



# Norsk digital valuta

*Innføring av digitale sentralbankpenger basert på  
desentralisert teknologi*

**Ørjan Borge og Andriy Morgal**

**Veileder: Malin Arve**

Masterutredning i Økonomisk Analyse

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

I denne oppgaven undersøker vi hvorvidt desentralisert teknologi kan tas i bruk for å øke effektiviteten i det norske betalingssystemet. Vi ser på hvordan ulike konsensusmekanismer kan benyttes i en blokkjede til å utføre betalinger raskere, sikrere og til lavere kostnader.

De eksisterende desentraliserte kryptovalutaene har utfordringer knyttet til prosesseringskapasitet og høye kostnader, som gjør teknologien lite egnet for digitale sentralbankpenger. Til tross for at kostnaden i liten grad overføres til forbrukerne er den samfunnsøkonomiske kostnaden per transaksjon langt høyere enn i det eksisterende betalingssystemet.

Vi presenterer implikasjoner digitale sentralbankpenger vil ha for sentralbankens likviditetsstyring og beskriver en modell for hvordan digitale sentralbankpenger kan utformes med tilpasninger i den desentraliserte teknologien. Ved å begrense verifisering av transaksjoner til kjente finansielle utvinnere kan kostnadene reduseres og skalerbarheten forbedres.

## Forord

Denne masteroppgaven markerer slutten på vår siviløkonomutdanning ved Norges Handelshøyskole. Masteroppgaven er skrevet innenfor masterprofilen: «økonomisk analyse».

Arbeidet med oppgaven har vært svært spennende. Digitale sentralbankpenger er et nytt tema hvor det først den siste tiden er publisert rapporter som gir en første innføring i konseptet. De fleste spørsmålene knyttet til digitale sentralbankpenger er fremdeles uavklarte. At det eksisterer lite litteratur å støtte seg til har gjort vår problemstilling meget interessant å arbeide med, men også desto mer krevende. Vi antar at flere rapporter og flere internasjonale erfaringer vil bli publisert i årene som kommer. Denne utviklingen blir svært spennende å følge videre da det kan ha en stor påvirkning på hver enkelt i samfunnet, men også for Norges Bank og hvordan pengepolitikken i Norge kan styres.

Vi vil benytte anledningen til å rette en stor takk til vår veileder Malin Arve. Hun har vært konstruktiv i sine tilbakemeldinger, vært tilgjengelig for spørsmål til enhver tid og gitt svært raske tilbakemeldinger på alle problemer vi har opplevd i dette løpet.

Vi vil også minne om at masteroppgaven er et selvstendig arbeid og at det er forfatterne av oppgaven som holdes ansvarlig for de konklusjonene som er trukket, de valgene som er foretatt og de beregningene som er utført.

