomenet finnes også i bank og finans, og det er spesielt noen aktører som peker seg ut – de store teknologiske selskapene. Noen av verdens største selskaper som Google, Amazon, Facebook og Apple søker å entre nye markeder (Burns & Toit, 2017). Markeder hvor det potensielt ligger mye penger, og hvor oppsiden er enorm dersom de lykkes. Ikke nødvendigvis ved å tilby finansielle tjenester, men fordi data de genererer kan gi helt nye muligheter. Google³⁵ har gått fra å være en søkemotor til å bli verdens største distributør av kart og GPS-tjenester, og Amazon³⁶ er på vei inn i transportverden med droner for å levere bøker og andre små duppeditter.

Google vet jo alt jeg gjør. De har mailen min, tilgang til mobilen min, de vet alt jeg søker på, hvor jeg er og hvem jeg er sammen med, men hvis de i tillegg kan se hva jeg handler på Rema 1000 og hvilken bil jeg har, så hadde de visst helt enormt mye mer enn de gjør i dag.

Eivind Gjenmdal – Bits

Hverken Google eller Facebook tjener penger direkte på deres kjerneprodukter (Cellan-Jones, 2018). Tjenestene er gratis og tilgjengelig for stort sett alle med internettilgang. Likevel har de blitt en av verdens største selskaper. Det selskapene tjener penger på er å selge informasjon om sine brukere, primært gjennom rettet annonsering. Google vet hva vi søker på, og kan derfor også gi oss reklame rettet mot våre interesser.

GAFAselskapene skjønner verdien av data, og jeg tror de vil gå inn i dette markedet og tilby gratis regnskapsprogrammer og likende for å få tilgang på informasjon. Den

³⁵ (Panko, 2018)

³⁶ (Shaban, 2018)

verdien de har av informasjonen er så stor at de er villig til å gi bort tjenester som i utgangspunktet koster å tilby.

Magnus Jones – EY

Når en tar en løpetur med pulsklokke, ser på TV eller sitter i trafikken, er mye av det vi eier i dag koblet til internett, ofte gjennom tjenester levert av de store teknologiske selskapene (Economist , 2017). Aktiviteten på nettet skaper digitale spor som lagres i datasiloer. Informasjonen kan prosesseres og analyseres, og gi grunnlag for å tilby varer og tjenester spesifikt rettet mot hver enkelt kunde. Jo mer data som samles om personer, desto mer treffsikre blir prediksjonene. Google har store datasiloer tilhørende hver enkelt bruker, opparbeidet over år med innsamling av søkehistorikk og kundenes bruk av deres tjenester (Curran, 2018).

Google, Amazon, Facebook og Apple, er alle på full fart inn i bank og finans (Williams-Grut, 2018). Facebook har allerede fått en bankkonsesjon i Irland, Apple har lansert Apple Pay, Amazon tilbyr mikrolån for betaling av bøker og Google har lansert Google Pay. Det er flere årsaker til at de ser på bank og finans som et attraktivt marked. Blant annet ved å dyrke det de er gode på – datainnsamling (Economist , 2017). Ved å kombinere data de allerede besitter, med informasjon om hva deres brukere faktisk kjøper, vil det kunne sette en ny standard for verdien av kundeinformasjon.

Informasjon er det nye gullet. Dette gjør at ulike aktører er ekstremt interessert i min handlekurv og mine transaksjoner, fordi det gir en enorm informasjon som kan brukes til å tilpasse bedriftenes markedsføring og produkter.

Eivind Gjerdal – Bits

Effekten av datainnsamlingen kan illustreres med et eksempel: En person som ønsker å starte et selskap har sannsynligvis både søkt på hvordan et selskap opprettes, hvordan skrive en forretningsplan og kanskje hvordan en bedrift får et lån, i Google sin søkemotor. Dersom Google i tillegg, på et lovlig vis, har tilgang til et selskaps regnskap gjennom for eksempel en gratis regnskapstjeneste, kan de bruke informasjonen til å analysere og vurdere sannsynligheten for at selskapet for eksempel vil lykkes. Når informasjonen blir satt sammen, har de potensielt bedre forutsetninger enn bankene til å beregne risikoen til et lån, og vil kunne tilby egne banktjenester skreddersydd for de enkelte kundene via rettet annonsering.

Om et selskap nærmer seg et stadium hvor de kan gå på børs vet mest sannsynlig Google dette lenge før ledelsen i selskapet selv vet det. Da kan Google kanskje vurdere om de skal investere i dette selskapet, eller for eksempel gi de et lån.

Magnus Jones – EY

Foruten økonomisk oppside er GAFA sitt inntog i bank og finans også et resultat av sterkt press fra deres største konkurrenter, ChinaTech (Greeven & Wei , 2017). ChinaTech består av selskapene Baidu, Alibaba, Tencent og Xiaomi, ofte referert til som BATX. De satser på en bredere portefølje enn GAFA-selskapene, og tilbyr tjenester og produkter innen blant annet sosiale medier, varehandel og finans.

Forretningsmodellen til BATX kan illustreres med følgende eksempel: Man ser en annonse for en jakke på Facebook, og kan enten kjøpe eller finansiere den gjennom et forbrukslån fra Facebook, og få den levert på døren neste dag. Slike tjenester eksisterer i Kina, og flere av BATX-selskapene har annonsert deres planer om å ekspandere til USA (Greeven & Wei , 2017). Dette kan være en av grunnene til at Google, Facebook, Amazon og Apple har planer om å integrere bank og finans i sine tjenester. Ved å entre nye markeder kan de få et bredere inntektsgrunnlag, og på så måte være bedre rustet til å forsvare og respondere på trusselen BATX-selskapene utgjør.

Responen på trusselen fra GAFA og BATX varierer stort blant de norske bankene. Flere av intervjuobjektene trakk ikke frem disse aktørene som store konkurrenter på kort sikt. De begrunnet dette med at det norske bankmarkedet er lite, og at GAFA-aktørene er relativt fornøyd med hvordan de selv drifter i dag.

The threat you are referring to is: what if they are becoming banks? Right now, we do not see any evidence of that happening, for all intent and purposes. Amazon are very happy with the way things work, why would they take the risk of compliance with the size of business that they have, especially with the good user experience that they have and payment integration with the solutions that they have today.

Ville Sointu – Nordea

Imidlertid kan en stille seg spørsmålet om hvorfor en profittmaksimerende suksessbedrift ikke skal entre et slikt marked, dersom de ser en økonomisk oppside. Et interessant funn i primærdata er uenighet mellom intervjuobjektene omkring hvor stor trussel GAFA-selskapene

utgjør for de norske bankene. Skillet går hovedsakelig mellom de som per dags dato er ansatt i en bank og de som ikke er det. Flere av de som er ansatt i en bank så ikke en betydelig trussel på kort sikt, i motsetning til de intervjuobjektene som ikke er ansatt i bank, som mente at bankene undervurderer trusselen.

Jeg personlig tror at norske finansinstitusjoner undervurderer trusselen fra GAFa

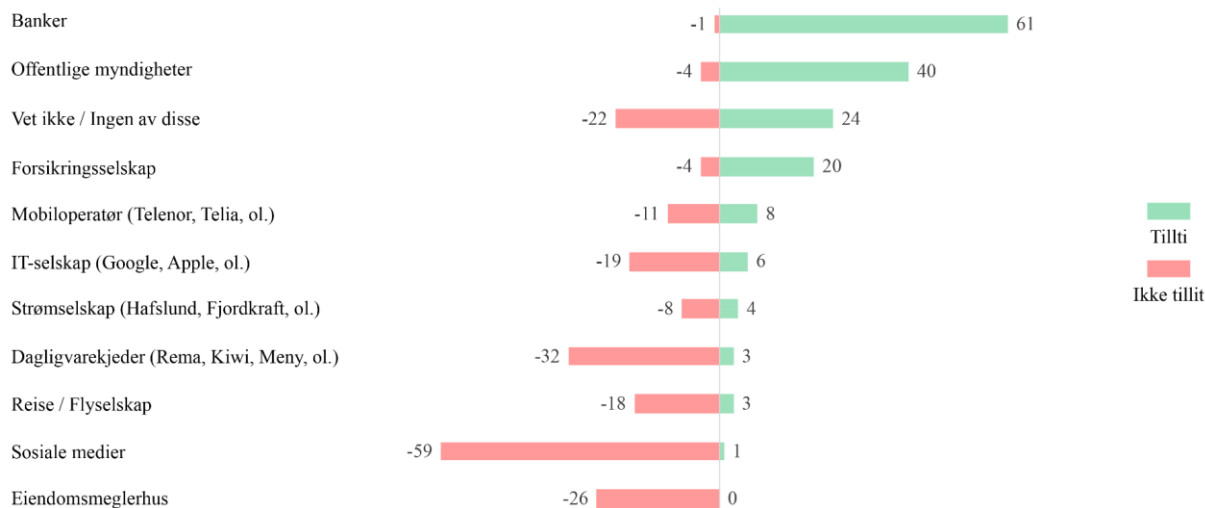
Magnus Jones³⁷ – EY

Hvorvidt GAFa utgjør en trussel på kort sikt er vanskelig å si. Likevel er de aller fleste enige om at det er en reell trussel på lang sikt. Nye tjenester fra disse leverandørene vil kunne trekke lønnsomheten ut av dagens tjenester³⁸, hvor flere av intervjuobjektene trekker frem tillit som en viktig del av forsvaret mot slike aktører. Tillit er en sentral del av bankvirksomheten – opparbeidet over flere år med tilknytning til kundene og næringslivet (EY, 2016). Mange mener også at tillit er en av suksessfaktorene til norsk næringsliv som sådan, blant annet PWC som beskriver tillit som den nye oljen (PWC, 2018b). I en undersøkelse gjort av Finans Norge om tillit til eksterne aktører i bank og finans, er det knyttet stor skepsis til at blant annet Facebook skal operere som en leverandør av finansielle tjenester (Finans Norge, 2017a). Over 2000 nordmenn ble spurt om hvilke aktører de har tillit til som leverandør av slike tjenester, og hvilke aktører de ikke har tillit til. Undersøkelsen, oppsummert i figur 8, viser at det er generell skepsis til at andre aktører enn banker og offentlige myndigheter skal håndtere transaksjons- og kontohistorikk i Norge. Spesielt skiller sosiale medier seg ut som aktører nordmenn ikke ønsker at skal håndtere slik data.

³⁷ Tidligere ansatt i Nordea

³⁸ Forklart nærmere på side 68 om aggregerte tjenester.