Bergen, Juni 2018

---

Ørjan Borge

---

Andriy Morgal

## Innhold

<b>1.</b>	<b>INNLEDNING .....</b>	<b>6</b>
<b>2.</b>	<b>PENGER.....</b>	<b>7</b>
2.1	ET HISTORISK TILBAKEBLIKK .....	7
2.2	HVA ER PENGER?.....	8
2.3	KONTANTER.....	8
2.3.1	<i>Kontantbruk i Norge</i> .....	9
2.3.2	<i>Beredskap og sikkerhet</i> .....	12
2.3.3	<i>Svart økonomi</i> .....	13
2.4	KONTOPENGER.....	14
2.5	ELEKTRONISKE PENGER .....	15
2.6	VIRTUELL VALUTA .....	16
2.7	SENTRALBANKENS ANSVAR .....	17
2.7.1	<i>Tillit og troverdighet</i> .....	17
2.7.2	<i>Sentralbankens likviditetsstyring</i> .....	18
2.7.3	<i>Betalingssystemet</i> .....	20
<b>3.</b>	<b>ET EFFEKTIVT BETALINGSSYSTEM .....</b>	<b>22</b>
3.1	DIGITALE FERDIGHETER .....	22
3.2	OPPTAK AV NYE BETALINGSLØSNINGER .....	22
3.3	TRANSAKSJONER MELLOM BANKER .....	23
3.4	CYBERKRIMINALITET .....	24
<b>4.</b>	<b>DESENTRALISERT TEKNOLOGI .....</b>	<b>25</b>
4.1	BLOKKJEDE.....	25
4.2	KONSENSUS.....	26
4.2.1	<i>Proof-of-Work</i> .....	26
4.2.2	<i>Proof-of-Stake</i> .....	27
4.3	TRANSAKSJONER.....	27
4.4	SMART CONTRACTS.....	28
4.5	DIGITALE LOMMEBØKER .....	28
<b>5.</b>	<b>IMPLIKASJONER AV DESENTRALISERT TEKNOLOGI.....</b>	<b>30</b>
5.1	ANONYMITET .....	30
5.1.1	<i>Etterspørsel etter anonymitet</i> .....	30
5.1.2	<i>Utfordringer ved anonymitet</i> .....	31
5.2	SKALERBARHET .....	31
5.2.1	<i>Transaksjonsvolum</i> .....	32
5.2.2	<i>Verifiseringskostnader</i> .....	33
5.3	KOSTNADER .....	34
5.3.1	<i>Bedriftenes kostnader</i> .....	34
5.3.2	<i>Bankenes kostnader</i> .....	35
5.3.3	<i>Brukernes transaksjonskostnader</i> .....	36
5.3.4	<i>Samfunnets transaksjonskostnader</i> .....	38
5.4	VOLATILITET.....	38
5.4.1	<i>Pengenes egenskaper</i> .....	39
5.4.2	<i>Tilbud</i> .....	40
5.5	SIKKERHET.....	40
5.5.1	<i>Tradisjonell infrastruktur</i> .....	41
5.5.2	<i>Desentralisert infrastruktur</i> .....	41
5.5.3	<i>Verdioppbevaring</i> .....	42
<b>6.</b>	<b>UTFORMING AV NORSK DIGITAL VALUTA .....</b>	<b>44</b>
6.1	SENTRALBANKENS OPPGAVER.....	44
6.1.1	<i>Likviditetsstyring ved innføring av digitale sentralbankpenger</i> .....	45
6.2	TEKNOLOGISK UTFORMING .....	48
6.2.1	<i>Verifisering</i> .....	48
6.2.2	<i>Struktur</i> .....	50
6.2.3	<i>Sikkerhet og anonymitet</i> .....	51
6.3	SLUTTKOMMENTARER.....	52
<b>7.</b>	<b>KONKLUSJON .....</b>	<b>53</b>
<b>8.</b>	<b>BIBLIOGRAFI .....</b>	<b>55</b>

---

## Figuroversikt

Figur 2.3.1-1. Verdi av kontanter i omløp og som prosentdel av verdien av betalingsmiddel (M1).....	10
Figur 2.3.1-2. Verdien av kontantbruk i Norge.....	11
Figur 2.7.2-1. Utvalgte poster i en forenklet oppstilling av sentralbankens balanse .....	19
Figur 4.1-1. Hashing i blokkjeden.....	25
Figur 5.2.2-1. Verifiseringskostnad per transaksjon .....	33
Figur 5.3.3-1. Gjennomsnittlig gebyr per transaksjon.....	37
Figur 6.1.1-1. Utvalgte poster i en forenklet oppstilling av sentralbankens balanse (inkludert ny post for digitale sentralbankpenger) .....	46
Figur 6.2.2-1. Verifiseringsprotokoll for digitale sentralbankpenger .....	50

# 1. Innledning

Flere land, inkludert Norge, har satt i gang forskningsgrupper for å utrede mulighetene til å utstede egne digitale sentralbankpenger. Endringer i hvordan vi gjennomfører betalinger og en økt interesse for teknologiske utviklinger, åpner opp for helt nye spørsmål om hvordan fremtidens betalingsmetoder og betalingssystemer kan se ut.