Hvilke aktører det er viet mest og minst tillit til som tilbyder av finansielle aggregeringstjenester



Figur 8 Figuren viser hvilke aktører nordmenn har tillit til som leverandør av aggregeringstjenester. Tallet gjengir prosent av totalen (Finans Norge, 2017a)

Jeg tror det er en generell skepsis til disse store aktørene når det gjelder penger. Penger er en form for tabu, og man er ikke interessert i å dele dette med andre. Man deler hvem man er i et forhold med og slike ting, men ikke hvor mye penger man har.

Svein Ove Langeland – Sparebanken Vest

GAFAselskapene har flere kvaliteter som gjør dem godt egnet til å entre bank og finans. Den største fordelen er at de allerede har en internasjonal kundebase på flere hundre millioner personer, i tillegg til stor finansiell- og humankapital (Statista, 2017). Likevel kan det vise seg at deres største fordel også kan være en svakhet. Hvis brukerne ikke endrer holdningene de har til GAFAs aktørene, vil trolig tilliten til at for eksempel Facebook skal håndtere kundenes monetære verdier være for lav. Nylige hendelser knyttet til både Google³⁹ og Facebook⁴⁰ sin misbruk av kundedata, og lignende skandaler, kan skape en global mistillit til aktørene som

³⁹ Tjenesten Google + hadde avslørt e-postadressen, okkupasjonen, kjønn og alder til brukerne av plattformen til 438 tredjeparts applikasjoner. (Eisele, 2018)

⁴⁰ Facebook ga informasjon om sine brukere til selskapet Cambridge Analytica. Selskapet fikk i ettertid sterk kritikk for deres bruk av personopplysninger og spredning av falske nyheter. (BBC, 2018b).

igjen kan slå hardt ut på deres banksatsing. Her kan en se paralleller til risikoen knyttet til sentraliserte aktører, diskutert i delkapittel 4.1. Sentraliserte aktører gir en høy konsentrasjon av kontroll, hvilket skaper en betydelig sikkerhetsutfordring, både menneskelig og teknologisk. Ved å ha all informasjonen lagret på et sted, er brukerne sårbare for angrep og misbruk av deres personlige data. En følge av dette er at i det øyeblikket data overlates til en sentralisert aktør, blir en avhengig av tillit til den menneskelige organisasjonen der informasjonen lagres.

På tross av det overnevnte, viser kundenes adferdstrender at når det kommer til praktiske løsninger og vaner, er de villige til å vekke ned viktigheten av tillit (Burns & Toit, 2017). En undersøkelse gjennomført av Bain & Company viser at det internasjonalt er en voksende mistillit til banksystemet. Samtidig har utradisjonelle leverandører av bank og finanstjenester, som for eksempel Apple og PayPal, opparbeidet seg en langt bedre tillitsposisjon enn de har hatt tidligere. Spesielt fant de at unge brukere verdsetter enkelhet, bekvemmelighet og personalisering i deres finansielle tjenester, som i stor grad påvirker deres valg av finansielle leverandører. Skiftet i forbrukeradferden har åpnet opp muligheten for at nye aktører kan trenge inn i den digitale lommeboken på internasjonal skala, noe som kan utgjøre en trussel mot hele den internasjonale bankbransjen.

Norske banker står i en særposisjon i kampen mot både GAFA og FinTech. Nordmenn har fortsatt høy tillit til banker, noe som er en helt sentral faktor for kundenes valg av finansiell leverandør (Finans Norge, 2017a). Med andre ord er ikke Norge nødvendigvis det landet hvor GAFA raskest klarer å etablere seg som finansinstitusjoner. Det er ikke nødvendigvis et stort problem for GAFA-selskapene at nordmenn i dag favoriserer de tradisjonelle bankene i Norge. Imidlertid kan de over tid opparbeide seg en kundebase på bakgrunn av billige og brukervennlige løsninger. På det nåværende tidspunkt har aktørene et fortrinn, ved at brukergrensesnittet som tjenestene leveres på, allerede er i bruk hos nordmenn. Blant annet er Messenger den mest nedlastede applikasjonen på norske smarttelefoner (Dinero, 2017). Ved å inkludere nye tjenester som pengeoverføringer er det ikke utenkelig at brukerne over tid vil benytte seg av disse i økende grad. Med tiden vil de nye aktørene kunne bygge opp tillitsforholdet til sine kunder, som igjen vil være essensielt når finansielle produkter skal selges i fremtiden.

Om man ser på Cambridge Analytics-skandalen så velger 200 000 nordmenn å legge inn kortinformasjonen på sin Facebook-bruker kun to dager etter for å støtte TV-

aksjonen, så convenience trumfer ofte tillit. Blir det enkelt nok så vil folk gjøre det likevel.

Svein Ove Langeland – Sparebanken Vest

Dersom GAFA og FinTech-selskaper opparbeider seg tillit i markedet på lik linje med bankene, går de en spennende tid i møte, hvor presset på norske banker trolig vil være større enn noen gang. Det vil ikke lenger bare være DNB som er den største konkurrenten til Sparebanken Vest. En bransje med tusenvis av utviklere vil kunne programmere et brukergrensesnitt som kan gjøre enhver nettbank overflødig. GAFA kan gjøre det fordi de ser verdien i to ender; verdien av data og verdien som ligger i de finansielle tjenestene. Transaksjoner kan for eksempel tilbys både nasjonalt og internasjonalt, helt gratis, fordi de ser merverdien av informasjonen. Uavhengig av om bankene på kort eller lang sikt frykter de nye aktørene, kan de ikke annet enn å ta høyde for at de utradisjonelle aktørene vil utfordre bransjen.

4.3.2 I bresjen for utvikling

Historien er full av eksempler på selskaper som har ignorert trusler i markedet. I tiden vi lever i er dette et så aktuelt tema at en kan gå seg lei av å snakke om Kodak og Nokia som begge er eksempler på internasjonale, store selskaper med vekten plassert godt på bakbeinet (Rønneberg, 2016). En av de viktigste årsakene til at selskapene til slutt endte opp med å miste sin dominerende markedsposisjon, var ikke at lønnsomheten ble drevet ut av bransjen, men at de vernet om sin egen drift i håp om at ingen skulle klare å løse det på en bedre måte.

Fremfor å ignorere truslene i markedet, kan bankene heller stå i bresjen for utviklingen i kampen mot de nye konkurrentene. Basert på informasjonen innhentet fra intervjuene, vil vi i det neste delkapitlet gå igjennom og drøfte et utvalg strategier bankene har benyttet, og benytter seg av, for å respondere på truslene.

Utvikle egen teknologi og egne løsninger

Med GAFA-selskapene på full fart inn i bankverdenen, er en av metodene bankene kan bruke i kampen mot disse aktørene er å utvikle egne løsninger og produkter som tilfredsstiller

fremtidens etterspørsel. Et slikt eksempel er DNB-prosjektet Vipps, en app som gjør person til person-betalinger langt mer brukervennlig for kundene (Vipps, 2018). Tjenesten er tilgjengelig for alle nordmenn uavhengig av hvilken bank de er kunde i. Konkurransen for vennebetalingsløsninger var stor da Vipps ble lansert i 2015. Sparebank 1 hadde sin egen vennebetalingstjeneste Mcash. Danske Bank hadde på sin side Mobile Pay, med akkurat det samme formålet. Sparebank 1 brukte over 185 millioner kroner på å utvikle Mcash, en løsning som halvannet år senere ble forkastet, da konkurransen mot Vipps var tilnærmet umulig (Rise, 2017).

DNB gikk ut av den første kampen som seierherre på grunn av noen marginale forskjeller fra de andre aktørene (Baille, 2017). Den første og sterkeste årsaken var at de var først ute med å kapre den kritiske kundemassen, på grunn av betydelige markedsføringsmidler. De hadde også trolig et marginalt bedre grensesnitt, noe som gjorde opplevelsen for brukerne litt bedre enn hos konkurrentene. Det store spørsmålet er hva som skjer med Vipps når GAFA for fullt kommer inn i vennebetalingsmarkedet. Fordelen til GAFA-selskapene er at de allerede, før de virkelig har etablert seg i bankmarkedet, har spredt brukerflaten sin ut til det norske folket. Bankene på sin side, må hver enkelt konkurrere på sine egne flater. Ingen av de norske bankene har i nærheten av så mange brukere som GAFA-aktørene. DNB har for eksempel 2,1 millioner⁴¹ personkunder i Norge, hvor 1,3 millioner av dem er aktive nettbankbrukere, sammenlignet med Facebook, som alene har omlag 2,8 millioner⁴² daglig aktive brukere.

Samarbeid mellom de etablerte bankene

En avveining mellom tillit og brukervennlighet gjøres nok av de aller fleste som benytter seg av finansielle tjenester. Det er heller ikke unaturlig å anta at tillitskravet ikke er like sterkt om det skal overføres 100 kroner til en venn, som det er å betale en ukjent person 100 000 kroner for en bruktbil. At GAFA-aktørene kan bli sentrale spillere på vennebetalingsløsninger, der behovet for tillit kan tenkes å være lavere, er sannsynlig. Eksempler ser vi allerede ved lansering av tjenester som Apple og Google Pay i Norge (Eidem, 2018). Når de norske aktørene innså at det var Vipps som gikk seirende ut av vennebetalingsduellen, ble diskusjonen

⁴¹ (DNB, 2018b)

⁴² (Ipsos, 2018)

raskt endret til hvordan norske aktører kan samarbeide om Vipps, for å styrke løsningen i kampen mot aktører som for eksempel Facebook (Sagmoen, 2017). I 2017 gikk derfor DNB, Sparebank 1, Sbanken, Eika-gruppen, Danske Bank og Nordea sammen for å utvikle et så godt produkt som mulig, noe som i dag betyr at 3 millioner⁴³ nordmenn har Vipps installert på sin telefon (Rise, 2017).

Det er stor uenighet om hvorvidt Vipps kan klare å vinne kampen mot Facebook, Apple og Google (Meland & Frøjd, 2018). Likevel er det en klar enighet om at brukervennligheten vil være den viktigste driveren i kampen om kundene. Vennebetalingsløsninger som Vipps er ikke nødvendigvis en investering for å bedre lønnsomheten til bankene, hvor Vipps i 2017 tapte over 150 millioner kroner (Proff.no, 2018). Vipps kan derimot være en viktig strategisk satsning for å opprettholde tilliten til et effektivt banksystem. Dersom Facebook klarer å etablere seg som en aktør innen vennebetalinger, vil de over tid kunne bygge opp tillit som en bank- og finansinstitusjon. Jo mer tillit de får, desto større sannsynlighet er det for at de over tid får tillit til å levere andre tjenester, som for eksempel lån. Så lenge Vipps leverer gode løsninger på produktene GAFAselskapene leverer, vil det være mer utfordrende for de nye aktørene å opparbeide seg den nødvendige tilliten (Pascual & Marchini, 2017).

Utestengelse

Apple og Google Pay har i løpet av 2018 rullet ut for fullt i Norge (Plikk, 2018). Tjenesten skal bidra til enklere person til person-betalinger, og er prinsipielt lik Vipps, hvor en bruker sitt eget bankkort til å overføre verdier via en app på telefonen. Bankenes respons på løsningene har i Norge vært lik for en stor majoritet, ved å aktivt gjøre det umulig for de respektives kunder å benytte tjenestene Apple og Google Pay, uten å bytte bank. Aktører som DNB, Eika-bankene og Danske Bank har alle valgt en slik tilnærming for å verne om sitt eget produkt, Vipps. En strategi som av flere eksperter er kritisk til, fordi bankene på lang sikt risikerer å miste tilliten fra sine kunder.

«Det jeg også tror er at DNB vil måtte skifte standpunkt når Apple Pay løsningen blir mer utbredt enten i kunde til kunde markedet (hvor Vipps er dominante i dag) eller

⁴³ (Vipps, 2018)

handelen legger forholdene til rette for bruk av Apple Pay i butikkene (hvor Vipps er svake i dag) I sum vil vi, avhengig av hvor god Apple Pay-løsningen er, kunne oppleve et DNB-kundeopprør i handlinger (skifter fra Vipps til Apple Pay) eller på sosiale medier snakke negativt om DNB (negativ vareprat), som i sum, tror jeg, tvinger DNB til å endre praksis for å ikke miste kunder eller få et vesentlig fall i merkenavn/renomme.»

Tor Wallin Andreassen – NHH (Andreassen, 2018)

Den kanskje største utfordringen med å forby og hindre nye aktører, er at brukervennligheten kundene opplever hos bankene kan svekkes. Det kan føre til at kundene enten mister tillit til sin bank over tid, som på sikt kan resultere i bytte av bank, eller at de oppretter et kundeforhold i en ny bank med det samme. Det kan være utfordrende for bankene som stenger ute nye konkurrenter, fordi deres kunder over tid kan bygge tillitsbånd til andre banker.

If you can't beat them, join them⁴⁴

Sommeren 2018 opplevde både Sbanken og Nordea en markant vekst i antall nye kunder (Plikk, 2018). De var de to eneste bankene som la til rette for bruk av Apple Pay i Norge. Tilnærmingen fremstår som fornuftig, da det er naturlig å anta at både Apple og Google vil lage de beste mobilbaserte betalingsløsningene for sine respektive mobilbrukere. At norske banker skal konkurrere om brukervennlighet på disse løsningene vil trolig i det lange løp være utfordrende. Spesielt utsatt er Vipps hvis for eksempel Apple og Google velger å stenge dem ute fra deres applikasjonsmarked. Da havner plutselig de bankene som valgte å motarbeide Apple og Google på etterskudd, sammenlignet med de som har vært samarbeidsvillige. I tillegg kan det bidra til et langsiktig samarbeid, som på sikt kan være lønnsomt og strategisk smart for begge parter. Bankene kan tilby GAFA-selskapene sine brukervennlige tjenester til sine kunder, og GAFA kan bruke den tillitsposisjonen banken har i samfunnet for å levere sine egne produkter og tjenester.

Apple controls the iPhone and can make the best user experience for our customers, and our services are available wherever our customers are. If and when Amazon is

⁴⁴Sitat hentet fra Martin Arnold i Financial Times (Arnold, Five ways banks are responding to the fintech threat, 2018b)

coming to the Nordics with a local presence, we are more than happy to work with Amazon to make sure that the Nordea instruments are available for people that are using Amazon.

Ville Sointu – Nordea

Nye kunder hos Sbanken og Nordea betyr ikke automatisk færre kunder hos de øvrige bankene, men nye kunder kan på lang sikt gjøre at tilliten til aktører som legger til rette for nye løsninger øker, sammenlignet med de som motarbeider. Dette kan igjen påvirke valget når det for eksempel skal tegnes et boliglån eller gjøres et bankinnskudd, som kan påvirke bankens fremtidige markedsposisjon.

Nye reguleringer og FinTech-selskaper

Innovasjon og gründerskap skjer stadig i bank og finans, men regulatoriske prosesser bidrar også til utvikling. PSD2 er et eksempel på en slik regulering, et europeisk direktiv som gjelder for alle EU- og EØS-land, og som skal bidra til å øke konkurransen i bank og finans (Dalsbø, 2018). Reguleringen fører til at bankene må offentliggjøre kontoopplysninger og transaksjonshistorikk om sine kunder. Nye aktører kan dermed hente ut og prosessere informasjonen, tilby nye tjenester basert på dette, og potensielt true de eksisterende, dominerende aktørene (Evry, 2018a).

Jeg tror ikke blokkjeder som vi kjenner dem i dag kommer til å endre bankbransjen fundamentalt, men sammen med reguleringer som PSD2 tror jeg vi kan se et skift i bankenes rolle for "Ola Nordmann".

Martin Knutli – Blockchangers

Den største inntjeningskilden til banker er lån (Statistisk Sentralbyrå, 2018). Ved innføringen av PSD2, er det en fare for at nye aktører kommer på banen, og at prisene i markedet kan bli presset ned mot marginalkost (Evry, 2018a). Ved å tilby tjenester som raskt og effektivt sammenlikner, og bytter til det billigste lånet, kan lønnsomheten over tid bli trukket ut av markedet.

Det bankene er redde for er at marginalkosten skal bli lik prisen, som driver all lønnsomhet ut, ved at en kontinuerlig kan bytte mellom bankene. Ved å tilby aggregattjenester, kan lån bli presentert og sammenlignet på en rettferdig måte.

Fredrik Haga – Dune Analytics

Hvorvidt lønnsomheten kommer til å drives helt ut av produkter som lån er usikkert. Finansportalen, en løsning levert av Forbrukerrådet, har i flere år sammenlignet renter på både boliglån, kredittkort og bankinnskudd (Finansportalen, 2018). Likevel er det få kunder som faktisk bytter bank, noe som fører til høye priser og god lønnsomheten i bransjen.

Når finansportalen kom og man kunne sammenligne rentene hos de ulike bankene, var det nok flere som var imot dette. Man antok at alle da kom til å bytte til det billigste, men folk gjør det fortsatt ikke. Når lånerentene har vært såpass lave som de har vært nå, så blir ikke effekten av å bytte bank stor nok for å gidde å gjøre det. Det er mange som synes det er rart at andelen som bytter bank ikke er større enn den er. Den er faktisk ikke særlig større enn hva den var før finansportalen.

Svein Ove Langeland – Sparebanken Vest

Likevel skal en ikke se bort ifra at aggregeringstjenester, som et resultat av PSD2, vil kunne dra lønnsomheten ned. Det er også signaler i markedet som tyder på at renten i Norge er på vei oppover, og det er derfor ikke unaturlig å anta at kundene i enda større grad vil være opptatt av å bli tilbudt det billigste lånet (Norges Bank, 2018a).

På en annen side bidrar PSD2 til at bankene selv får lov til å benytte en større del av data de besitter, samtidig som de får data tilgang til data fra de andre aktørene i markedet. Slike reguleringer åpner opp for helt nye muligheter i nye markeder, blant annet innenfor økonomisk rådgivning. Flere norske banker tilbyr i dag for eksempel regnskapsløsninger som kan gi ytterligere rom for rådgivning og datainnsamling. DNB Regnskap syr blant annet sammen alle DNB sine produkter som Vipps, driftskonto og lån, slik at det skal bli enkelt for bedriftskunder å følge med på sin egen økonomi (DNB, 2018a). Om bankene kan fungere som en pålitelig sparringspartner og rådgiver for sine kunder, ved å tilby digitaliserte og effektive løsninger, kan tilliten styrkes ytterligere, som igjen kan føre til at kundene velger flere produkter fra den aktuelle banken.

PSD2 spesifikt kan jo være en risiko for bankene, men også en mulighet. Spesielt i Norge hvor bankene har stor tillit hos kundene. Er man tidlig ute med å kunne gi gode analyser og tips på smartere bruk, og så videre, er dette en posisjon bankene vil ta.

Svein Ove Langeland – Sparebanken Vest

En av de store utfordringene for de norske etablerte bankene i kampen mot GAFAs, er å levere like, eller mer brukervennlige løsninger til sine kunder. Som forklart i kapittel 4.1, kan bankens kjernesystemer begrense muligheten til å integrere og utvikle nye løsninger. Det er også begrenset med kapital til å utvikle nye systemer, fordi majoriteten av investeringsmidlene er bundet opp i å holde de eksisterende systemene vedlike. Investeringer av denne typen er viktige, fordi så snart bankenes datasystem svikter vil det gå utover alle bankens kunder, noe som kan rokke ved tilliten kundene har viet til banken og deres systemer.

The second largest investment is the maintenance of the existing system, we as a financial service provider have been around for more than 100 years. There is a certain amount of technology depth that has been created during this time, so a lot of money goes into “keeping the lights on”.

Ville Sointu – Nordea

Når GAFAselskapene begynner å bevege seg inn i finanssektoren, kan det imidlertid oppmuntre FinTechs og eksisterende banker til å jobbe sammen for å bekjempe en felles trussel. En slik trussel kan være nøyaktig hva sektoren trenger for å fremme samarbeidende innovasjon. Begrenset av de store kostnadene og kompleksiteten rundt sitt banksystem, kan det være lettere å kjøpe opp små konkurrenter enn det er å endre den eksisterende infrastrukturen. I prosessen kan også bankene, til en viss grad, gardere seg mot risiko ved å plukke ut selskaper som har et etterprøvd system. Dersom all teknologisk utvikling skulle skjedd internt, ville det vært en risiko for at en stor del av utviklingskostnadene hadde gått med på mislykkede prosjekter.

Trenden ser en allerede i det norske markedet, hvor tall fra Fintech Disruptors Report 2017, viser at 74 % av bankene i Norden vil i løpet av 2017 innlede et samarbeid med, eller gjøre oppkjøp av FinTech-selskaper (Fintech Mundi, 2017). Trenden ser vi også blant våre intervjuobjekter, hvor både Nordea og DNB trakk frem samarbeidsavtaler og selskaper de nylig hadde kjøpt opp.

Jeg blir overrasket om det ikke er noen småselskaper innen FinTech som kommer til å lage løsninger vi kommer til å kjøpe eller bruke. Akkurat som at vi kjøper regnskapssystem, så kommer vi til å kjøpe systemer av andre aktører i fremtiden. Noe annet synes jeg blir rart å se for seg. Vi har ikke noe ønske om å utvikle all teknologi selv. Vi har bestemt oss for at om noen andre er gode på noe, så lar vi heller de utvikle dette enn å holde på med det selv, da går ting mye fortere. Selv om vi må endre litt for å få de til å passe inn hos oss selv, så er det bedre å gjøre dette med et produkt som er 80% fra perfekt, enn å starte på null.