Det er først og fremst det siste året at det har dukket opp artikler som omtaler digitale sentralbankpenger i de norske avisene. Dette i kjølvannet av den store interessen som har vokst frem rundt kryptovalutaer. Norges Bank sin første rapport om digitale sentralbankpenger ble publisert 18.mai 2018 med formål om å spre kunnskap og informasjon om emnet.

Tilgjengelige rapporter som presenterer digitale sentralbankpenger gir lite oppmerksomhet til digitale sentralbankpenger basert på desentralisert teknologi. Målet med oppgaven er å gi en innsikt i hvordan desentralisert teknologi kan benyttes i utformingen av digitale sentralbankpenger.

Vi vil referere til rapporten som nylig ble publisert av Norges Bank om digitale sentralbankpenger i løpet av oppgaven for å gi leseren et innblikk i hvorvidt slutningene som trekkes i denne oppgaven samsvarer med slutningene som er trukket av Norges Bank.

Oppgaven er strukturert på følgende måte: Del 2 vil kartlegge hva penger er og hvilke betalingsinstrument som allerede eksisterer i våre dager. Vi vil også beskrive sentralbankens likviditetsstyring. Del 3 vil redegjøre for utfordringer i betalingssystemet og hva den påvirkes av. Del 4 vil beskrive desentralisert teknologi før vi i del 5 tar for oss implikasjonene ved teknologien. Til slutt, i del 6, vil vi benytte teknologien som er vurdert i de foregående delene for å gi en anbefaling til hvordan digitale sentralbankpenger basert på desentralisert teknologi kan utformes.

## 2. Penger

I oppgavens første del vil vi ta for oss hva penger er og hvilke metoder vi kan benytte for å utføre betalinger i våre dager. Da digitale sentralbankpenger vil bli enda en betalingsmetode som kan benyttes, er det nødvendig å kartlegge de ulike betalingsmetodene som eksisterer og se på fordelene og ulempene ved disse. Videre kan digitale sentralbankpenger påvirke sentralbankens likviditetsstyring og det norske betalingssystemet. Vi vil avslutningsvis i denne delen ta for oss hvordan disse systemene fungerer i dag.

### 2.1 Et historisk tilbakeblikk

Penger har historisk sett vært ulike «gjenstander med en form for egenverdi» (Holden, 2004, s.1). Dette har vært eiendeler som hadde en bruksverdi (kyr, kameler, salt, osv.), eller andre gjenstander det var begrenset tilgang til (sølv, gull, osv.). Dette var et lite effektivt økonomisk system, både på grunn av at pengemengden var knyttet opp mot tilgangen til de ulike gjenstandene, men også at byttehandler med store verdier var vanskelig å håndtere og inkluderte høye transaksjonskostnader.

Effektiviteten i pengesystemet økte, da konger etterhvert utstedte egne pengemynter. Dette førte derimot til hyperinflasjon og at pengene falt i verdi, da kongene stadig utstedte mer penger for å finansiere egne behov eller utstedte pengemynter med høyere grad av uedle metaller (Olsen, 2014). Det var fremdeles upraktisk å frakte store verdier, som førte til utfordringer knyttet til de store transaksjonene.

Etterhvert kunne mennesker plassere myntene sine i private banker i bytte mot pengesedler. I Skandinavia var pengesedlene garantert av metaller som gull og sølv og kunne benyttes til handel (Nicolaisen, 2017). Dette førte til at det ble mer praktisk å håndtere handel med store verdier. Videre ble transaksjonskostnadene lavere, da det ble lettere å frakte verdier over lengre avstander (European Central Bank, 2012).

Da det ikke var restriksjoner på utlån av pengesedler, oppstod det problemer når verdien av utlånene ble høyere enn verdien av metaller banken satt på. Dette førte til at tilliten til pengesedlene forsvant og mange ønsket å innløse sedlene sine. Sveriges første bankkrise kom på bakgrunn av at banken ikke hadde nok metaller til å dekke etterspørselen når tilliten til pengesedlene forsvant (Nicolaisen, 2017). Sveriges bankkrise oppstod i årene 1664 til

1665 og førte til etableringen av den svenske sentralbanken i år 1668 (Sveriges Riksbank, 2009).

Gjennom et kort historisk tilbakeblikk på penger, ser vi at viktige motivasjoner bak historiske endringer i pengepolitikken har vært effektivitet og reduksjon av transaksjonskostnader. I våre tider er ikke pengenes verdi knyttet til edle metaller. Penger har verdi, ene og alene, på grunn av tillit og fordi vi tror på pengenes verdi (Nicolaisen, 2017).

## 2.2 Hva er penger?

Penger er definert som et alminnelig godttatt betalingsmiddel, som innebærer at penger kan benyttes til å kjøpe varer og tjenester, tilbakebetale lån, samt til kjøp av verdipapirer som aksjer og obligasjoner (Norges Bank, 2014).

Penger fungerer som et standardisert mål for verdi, som fører til at varer og tjenester kan verdsettes og at verdien av ulike produkter og tjenester kan sammenlignes. Penger har derfor en sentral rolle når handler skal gjøres opp.

For at mennesker skal ta imot penger som betaling, må penger kunne benyttes som betalingsmiddel i fremtiden; vi må stole på at pengenes verdi holder seg over tid. En noenlunde stabil pengeverdi gir dermed frihet til å velge når bruken av pengene skal skje (Olsen, 2014).

Penger oppfyller dermed tre grunnleggende oppgaver: (1) et byttemiddel, (2) et verdimål og (3) et verdioppbevaringsmiddel.

## 2.3 Kontanter

I Norge er norske sedler og mynter tvungne betalingsmidler (Sentralbankloven, 1985, § 14). Finansavtaleloven (2000, § 38-3) slår fast at «en forbruker alltid har rett til å foreta oppgjør med tvungne betalingsmidler hos betalingsmottakeren». Sentralbankloven oppstiller likevel noen begrensninger i loven, som omhandler ødelagte sedler og mynter og antallet ulike valører man kan benytte når man betaler (Sentralbankloven, 1985, § 14). Loven synes likevel



å være absolutt; både betaler og betalingsmottaker har rett til å kreve betaling i sedler og mynter.

Begrepet «kontanter» vil heretter benyttes i oppgaven som en betegnelse på «sedler og mynter» utstedt av Norges Bank.

Det er Norges Bank som har enerett til å utstede kontanter i Norge. Sentralbankloven skal fremme et effektivt samlet betalingssystem (Norges Bank, 2014). Det innebærer at Norges Bank skal sikre at det er *tilstrekkelig* med kontanter i omløp<sup>1</sup>, slik at den økonomiske aktiviteten ikke begrenses (Holden, 2004).

### **2.3.1 Kontantbruk i Norge**

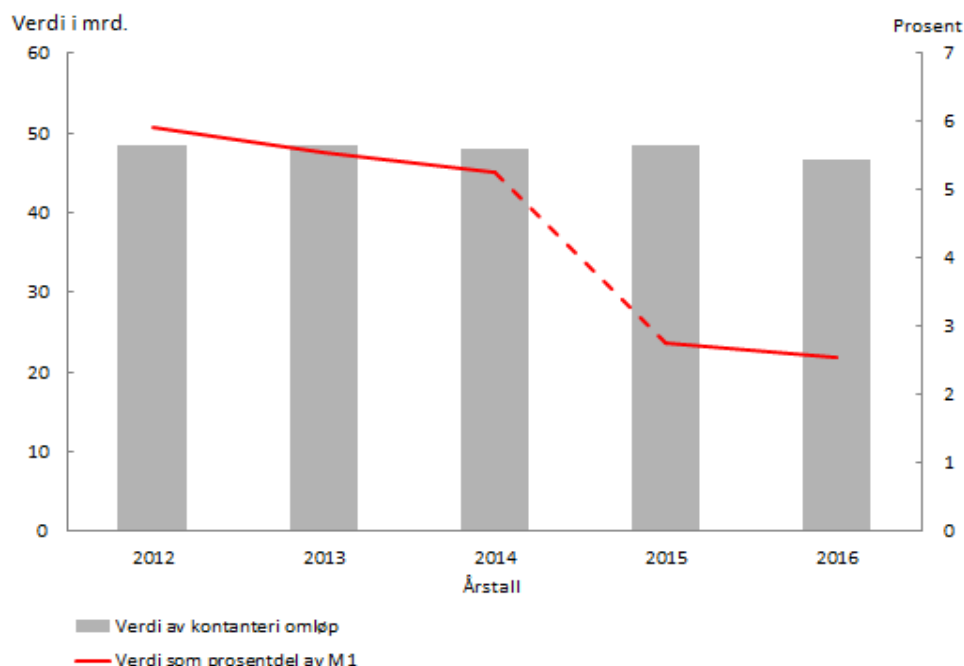
Norges Bank (2017) stadfester at verdien av kontanter i omløp har vært relativt stabil, i underkant av 50 milliarder, de siste årene. Målt som andel av den smale pengemengden<sup>2</sup>, i år 2016, utgjorde dette 2,5 prosent (se Figur 2.3.1-1). Til sammenligning utgjorde andelen 2,7 prosent i år 2015. Norges Bank (2017) påpeker også at uttak fra både minibank og ved varekjøp reduseres.