Lasse Meholm – DNB

Oppkjøps- og samarbeidsstrategien bekreftes også i en rapport gjort av Accenture, som konkluderer med at store banker bør se på FinTech-selskapene som venner, ikke konkurrenter (Accenture, 2015). I rapporten oppfordrer Accenture bankene til å strategisk integrere FinTech-aktører inn i deres eksisterende systemer og infrastruktur. Samarbeid vil resultere i banker som er bedre rustet for å konkurrere i den stadig utviklende finansbransjen. Bankene oppfordres i samme rapport til å søke miljøer for nyskaping, en oppfordring bankene har tatt på alvor. Finance Innovation er en norsk FinTech-klynge, som høsten 2018 fikk klassifiseringen som et nasjonalt kompetansesenter, som alle de største norske bankene er en del av (Øyvann, 2018). Ved å være en del av disse miljøene sørger bankene for at de henger med i utviklingen.

Det finnes alltid et nytt marked

I en verden som endrer seg raskere enn noen gang, kan en mulig forsvarsstrategi være å utvide satsningsområdet. En slik tilnærming er det flere eksempler på, og en trenger ikke å gå lengre enn å se på bankenes største utfordrer. Samtlige GAFAselskaper er opprinnelig teknologiselskaper som har valgt å se utover sin kjernevirksomhet, og inn i bank og finans. En mulig forsvarsstrategi for de norske bankene mot GAFAselskaper og FinTech-selskapene, kan derfor være å se nye veier, og etablere seg i nye markeder.

Satsninger på nye områder kan bidra til å gjøre bankene økonomisk bærekraftige, og redusere risikoen for at nye aktører skal ta over hele inntektsgrunnlaget. Problemstillingen ble dratt frem av flere intervjuobjekter, og er en av de strategiene som i størst grad kan benytte seg av mulighetene blokkjedeteknologi skaper.

In terms of DLT and Blockchain we have already taken some solutions into production, as mentioned earlier, and we are looking into turning that into profitability soon, so we have created a technology that acutely did not exist before. By using blockchain technology we have managed to get SME⁴⁵ trading down to a point where it becomes viable service for our customers, in a way we could not do before. Here in lays the opportunities of blockchain, finding these areas where we get immediate new business instead of trying to replace something that already exist.

Ville Sointu – Nordea

Bankbransjen tilbyr forskjellige forsikringsløsninger til sine kliner og kunder (Bytt.no, 2018). Av Frode Bjuglerud, fagdirektør for økonomisk kriminalitet i Finans Norge, forklares forsikring som et gjensidig tillitsforhold mellom kunde og selskap (FinansNorge, 2018a). Det legges til grunn at kunden oppgir korrekte og ærlige opplysninger både ved kjøp av forsikring, og ved skadeoppgjør. Undersøkelser og svindelrapporter gjort av Finanstilsynet viser imidlertid at ikke alle kunder fremstår ærlige. I 2018 ble det avdekket forsikringssvindel for 428 millioner kroner i Norge (FinansNorge, 2018a).

I likhet med mange andre bransjer, er det i forsikringsbransjen et godt teoretisk grunnlag for at blokkjeder kan effektivisere forsikringsbransjen. Hvert enkelt produkt kan for eksempel registreres på en blokkjede, og forsikringsselskapene vil da kunne ha kontroll på at den samme klokken ikke meldes som stjålet samtidig som den overleveres til noen andre. En stjålet klokke vil heller ikke ha en gyldig kobling tilbake til forrige blokk, som blant annet kan bidra til å redusere tjuvgods-markedet.

Utfordringen til blokkjeder i forsikringsbransjen, som resten av finansverdenen, er at blokkjeden ikke garanterer at informasjonen som puttes på er riktig. Behovet for verifisert informasjon gjør at bank- og finansbransjen er strengt regulert, noe som gjør utvikling av nye systemer og teknologi vanskelig.

⁴⁵ En tjeneste utviklet av Nordea på we.trade plattformen, les mer om prosjektet her: <https://financefeeds.com/nordea-reports-first-trades-blockchain-based-platform/>

Kan jo nevne hvor vi og hele markedet står. Fordi på systemsiden er vi styrt veldig mye av regulatoriske forhold. Ekstrem kompleks lovgivning, gjør det svært krevende å utvikle moderne brukervennlige løsninger innenfor forsikring.

Rune Smådal – IF

Blokkjeder har, gjennom mekanismene forklart i kapittel 3, muligheten til å pålitelig registrere forskjellige typer tidsbestemt data, inkludert trinnene som kreves for å utføre prosessen kjent som smartkontrakter. En smartkontrakt kan for eksempel sende en betaling til en leverandør så snart en forsendelse er levert (Buterin, 2015). Et firma kan signalisere at et bestemt objekt har blitt mottatt, som i sin tur utløser en gjensidig anerkjent betinget betaling. En viktig egenskap ved smartkontrakter, er at de ikke krever en pålitelig tredjepart mellom aktørene. Blokkjedenettverket håndhever utførelsen av kontrakten alene, noe som potensielt kan redusere friksjon i overføring av verdi mellom enheter, og åpner opp for mer automatiserte prosesser (Ethereum, 2018a). Ved å bruke blokkjedeteknologi på nye måter, kan mange av de eksisterende prosessene i forsikringsbransjen potensielt effektiviseres. Et eksempel er EY og Maersk sitt samarbeid om forsikring av lasten på skip ved hjelp av blokkjedeteknologi, som kan være med på å redusere noe av risikoen og kostnadene i forsikringsbransjen.

For eksempel, om de mistet en container, så kunne det ta opp til to og et halvt år å få betalt ut erstatning for innholdet i denne containeren. Med systemet vi utviklet i EY, som er basert på smartkontrakt i et program som heter EY Ops Chain⁴⁶, som er en veldig enkel sporingsmekanisme basert på blokkjeder, så kuttet vi behandlingstiden ned til tre dager. Så om Maersk mister en container nå så tar det bare tre dager å utbetale erstatning. Og ja, det er sikkert mye feil, og det kan være kvalitetsendringer, men litt av det som er positivt med blokkjede er at man før ulykken skjer må melde inn hva containeren inneholder.

Bjørn Bjercke – Bitgate

Fremfor å endre den eksisterende teknologiske infrastrukturen hos bankene, kan blokkjeder bidra til å åpne opp, og utvikle helt nye tjenester som kan bidra til en mer diversifisert produktportefølje. Her ligger trolig, på kort sikt, blokkjedebaserte tjenester sin største

⁴⁶ EY Ops Chain er plattform som privat og sikkert gjør det mulig for bedrifter å lage og selger produkter på en åpen blokkjedeteknologi (Sankaran, 2018).

mulighet. Teknologien vil mest sannsynlig ikke fjerne dagens system, men åpne opp for nye muligheter ved å implementere den i nye finansielle løsninger. På så måte kan banker spre sitt inntektsgrunnlag, og bedre sikre seg mot endringer i markedet fra nye aktører og reguleringer.

5. Oppsummering og konklusjon

Gjennom en kvalitativ analyse med dybdeintervjuer og et litterærssøk på emnet, ønsket vi å besvare hvordan banker tilpasser seg de endringene som kommer når blokkjedeteknologi og nye aktører truer norske bankers markedsposisjon.

Blokkjedens potensiale til å redusere behovet for tredjepartsaktører og effektivisere komplekse og krevende prosesser i bank- og finanssektoren har gjort teknologien til en verdensomspennende idé. Teknologiens evne til trygt og effektivt spore eierskapet til alle finansielle handlinger, ved at all intervensjon lagres kryptografisk sikret på en distribuert kjede, gjør at behovet for tillit til mellommenn kan reduseres. Oppgaven trekker frem teknologiens potensial til å korte ned transaksjonstiden på internasjonale transaksjoner, samt gjøre autentiseringsprosesser mer brukervennlige og effektive.

Permissionless-blokkjeder har, som de fleste andre teknologier, noen grunnleggende utfordringer. Den sikre oppbygningen gjør teknologien ressurskrevende, og tilnærmet umulig å implementere i storskala. Blokkjedeteknologi sitt grunnleggende mål om å umuliggjøre endring av informasjon som allerede ligger på kjeden, hjelper lite dersom informasjonen som blir puttet på blokkjeden ikke er autentisk.

Permissioned-blokkjeder og Distributed Ledger Technology bygger på prinsippene til åpen blokkjedeteknologi, men løser noen av de overnevnte problemene ved å nedprioritere den desentraliserte strukturen. Slike lukkede løsninger krever på sin side en helt annen form for koordinering mellom aktørene, om teknologien skal kunne implementeres i bankenes daglige drift. Det hjelper lite for DNB om de har utviklet en egen løsning, dersom systemet ikke kan samarbeide med andre systemer og aktører i markedet. Ulike konsortium har av den grunn utviklet seg, hvor Hyperledger og R3 Corda er to prosjekter som trekkes frem. Samarbeid mellom banker over hele verden, primært med hensikt om å dele kostnader og sikre en bredere forankring i systemets struktur. Det er imidlertid flere utfordringer, blant annet at hver enkel bank er avhengig av at nye systemer må integreres med deres eksisterende infrastruktur, hvor det ofte eksisterer divergerende interesser mellom aktørene. Det er av bankene og konsortiene utarbeidet ulike strategier for å løse problemene, men per dags dato er det ingen som er like effektive som de sentraliserte databasene og systemene styrt av pålitelige mellommenn.

Aktørene i bank og finans har vært proaktive på å finne alternative løsninger til de iboende problemene dagens system har, blant annet ved økt fokus på å levere bedre og raskere tjenester.

Blant annet har det dominerende systemet for internasjonale overføringer, SWIFT, utviklet ny teknologi for å effektivisere sin egen infrastruktur, som fører til lavere kostnader for både bankene og deres kunder.

Flere av intervjuobjektene trakk frem at blokkjedeteknologi sitt viktigste bidrag til banknæringen, er at det omsider har samlet lederne rundt bordet. Ikke bare for å diskutere blokkjeders påvirkning på bransjen, men også for å legge planer og strategier for fremtidens banker, i et mer komplekst marked. I tiden som kommer vil presset fra nye aktører være større enn noen gang, med utradisjonelle aktører som Google, Apple, Facebook og Amazon på full fart inn i bank og finans. Aktørene kan true de norske bankene ved å tilby brukervennlige og billige banktjenester, gjennom plattformer hvor de allerede er dominerende.