---

<sup>1</sup> Det innebærer også å tilrettelegge for at kontanter er tilgjengelige for befolkningen (Norges Bank, 2014).

<sup>2</sup> Den smale pengemengden, M1, er penger som er umiddelbart tilgjengelige for bruk. Dette inkluderer kontanter i omløp og innskudd på transaksjonskontoer (Norges Bank, 2017).

Figur 2.3.1-1<sup>3</sup>. Verdi av kontanter i omløp og som prosentdel av verdien av betalingsmiddel (M1)



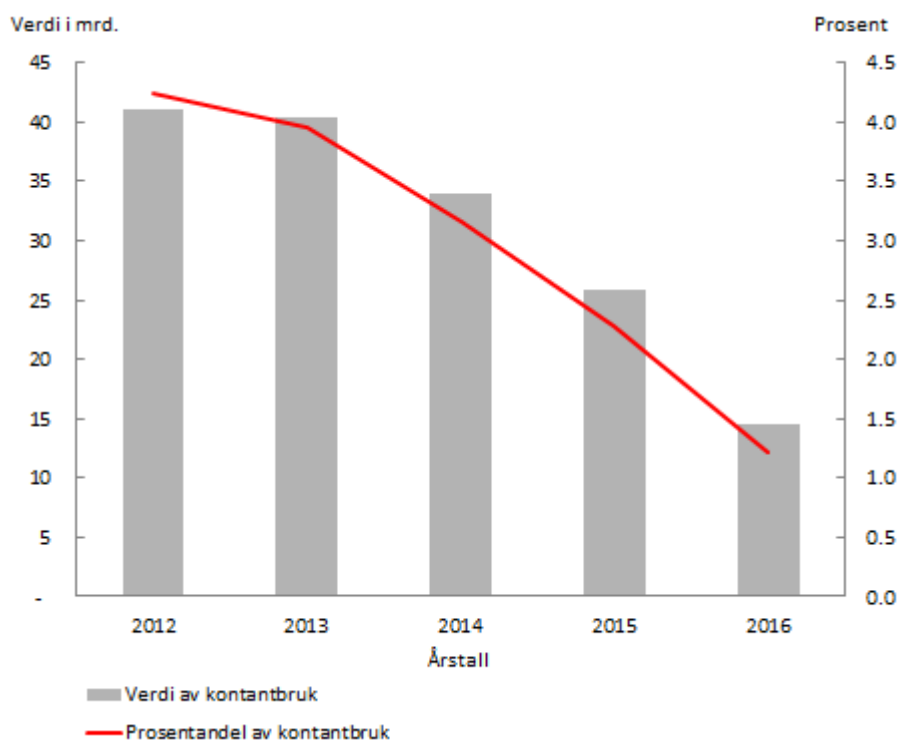
Kilde: Tallene er hentet fra tabellvedlegget til Norges Bank sin rapport: «Kunderetta betalingsformidling 2016» (Norges Bank, 2017).