Norske banker sin respons på trusselen fra de nye aktørene varierer i stor grad fra bank til bank. Der Nordea og Sbanken velger å tilgjengeliggjøre Google og Apple Pay i sine produkter, velger DNB å aktivt stenge dem ute fra sine tjenester, for å dyrke sin egen løsning, Vipps. Til gjengjeld er Vipps et resultat av en offensiv strategi. DNB tok føringen i vennebetalingsmarkedet, og dominerer markedet foran løsningene til Facebook, Apple og Google. Hovedårsaken er at Vipps i dag er en fellesplattform for samtlige norske banker, et samarbeid som har vært en helt avgjørende strategi for å lykkes. På tross av Vipps sin klare dominans i Norge og norske bankers dominerende posisjon i det norske bankmarkedet for øvrig, er trusselen fra GAFA reell. Flere av intervjuobjektene mener de norske bankene undervurderer de utradisjonelle aktørene, hvor faren for at kunder går til konkurrerende bedrifter, blir stadig større jo lengere tid bankene bruker på å etterfylle fremtidens kundekrav.

Bankene må utarbeide en klar strategi om å kapitalisere på den nye epoken, med ny teknologi og nye konkurrenter som truer deres markedsposisjon. Det krever omstilling, nytenkning og utvikling av nye digitale tjenester ved prioritering av intern IT-utvikling, og oppkjøp av selskaper som besitter den kompetanse de trenger for å utvikle nye løsninger. Norske banker har en fordel ved at de allerede besitter store mengder data om sine kunder. Data de kan bruke for å skreddersy produkter og tjenester på lik linje som GAFA-selskapene, som ikke bare samsvarer med kundenes eksisterende behov, men også forutse deres fremtidige behov. Ved å utvikle bedre tjenester, vil bankene ikke bare redusere kostnader og øke brukervennligheten, men også styrke tillitsforholdet til sine kunder – et bærende element i deres forretningsmodell, og et forhold som er helt essensielt når kundene skal velge leverandør av finansielle tjenester.

Bibliografi

- Accenture. (2015). *The Future of Fintech and Banking*. Accenture.
- Accenture. (2016). *Blockchain Technology: How Banks Are Building a Real-Time Global Payment Network*. Accenture .
- Accenture. (2018). *Accenture Banking Beyond North Star Gazing*. Retrieved Oktober 16, 2018, from www.accenture.com:
https://www.accenture.com/t20181009T020501Z__w__/no-en/_acnmedia/PDF-85/Accenture-Banking-Beyond-North-Star-Gazing.pdf#zoom=50
- Ageras. (2018, November 3). *Ekspansjonsstrategier*. Retrieved from <https://www.ageras.no/blog/ekspansjonsstrategier-er-du-klar-til-aa-erobre-nye-markeder>
- Andreassen, T. W. (2018, Juni 21). *Dnb velger feil strategi*. Retrieved from [dagensperspektiv.no](https://www.dagensperspektiv.no): <https://www.dagensperspektiv.no/2018/dnb-velger-feil-strategi>
- Arnold, M. (2018a, Mars 4). *Swift says blockchain not ready for mainstream use*. Retrieved from www.ft.com: <https://www.ft.com/content/966f5694-22c6-11e8-ae48-60d3531b7d11>
- Arnold, M. (2018b, November 12). *Five ways banks are responding to the fintech threat*. Retrieved from www.ft.com: https://www.ft.com/content/d0ab6b84-c183-11e8-84cd-9e601db069b8?fbclid=IwAR0X9SJcCS7jBEDDFI6WfC9c3fzna25lxHXEG2Oi0BW1ZoWs4xR3_hfdGfM
- Back, A. (2018, Juni 11). *Blockchain bitcoin problems limitations issues weaknesses*. Retrieved from blockchainreview.io: <https://blockchainreview.io/blockchain-bitcoin-problems-limitations-issues-weaknesses/>
- Baille, S. (2017, Februar 14). *Derfor måtte vipps vinne*. Retrieved from www.e24.no:
<https://e24.no/kommentarer/bank/kommentar-derfor-maatte-vipps-vinne-enn-saa-lenge/23924403>
- Balakrishnan, A. (2017, November 1). *News*. Retrieved from www.cnn.com:
<https://www.cnn.com/2017/10/31/facebook-senate-testimony-doubling-security-group-to-20000-in-2018.html>
- BankID. (2018a, November 30). *Om oss - Tjenester*. Retrieved from <https://www.bankid.no/om-oss/tjenester/>
- BankID. (2018b, Desember 6). *Hvordan sikrer banken at BankID utstedes til rett person*. Retrieved from www.bankid.no: <https://www.bankid.no/privat/los-mitt-bankid-problem/ofte-stilte-sporsmal/?fbclid=IwAR0D0595Q6SpskTDEvWDNM2V0nBzLOpX2C5wqwwMjBJ4RXDjTdjJa90zCdk>
- BankID. (2018c, Desember 8). *Privat*. Retrieved from <https://www.bankid.no/privat/>

- BankID. (2018d, Desember 7). *BankId AML*. Retrieved from www.bankid.no:
<https://www.bankid.no/bedrift/bankid-aml/>
- Barth, J. R., Caprio, G., & Levine, R. J. (2013). *Bank Regulation and Supervision in 180 Countries from 1999 to 2011* .
- BBC. (2018a, November 26). *bitesize*. Retrieved from www.bbc.com:
<https://www.bbc.com/bitesize/articles/z8yk87h>
- BBC. (2018b, November 25). *Facebook cambridge analytica data breach*. Retrieved from
https://www.bbc.com/news/business-46334810?intlink_from_url=https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-data-breach&link_location=live-reporting-story
- Befring, E. (2015). *Forskningsmetoder i utdanningsvitenskap*. Oslo: Cappelen Damm Akademisk.
- Bernhardsen, E., & Larsen, K. (2002). Bankenes prising av risiko ved utlån til foretakssektoren. *Penger og Kreditt* 4/2002, 185-195. Retrieved from
<https://brage.bibsys.no/xmlui/bitstream/handle/11250/2503332/bernhardsen.pdf?sequence=1>
- BitInfoCharts. (2018, November 26). *Bitcoin transactionfees*. Retrieved from
bitinfocharts.com: <https://bitinfocharts.com/comparison/bitcoin-transactionfees.html>
- Bits. (2018a, November 3). *Om bits*. Retrieved from <https://www.bits.no/om-bits/>
- Bits. (2018b, November 27). *betalinger med raskere oppgjør* . Retrieved from
<https://www.bits.no/project/betalinger-med-raskere-oppgjor-bro/>
- Blockgeeks. (2018, November 28). *proof of work vs proof of stake*. Retrieved from
www.blockgeeks.com: <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>
- Britannica. (2018, November 28). *Financial Crisis of 2008*. Retrieved from
<https://www.britannica.com>: <https://www.britannica.com/topic/Financial-Crisis-of-2008-The-1484264>
- Brown, R. G. (2013, November 24). *Thoughts on the future of finance*. Retrieved from
www.gendal.me: <https://gendal.me/2013/11/24/a-simple-explanation-of-how-money-moves-around-the-banking-system/>
- Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). *Corda: An Introduction*.
- Browne, R. (2017, Desember 17). *big transactions fees are a problem for bitcoin*. Retrieved from
www.cnb.com: <https://www.cnb.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html>
- Burns, M., & Toit, G. d. (2017). *Evolving the Customer Experience in Banking*. Bain and Company .
- Businessdictionary. (2018, November 12). *white paper*. Retrieved from
www.businessdictionary.com: <http://www.businessdictionary.com/definition/white-paper.html>

-
- Buterin, V. (2015). *A next generation smart contract & decentralized application platform*. Ethereum (ETH).
- Bytt.no. (2018, Desember 10). *Liste over norske forsikringsselskaper*. Retrieved from www.bytt.no: <https://www.bytt.no/forsikring/liste-over-norske-forsikringsselskaper>
- Callahan, J. (2018, Juli 10). *Forbes Tech Council*. Retrieved from www.forbes.com: <https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#7729c0e38dbb>
- Castelles, M. (2013). *Open Mind*. Retrieved Oktober 13, 2018, from www.bbvaopenmind.com: https://www.bbvaopenmind.com/en/articles/the-impact-of-the-internet-on-society-a-global-perspective/?utm_source=views&utm_medium=article07&utm_content=Internet-society&fbclid=IwAR3nR9shV1rTsN18pEcXaJCCRaml9tulRqFglEyEy_kt2KhJT48ItAoVcKc
- Cecchetti, S., & Schoenholtz, K. (2018, August 28). *Article*. Retrieved from voxeu.org: <https://voxeu.org/article/finance-and-blockchains>
- Cellan-Jones, R. (2018, November 18). *Guide*. Retrieved from www.bbc.com: <http://www.bbc.co.uk/guides/z9x6bk7>
- Chester, J. (2018, Juni 18). *Your guide on the lightning network the opportunities and the issues*. Retrieved from www.forbes.com: <https://www.forbes.com/sites/jonathanchester/2018/06/18/your-guide-on-the-lightning-network-the-opportunities-and-the-issues/#38047e563677>
- Cisco. (2018, Desember 5). *What is a Firewall*. Retrieved from <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- Creswell, J. W. (2014). *Research Design. Qualitative, Quantitative and Mixed Methods Approaches Fourth ed*. Lincoln: Sage Publications.
- Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches. Research design 4th edition*. Los Angeles: Calif: SAGE.
- Curran, D. (2018, Mars 30). *The data facebook google has on you privacy*. Retrieved from www.theguardian.com: <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>
- Dalsbø, V. K. (2018, Januar 3). *Hva vil psd2 bety for deg*. Retrieved from www.dnbnyheter.no: <https://www.dnbnyheter.no/privatokonomi/hva-vil-psd2-bety-for-deg/>
- Datatilsynet. (2017, Oktober 20). *Rettigheter og plikter*. Retrieved from <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonsikkerhet/sterk-autentisering/>
- Datatilsynet. (2018, November 8). *Personvern på ulike områder*. Retrieved from <https://www.datatilsynet.no/personvern-pa-ulike-omrader/kundehandtering-handel-og-medlemskap/kredittvurdering/>

- Diar. (2018, Juni 5). *volume-2-issue-25*. Retrieved from <https://diar.co/volume-2-issue-25/>
- Digranes, J. (2017, Januar 24). *Finans Norge*. Retrieved from www.finansnorge.no:
<https://www.finansnorge.no/globalassets/presentasjoner/2017/forsikringskonferansen---digitalisering-og-cybersikkerhet.pdf>
- Dinero. (2017, November 30). *Facebook messenger betaling tilgjengelig i norge*. Retrieved from www.dinero.no: <https://dinero.no/facebook-messenger-betaling-tilgjengelig-i-norge/>
- DNB. (2018a, November 22). *Regnskap*. Retrieved from <https://www.dnb.no/regnskap>
- DNB. (2018b, September 30). *Om DNB*. Retrieved from <https://www.dnb.no/om-oss/om-dnb.html>
- Economist . (2017, Mai 6). *The worlds most valuable resource is no longer oil but data*. Retrieved from <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>
- Edwards, I. (2018, Juni 14). *Investment in blockchain*. Retrieved from [bitsonline](http://bitsonline.com):
<https://bitsonline.com/investment-in-blockchain-by-financial-services-industry-grew-strongly-in-2017/>
- Eidem, M. (2018, November 8). *Teknologi* . Retrieved from www.dn.no:
<https://www.dn.no/teknologi/teknologi/mobilbetaling/google-pay/apple-og-google-vil-at-du-skal-betale-med-mobilen-men-nordmenn-tviholder-pa-plastkortene-sine/2-1-464693>
- Eisele, J. (2018, Oktober 18). *DealBook Briefing: Google's Turn for a Data Scandal*. Retrieved from www.nytimes.com:
<https://www.nytimes.com/2018/10/09/business/dealbook/google-data-scandal.html>
- Ekroll, H. C. (2018, September 19). *Økonomi*. Retrieved from www.aftenposten.no:
<https://www.aftenposten.no/okonomi/i/VR8pe4/Danske-Bank-toppsjef-trekker-seg-for-presentasjon-av-hvitvasking-gransking>
- Equinor. (2018, Mai 22). *News*. Retrieved from www.equinor.com:
<https://www.equinor.com/no/news/archive/2008/05/22/hywindfullscale.html>
- Eriksen, N. (2018, Januar 1). *Nyheter*. Retrieved from www.dagbladet.no:
<https://www.dagbladet.no/nyheter/nigeriansk-prins-var-hvit-amerikaner-67/69227770>
- Ethereum. (2018a, Desember 9). *greeter*. Retrieved from <https://www.ethereum.org/greeter>
- Ethereum. (2018b, Desember 10). *About*. Retrieved from www.ethereum.org:
<https://www.ethereum.org/>
- Evry. (2018a, November 18). *Psd2 the directive that will change banking as we know it*. Retrieved from www.evry.com: <https://www.evry.com/no/media/artikler/psd2-the-directive-that-will-change-banking-as-we-know-it/>
- Evry. (2018b, Desember 1). *Evry*. Retrieved from www.evry.com:
<https://www.evry.com/no/bransjer-og-tjenester/bransjer/financialservices/sikkerhet/autentisering/>

-
- EY. (2016). *Industries*. Retrieved Desember 2018, from <https://www.ey.com/gl/en/industries/financial-services/banking---capital-markets/ey-trust-without-it-youre-just-another-bank>
- Faridi, O. (2017, Juli 23). *What is proof of work*. Retrieved from www.cryptocompare.com: <https://www.cryptocompare.com/mining/guides/what-is-proof-of-work/>
- Finance Innovation. (2018, November 18). *About*. Retrieved from <https://www.financeinnovation.no/about/>
- Finans Norge. (2017a, April 26). *liten tillit til sosiale medier*. Retrieved from www.finansnorge.no: https://www.finansnorge.no/aktuelt/sporreundersokelser/forbruker-og-finanstrender/forbruker--og-finanstrender-2017/liten-tillit-til-a-la-sosiale-medier-utfore-betalingstjenester/?fbclid=IwAR0XEpR8Nm_mInsOmAo2ZUIxxfRI54Rj2pJ70qF0UuHJkrL6uPID8Gc__cg
- Finans Norge. (2017b, Februar 16). *Konsesjon*. Retrieved from <https://www.finanstilsynet.no/konsesjon/banker/?header=Konsesjon%20for%20%C3%A5%20drive%20bankvirksomhet%20i%20Norge>
- Finans Norge. (2018b, Oktober 15). *Hvitvasking og Terrorfinansiering*. Retrieved from <https://www.finansnorge.no/tema/hvitvasking-og-terrorfinansiering/hvitvaskingslovens-krav-om-kundetiltak-og-kyc-prinsippet/>
- FinansNorge. (2018a). *Svindelrypport 2018*. FinansNorge. Retrieved from <https://www.finansnorge.no/siteassets/statistikk/forsikringssvindel-i-norge---svikstatistikk-2018-2017-tall.pdf>
- Finansportalen. (2018, November 22). *om finansportalen*. Retrieved from <https://www.finansportalen.no/andre-valg/om-finansportalen/>
- Finanstilsynet. (2008, April 11). *Nyhetsarkiv*. Retrieved from <https://www.finanstilsynet.no/nyhetsarkiv/pressemeldinger/2008/tilbakekall-av-glitnir-privatokonomi-as-tillatelser-til-a-yte-investeringstjenester/>
- Finanstilsynet. (2016, Mai 26). *Forbrukerinformasjon*. Retrieved from <https://www.finanstilsynet.no/forbrukerinformasjon/bank-og-finans/>
- Fintech Mundi. (2017). *Fintech Disruptors Report 2017 – Nordic Edition*. FintechMundi.
- Fox, J. (2016, April 29). *Amazon and facebook are big spenders*. Retrieved from www.bloomberg.com: https://www.bloomberg.com/opinion/articles/2016-04-29/amazon-and-facebook-are-big-spenders-on-r-d?fbclid=IwAR3W9wbZoS88T5KhbkAUvTUYQXZU2bZr_h7d4xw035D0LCGa1sL3StmGjyE
- Goldman Sachs. (2018, November 2). *The new technology of trust*. Retrieved from www.goldmansachs.com: <https://www.goldmansachs.com/insights/pages/blockchain/>

-
- Greeven, M., & Wei, W. (2017, Oktober 17). *New technology giants*. Retrieved from [www.telegraph.co.uk: https://www.telegraph.co.uk/news/world/china-watch/technology/new-technology-giants/](https://www.telegraph.co.uk/news/world/china-watch/technology/new-technology-giants/)
- Gupta, M. (2018). *Blockchain for dummies 2nd IBM Limited Edition*. John Wiley & Sons, Inc.
- Hackett, R. (2017, Mars 23). *Apple iphone hacker ransom*. Retrieved from [www.fortune.com: http://fortune.com/2017/03/22/apple-iphone-hacker-ransom/](http://fortune.com/2017/03/22/apple-iphone-hacker-ransom/)
- Harber, S., & Stornetta, S. w. (1991). *How to timestamp a digital documnet*. Bellcore: Journal of Cryptology, Vol. 3, No. 2, pp. 99-111, .
- Havemann, J. (2018, Oktober 9). *Financial Crisis of 2008*. Retrieved from [britannica.com: https://www.britannica.com/topic/Financial-Crisis-of-2008-The-1484264#](https://www.britannica.com/topic/Financial-Crisis-of-2008-The-1484264#)
- Hidas, P. (2016, September 20). *Computerworld*. Retrieved from [www.cw.no: http://www.cw.no/artikkel/peters-plass/sikker-som-banken](http://www.cw.no/artikkel/peters-plass/sikker-som-banken)
- Hoggson, N. F. (2007). *Banking through the ages*. New York: Cosimo Classics.
- Hole, S.-E. (2018, August 28). *Artikler*. Retrieved from Teknisk Ukeblad: <https://www.tu.no/artikler/equinor-lanserer-en-av-sine-viktigste-fornybarsatsnimmer-noensinne/444670>
- Holm, J., & Frøystad, P. (2015). *Whitepaper Blockchain: Powering the Internet of Value*. Evry.
- Holm-Nilsen, S., & Mjaaland, O. (2018, September 20). *De kriminelle har alltid overtaket*. Retrieved from [www.nrk.no: https://www.nrk.no/norge/hackerangrep-mot-bedrifter-oker_-_de-kriminelle-har-alltid-overtaket-1.14214930](https://www.nrk.no/norge/hackerangrep-mot-bedrifter-oker_-_de-kriminelle-har-alltid-overtaket-1.14214930)
- Hosseini, S. B., & Dr. Mahesh, R. (2016, August 31). The Lesson From Enron Case - Moral And Managerial Responsibilities. *International Journal of Current Research*, pp. 37451-37460.
- Hvitvaskingsloven. (2018, Oktober 15). Retrieved from <https://lovdata.no/dokument/NL/lov/2018-06-01-23?q=hvitvaskingsloven>
- Hyperledger. (2018a, November 10). *About*. Retrieved from <https://www.hyperledger.org/about>
- Hyperledger. (2018b, Desember 3). *hyperledger-fabric*. Retrieved from [www.hyperledger-fabric.com: https://hyperledger-fabric.readthedocs.io/en/release-1.3/whatis.html](https://hyperledger-fabric.readthedocs.io/en/release-1.3/whatis.html)
- IBM. (2012). *Analytics: The real-world use of big data*. New York: IBM Institute for Business Value.
- IBM. (2018a, November 15). *fintech banking industry disruptor*. Retrieved from <https://www.ibm.com/think/fintech/fintech-banking-industry-disruptor/>
- IBM. (2018b, Desember 8). *Hyperlegder*. Retrieved from <https://www.ibm.com/blockchain/se-sv/hyperledger.html>

-
- Iotw. (2018, Oktober 11). *About*. Retrieved from www.iotw.io: <https://iotw.io/>
- Ipsos. (2018, Oktober 22). *Ipsos SoMe-tracker Q3'18*. Retrieved from <https://www.ipsos.com/nb-no/ipsos-some-tracker-q318>
- Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser*. Oslo: Høyskoleforlaget.
- Kunz, J. H., & Schirmer, M. (2015, September). *Key elements of the 4th EU Anti-Money Laundering Directive*. Retrieved November 5, 2018, from www.financierworldwide.com: <https://www.financierworldwide.com/key-elements-of-the-4th-eu-anti-money-laundering-directive/#.XA-6mxNKhTa>
- Lakhani, K. R., & Iansiti, M. (2017, Januar 23). *The truth about blockchain*. Retrieved from hbr.org: <https://hbr.org/2017/01/the-truth-about-blockchain>
- Lazanis, R. (2015, Januar 19). *How technology behind bitcoin could transform accounting as we know it*. Retrieved from techvibes.com: <https://techvibes.com/2015/01/22/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22>
- Leite, E. (2015, Januar 19). *Why trust matters in business*. Retrieved from Weforum.org: <https://www.weforum.org/agenda/2015/01/why-trust-matters-in-business/>
- Lightning Labs. (2018, Desember 4). *lightning.engineering*. Retrieved from <https://lightning.engineering/index.html#faq>
- Lightning Network. (2016, Januar 14). *lightning network paper*. Retrieved from lightning.network: <https://lightning.network/lightning-network-paper.pdf>
- Lov om kredittvurderingsbyrå. (2016, November 25). *Lov om kredittvurderingsbyrå*. Retrieved from lovdata.no: <https://lovdata.no/dokument/NL/lov/2014-06-20-30>
- Marcopolo. (2018, November 27). *About*. Retrieved from <https://www.marcopolo.finance/>
- Margaritoff, M. (2018, Juli 2). *The scalability trilemma*. Retrieved from www.jeffersoncapital.info: <https://www.jeffersoncapital.info/the-scalability-trilemma/>
- Marr, B. (2016, Mai 27). *How blockchain technology could change the world*. Retrieved from www.forbes.com: <https://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#27497929725b>
- Max.J.Krause, & Tolaymat, T. (2018). *Quantification of energy and carbon costs for mining cryptocurrencies*. NATURE SUSTAINABILITY.
- McKinsey. (2016, Mai). *how blockchains could change the world*. Retrieved September 12, 2018, from www.mckinsey.com: <https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world>
- McKinsey. (2018). *Digital*. Retrieved November 1, 2018, from www.mckinsey.com: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>
- Meland, H., & Frøjd, K. (2018, Januar 27). *Ekspert tror Facebook vil overta for Vipps*. Retrieved from www.Tv2.no: <https://www.tv2.no/a/9639248/>

-
- Menon Economics . (2017). *En internasjonal sammenligning av finansiell teknologi*. Menon-publikasjon nr. 40.
- Nakamoto, S. (2008, Oktober 31). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from bitcoin.org: <https://bitcoin.org/bitcoin.pdf>
- Nordea. (2018, Desember 2). *Om oss*. Retrieved from <https://www.nordea.no/om-nordea/om-nordea/juridisk-informasjon/hvorfor-stiller-vi-sporsmal.html>
- Norges Bank. (2009). *Kostnader i betalingssystemet*. Oslo: Norges Bank. Retrieved September 13, 2018, from https://www.norges-bank.no/contentassets/6de3f88488924a34a278d4c36a6bdef8/kostnader_i_betalingssystemet.pdf
- Norges Bank. (2014). *Kostnader i det norske betalingssystemet Memo Nr. 5*. Oslo: Norges Bank. Retrieved November 3, 2018, from static.norges-bank.no: https://static.norges-bank.no/contentassets/c6ed2ec861034f47afb5ea233363a5d3/norges_bank_memo_5_2014.pdf?v=03/09/2017123516&ft=.pdf
- Norges Bank. (2018a, November 22). *Styringsrenten*. Retrieved from <https://www.norges-bank.no/pengepolitikk/Styringsrenten/>
- Norges Bank. (2018b). *contentassets*. Retrieved from norgesbank.no: https://static.norges-bank.no/contentassets/d8039ff2c8a9438c9400132c46c241e1/nfs_2018.pdf?v=09/24/2018121310&ft=.pdf
- Norsk senter for informasjonssikring. (2014, September 30). *svindel ser ut som det er fra bankid*. Retrieved from norsis.no: <https://norsis.no/svindeler-ser-ut-som-det-er-fra-bankid/>
- NOU. (2011, Mai 27). Lov om finansforetak og finanskonsern, 2011: 8 Bind B. *Ny finanslovgivning*. Norges offentlige utredninger.
- Olsen , T., Ford, F., Ott, J., & Zeng, J. (2017). *Blockchain in Financial Markets: How to Gain an Edge*. Bain and company.
- Olsen, Ø. (2014, Juni 3). *Norges Bank*. Retrieved from www.norges-bank.no: <https://www.norges-bank.no/Publisert/Foredrag-og-taler/2014/3-juni-Oystein-Olsen-Kulturhistorisk-museum/>
- Olsen, Ø. (2018, November 30). *Norges Banke*. Retrieved from www.norges-bank.no: <https://www.norges-bank.no/Publisert/Foredrag-og-taler/2018/2018-09-25-cme/>
- Panko, R. (2018, Juni 10). *Google maps*. Retrieved from www.themanifest.com: <https://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018>
- Pascual, A., & Marchini, K. (2017). *Trust in Banking*. Pleasanton: Javelin.
- Perloth, N. (2017, Oktober 3). *Technology*. Retrieved from www.nytimes.com: <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>
- Plikk, N. (2018, August 29). *Nå får flere tilgang til apple pay*. Retrieved from www.tek.no: <https://www.tek.no/artikler/na-far-flere-tilgang-til-apple-pay/444759>

-
- Pokrandt, H. (2018, Juli 6). *Blockchian mining*. Retrieved from www.forbes.com:
<https://www.forbes.com/sites/forbestechcouncil/2018/07/06/blockchain-mining-the-key-to-powering-a-decentralized-world/#66149b415a11>
- Proff.no. (2018, November 22). *Finans*. Retrieved from www.proff.no:
<https://www.proff.no/selskap/vbb-as/oslo/finans/IF6Z85N0RSY/>
- Psalia, S. (2017, September 22). *Blockchain a game changer for audit*. Retrieved from www.deloitte.com: <https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html>
- PWC. (2018a, November 7). *hvorfor regulering og kapitalkrav*. Retrieved from <https://www.pwc.no/no/bransjer/bank-og-finans/finreg-skolen/grunnleggende-om-finreg/hvorfor-regulering-og-kapitalkrav-mv.html>
- PWC. (2018b, November 18). *den nye oljen* . Retrieved from <https://www.pwc.no/no/pwc-aktuelt/tillit---den-nye-oljen.html>
- PWC. (2018c). *Blockchain is here. What's your next move?* Retrieved Oktober 3, 2018, from pwc.no: <https://www.pwc.com/blockchainsurvey>
- R3. (2018, November 27). *About*. Retrieved from <https://www.r3.com/about/>
- Rawson, P. (2017). *Blockchain: The New Internet? How You Can Benefit from Blockchain Technology Beyond Bitcoin, Cryptocurrency, and Ethereum* . CreateSpace Independent Publishing Platform.
- Regjeringen. (2014, Juni 27). *Økonomi og budsjett*. Retrieved from www.regjeringen.no:
<https://www.regjeringen.no/no/tema/okonomi-og-budsjett/finansmarkedene/lover-innen-bank-finans-selskapsrett-mv/id434565/>
- Regnskapsloven. (1999, Januar 1). Retrieved from <https://lovdata.no/dokument/NL/lov/1998-07-17-56>
- Rise, K. V. (2017, Jun1 27). *185 millioner på å bygge en klar nummer to*. Retrieved from <https://www.dn.no/marked/mobilbetaling/mcash/vipps/sparebankene-svidde-av-185-mill-pa-a-bygge-en-klar-nummer-to/2-1-112450>
- Røise, M. B. (2016, Desember 13). *Evry har fått mye kritikk*. Retrieved from www.digi.no:
<https://www.digi.no/artikler/evry-har-tidligere-fatt-mye-kritikk-for-sine-eldgamle-banksystemer-na-er-de-pa-rett-vei-med-enda-en-storkontrakt/366200>
- Rønneberg, K. (2016, September 15). *Derfor overlevde IBM og ikke Nokia og Kodak*. Retrieved from www.aftenposten.no:
<https://www.aftenposten.no/okonomi/i/A5gPx/Derfor-overlevde-IBM--og-ikke-Nokia-og-Kodak>
- Sagmoen, I. (2017, November 8). *Digital*. Retrieved from <https://e24.no/digital/vipps/to-nye-banker-paa-vipps-laget-ruster-seg-mot-internasjonale-giganter/24181918>
- Sankaran, A. (2018, Oktober 30). *Ethereum public blockchain*. Retrieved from www.ey.com: https://www.ey.com/en_gl/news/2018/10/ey-launches-the-world-s-first-secure-private-transactions-over-the-ethereu-public-blockchain

-
- Santander Consumer Bank. (2018, Mars 21). *Santander Consumer Bank*. Retrieved from Magasinet : <https://www.santanderconsumer.no/magasinet/ferie-og-fritid/garpassord-fella/>
- Saunders, M. N. (2015). *Research Methods for Business Students*. Pearson Education Limited.
- Saunders, M. N., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students 7th edition*. Harlow: Pearson.
- Sbanken. (2018, November 18). *Historie*. Retrieved from www.sbanken.no: <https://sbanken.no/om-oss/om-sbanken/historie/>
- Seth, S. (2017, September 12). *How swift system works*. Retrieved from www.investopedia.com: <https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp?>
- Shaban, H. (2018, Mars 22). *The switch*. Retrieved from www.washingtonpost.com: https://www.washingtonpost.com/news/the-switch/wp/2018/03/22/amazon-issued-patent-for-delivery-drones-that-can-react-to-screaming-flailing-arms/?utm_term=.f70dd05122d4
- Sharma, R. (2017, Oktober 22). *Does blockchains popularity mean end swift*. Retrieved from [investopedia](http://investopedia.com): <https://www.investopedia.com/news/does-blockchains-popularity-mean-end-swift/>
- Singh, M. (2018, Oktober 9). *Financial crisis review*. Retrieved from www.investopedia.com: <https://www.investopedia.com/articles/economics/09/financial-crisis-review.asp>
- Sinrod, M. L. (2018, Mars 9). *World Economic Forum*. Retrieved from www.weforum.org: <https://www.weforum.org/agenda/2018/03/blockchain-bitcoin-explainer-shiller-roubini>
- SNL. (2018, Februar 20). *Store Norske Leksikon*. Retrieved from snl.no: <https://snl.no/hype>
- Sparebankforeningen. (2018, Desember 1). *Sparebankforeningen*. Retrieved from www.sparebankforeningen.no: <https://www.sparebankforeningen.no/banker-og-stiftelser/antall-sparebanker/>
- Statens innkrevingsentral. (2012, Mars 2). *Ordforklaringer*. Retrieved from www.sismo.no: <https://www.sismo.no/no/pub/ordforklaringer/realregister>
- Statista. (2017). *Google, Apple, Facebook, and Amazon (GAFa)*. Statista.
- Statista. (2018, November). *Statista*. Retrieved November 5, 2018, from www.statista.com: <https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/>
- Statistisk Sentralbyrå. (2018, September 27). *Godt resultat for bankene*. Retrieved from www.ssb.no: <https://www.ssb.no/bank-og-finansmarked/artikler-og-publikasjoner/godt-resultat-for-bankene--363898?fbclid=IwAR3InoD2AyqJXeNBD3yIngUUbPr-vO8wceg0DzZpE4hzCWPZWPImBBak6p8>

-
- Stigsen, A. (2017, Juli 14). *who owns your business data*. Retrieved from [www.forbes.com: https://www.forbes.com/sites/forbestechcouncil/2017/07/14/who-owns-your-business-data/?fbclid=IwAR0QpQMusjHh8DM031SherKgh5P1EsdcPAoSD36zYAOIE8M5-VBiV6pGcYE#45869e519750](https://www.forbes.com/sites/forbestechcouncil/2017/07/14/who-owns-your-business-data/?fbclid=IwAR0QpQMusjHh8DM031SherKgh5P1EsdcPAoSD36zYAOIE8M5-VBiV6pGcYE#45869e519750)
- SVEA. (2017, November 29). *Derfor tar det sa lang tid før pengene er på konto*. Retrieved from [www.svea.com: https://www.svea.com/no/nb/bedrift/svea-innsikt/tips-og-rad/derfor-tar-det-sa-lang-tid-for-pengene-er-pa-konto/](https://www.svea.com/no/nb/bedrift/svea-innsikt/tips-og-rad/derfor-tar-det-sa-lang-tid-for-pengene-er-pa-konto/)
- Swanson, T. (2018, Desember 7). *Blockchain key challenges*. Retrieved from [www.deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf](https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf)
- SWIFT. (2018a). *Swift gpi*. Retrieved Oktober 5, 2018, from <https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi>
- SWIFT. (2018b, November 14). *about us*. Retrieved from <https://www.swift.com/about-us>
- Szabo, N. (1996). *fon.hum.uva*. Retrieved Desember 3, 2018, from <http://www.fon.hum.uva.nl>: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
- Tapscott, A., & Tapscott, D. (2018). *Blockchian Revolution*. Greate Britan: Penguin Random House.
- Thake, M. (2018, Feburar 8). *whats the difference between blockchain and dlt*. Retrieved from [medium.com: https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd](https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd)
- The World Bank . (2018). *Remittance Prices Worldwide*. The world bank.
- Thirani, V., & Gupta, A. (2017, September 22). *The value of data*. Retrieved from Agenda - 2017: <https://www.weforum.org/agenda/2017/09/the-value-of-data/>
- Ticoll, D., & Tapscott, D. (2012). *The Naked Corporation: How the Age of Transparency Will Revolutionize Business* . Free Press.
- Timberg, C., Dwoskin, E., & Fung, B. (2017, September 7). *Equifax hack hits credit histories of up to 143 million americans*. Retrieved from Business - Technology: https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html?noredirect=on&utm_term=.ac634ccc534a
- Tomaino, N. (2018, mai 23). *The scalability of blockchains*. Retrieved from [medium.com: https://thecontrol.co/on-the-scalability-of-blockchains-ec76ed769405](https://thecontrol.co/on-the-scalability-of-blockchains-ec76ed769405)
- U.S. Department of the Treasury. (2006). *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act*.

- Vipps. (2018, November 22). *Om oss*. Retrieved from Vipps.no: <https://www.vipps.no/om-oss>
- Waupsh, J. (2016). *Bankruption: How Community Banking Can Survive Fintech*. New Jersey: John Wiley & Sons, Inc.
- Williams-Grut, O. (2018, Januar 13). *will facebook and amazone get into finance*. Retrieved from [www.nordic.businessinsider.com](https://nordic.businessinsider.com/open-banking-will-facebook-google-and-amazon-get-into-finance-2018-1?r=UK&IR=T): <https://nordic.businessinsider.com/open-banking-will-facebook-google-and-amazon-get-into-finance-2018-1?r=UK&IR=T>
- World Justice Project. (2018, Desember 2). *Rule of Law Index*. Retrieved from <http://data.worldjusticeproject.org/>
- Worldbank. (2018, April 12). *blockchain dlt*. Retrieved from <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt>
- Øyvann, S. (2018, November 9). *Forfremmet pa rekordtid*. Retrieved from [www.computerworld.com](http://www.cw.no/artikkel/fintech/forfremmet-pa-rekordtid): <http://www.cw.no/artikkel/fintech/forfremmet-pa-rekordtid>

Apendiks A - Intervjuforespørsel

Master innen Økonomi og Administrasjon, Norges Handelshøyskole

Emne: Blokkjedeteknologi og dens påvirkning på finansmarkedene

Vi ønsker i oppgaven å analysere hvordan blokkjedeteknologi, og annen ny teknologi, kan endre det finansielle markedet og aktørene som operer i det. Hvordan må norske aktører endre seg og tilpasse seg disse endringene, eller legger norske aktører premissene for utviklingen er sentrale spørsmål ønsker å se nærmere på. Vi ønsker å basere analysen på intervjuer med relevante personer i norsk og internasjonalt næringsliv, inviterer derfor deg til et intervju for å diskutere følgende emner:

- Hvordan ditt selskap ser muligheter og utfordringer i ny teknologi?
- Hva er nye teknologiske satsningsområder for selskapet?
- Hvordan vil ny teknologi endre ditt selskap og selskapets markedsposisjon?
- Påvirker blokkjedeteknologi den fremtidige utviklingen for ditt selskap, og i så tilfelle hvordan og hvorfor?

Intervjuer kan gjøres ansikt til ansikt, via Skype, telefon eller andre ønsker som måtte passe best for deg. Intervjuet vil vare mellom 30-45 minutter.

Vi vil ta notater under intervjuet, men vi ønsker om du godkjenner det å ta opptak slik at sitering kan foregå på en presis måte. Vi ønsker også å sitere deg med navn. Alle sitater vil bli sendt deg på forhånd for din godkjenning før vi leverer inn endelig versjon av vår utredning. Dersom du ønsker kan vi sitere deg anonymt. Etter at prosjektet er ferdig vil alle personlig data bli slettet (etter forskrifter fra NSD). Det er også mulig å korrigere eller fjerne sitater frem til ferdigstilling av prosjektet, senest 13 desember 2018.

Vi håper du kan bistå oss med dette prosjektet og vi vil sette stor pris på din deltagelse. Dersom du har spørsmål eller innspill så hadde det vært veldig hyggelig om du tar kontakt via telefon eller mail. Vi ser frem til å snakke med deg.

Med vennlig hilsen,

Nicolai Herman Grann Greve

Telefon:

Mail:

Eilev Haukaas

Telefon:

Mail:

Studien er meldt inn til behandling for personopplysninger, Norsk senter for Forskningsdata (NSD)

Apendiks B - Intervjuguide

Master innen Økonomi og Administrasjon, Norges Handelshøyskole

Emne: Blokkjedeteknologi og dens påvirkning på finansmarkedene

DEL 1

Introduksjon

Formål:

- Takke kandidat for deltagelse i intervjuet og presentere oss
- Informasjon om masteroppgave og tema, informere om opptak
- Informere om tiltenkt lengde og behandling av personlig informasjon
- Informere om at intervjuet kan avsluttes når som helst, og at kandidaten ikke trenger å besvare på alle spørsmål

Bakgrunn til kandidat

Formål: Få oversikt over personen/selskapet og deres innstilling til ny teknologi, slik at de kan inndeles i en av sektorene

- Hvilken stilling innehar intervjuobjektet og hvilken rolle har personen i selskapet
- Hvor stor andel av investeringer i selskapet går i ny teknologi, og i hvilke områder er dette?
 - o AI-teknologi
 - o Generell automatisering
 - o Blokkjedeteknologi
 - o Hvordan ser dette ut om 5, 10 og 20 år?
 - Er det noe helt nytt på gang?
- Hva er din kjennskap til/om blokkjedeteknologi?
- Hvordan stiller ditt selskap seg til blokkjedeteknologi i den finansielle sektoren?
 - o Utvikler dere?
 - o Adapterer dere?
 - o Lar dere være?
- Vet du om noen av deres konkurrenter har adaptert blokkjedeteknologi nå, eller kommer til å gjøre dette i fremtiden?
 - o Selskapets respons på dette?

DEL 2

Formål: *Få personen til å forklare endringene som har skjedd og kommer til å skje innen deres bransje*

- Hvilke deler av virksomheten er under sterkest teknologisk utviklingspress?
 - o Er det andre finansinstitusjoner, eller helt nye aktører som er hovedkonkurrenten?
 - o Hvilket selskap er deres største konkurrent på et 5 – 10 – 20 års perspektiv?
- Hva gjør ditt selskap for å imøtekomme de teknologiske endringene som kommer?
 - o Hva er hovedutfordringen?
 - o Hva er mulighetene?
- Har ditt selskap noen form for komparativt fortrinn i utviklingen av ny teknologi – både nasjonalt og internasjonalt?
 - o Norske selskaper er små sammenlignet med store giganter – er det en fordel?

Del 3

Formål: *Finn ut hvilken av de implementerte teknologiene som kan bli/blir truet av blokkjedeteknologi.*

- Kan du nevne tre av de største og nyeste teknologiprojektene i ditt selskap?
- Ser du for deg at noen av disse teknologiene kan utfordres av blokkjedeteknologi?
 - o Hvorfor / hvorfor ikke?
 - o Hva kan blokkjedeteknologi gjøre bedre?
- Har dere generell tro på blokkjedeteknologi?
 - o Eventuelt når tror du den blir en sentral del av virksomheten?
 - o Hva tror du er de største fordelene blokkjede teknologi vil ha på finansverden?
 - o De største utfordringene teknologien vil møte?

Del 4

Formål: *Kartlegge om det er andre elementer som er relevante for oppgaven*

- Hvilke aktører er bankenes største trussel på kort og lang sikt?
 - o Vil reguleringer spille en sentral rolle?
 - o Kommer GAFA til å utgjøre en trussel for bankene?
- Har du noen tanker om annet relevant informasjon som kan brukes i oppgaven?

Apendiks C - Intervjulist

Master innen Økonomi og Administrasjon, Norges Handelshøyskole

Emne: Blokkjedeteknologi og dens påvirkning på finansmarkedene

Navn	Selskap	Tittel	Format og lengde
Lasse Meholm	DNB	Head of Blockchain & DLT Strategy	Telefon 40 minutter
Ville Sointu	Nordea	Head of Emerging Technologies	Skype 45 minutter
Bjørn Bjercke	BitGate	Chief Executive Officer	Google Hangouts 75 minutter
Svein Ove Langeland	Sparebanken Vest	Head of Strategy	Fysisk møte 50 minutter
Torbjørn Bull Jensen	Arcane Crypto	Chief Executive Officer	Google Hangouts 75 minutter
Magnus Jones	EY	Tax Technologist	Telefon 40 minutter
Fredrik Haga	Dune Analytics	Co-Founder & Chief Executive Officer	Fysisk møte 55 minutter
Thomas Tjøstheim	Sbanken	Concept & business developer	Fysisk møte 45 minutter
Martin Knutli	Blockchangers	Blockchain adviser & business developer	Fysisk møte 60 minutter
Rune Smådal	IF P&C Insurance	Head of Product Norway	Fysisk møte 40 minutter
Eivind Gjerdal	Bits	Chief Executive Officer	Telefon 45 minutter

Merknad: Alle sitater er godkjent av de respektive intervjuobjektene. Det gjøres oppmerksom på at utsagnene er personlige og ikke nødvendigvis en del av selskapets strategi eller holdning.