Kontanter i omløp er et mål på sirkulasjonen av kontanter i samfunnet. Det er ikke et tall for den faktiske bruken av kontanter. Da store deler av betalinger gjennomført med kontanter ikke registreres, er det vanskelig å beregne den virkelige verdien og det virkelige antallet transaksjoner som er gjennomført med kontanter.

På bakgrunn av vår analyse, utgjør betalinger med kontanter en svært liten del av betalingene som gjennomføres i Norge (se Figur 2.3.1-2). I vårt estimat er verdien av kontantbruk rundt 14,5 milliarder kroner i år 2016. Dette utgjør 1,22 prosent av totalverdien for betalinger gjennomført med enten kort, giro, sjekk eller kontanter. Til sammenligning utgjorde verdien i år 2015 rundt 25,7 milliarder kroner, som tilsvarer en prosentandel på 2,28 prosent.

<sup>3</sup> Definisjonen av M1 ble endret i 2015, som fører til brudd i statistikken til statistisk sentralbyrå. Endringen innebar at flere typer innskudd skulle regnes med i definisjonen (Regjeringen, 2017).

Figur 2.3.1-2<sup>4</sup>. Verdien av kontantbruk i Norge



Kontanter utgjør en stadig mindre del av pengene våre og betydningen av kontanter som betalingsmiddel i Norge reduseres. Norges Bank (2018) har imidlertid uttalt at kontantene ikke vil forsvinne på lang tid og at de vil møte etterspørsel etter kontanter i mange år fremover. At elektroniske betalingsmetoder i større grad velges til betaling fremfor kontantene, indikerer likevel at det er et pågående skift i forbrukernes betalingsatferd som Norges Bank må ta hensyn til.

### **Fremgangsmåte for estimat av verdien av kontanter i Norge:**

For å finne et estimat på kontantbruken i Norge har vi tatt utgangspunkt i forbruket til norske husholdninger etter varer- og tjenestegrupper. Videre har vi analysert de ulike posteringene i forbruket per husholdning og trukket vekk poster hvor det er stor sannsynlighet for at

<sup>4</sup> Det har vært to omlegginger i produksjonen av familie- og husholdningsstatistikken i hhv. 2014 og 2015. Fra 2014 ble ugifte studenter bosatt hjemme hos foreldrene flyttet ut og plassert i husholdninger i nærhet til studiestedet, samt at det ble gjennomført en samordning i 2015 mot boligstatistikken. Det er beregnet tall per 01.01.2014 med begge omleggingene for å hindre to brudd i statistikken. Totalt sett førte de to omleggingene til en nedgang i antall privathusholdninger på 0,7 prosent i forhold til hva den gamle rutinen ville gitt (Statistisk sentralbyrå, 2015).

betalinger ble gjennomført med andre betalingsinstrumenter enn kort eller kontanter<sup>5</sup>. Da står vi igjen med forbruket i norske husholdninger som er gjennomført enten med kort eller kontanter. Da Norges Bank har statistikk på verdien av korttransaksjoner, trekkes verdien ifra for å få et estimat på verdien av kontantbruk i Norge.

Den siste forbruksundersøkelsen ble gjennomført av SSB i 2012. For å beregne forbruket til norske husholdninger fra 2013 til og med 2016 har vi beregnet gjennomsnittlig endring i det totale forbruket fra 2002 til og med 2012 og funnet en prosentvis økning på 3,84 prosent.

Vi har antatt at fordelingen i forbruket etter varer – og tjenestegrupper fra 2013 til og med 2016 er lik som fordelingen i år 2012. Fordelingsmønsteret skiller seg ikke i stor grad fra år til år de tidligere årene. Forskjellen blir enda mindre om vi sammenligner 3-årsperioder i ett. Vi mener dermed at det er en akseptabel antagelse å legge til grunn fordelingen etter forbruket i år 2012 også i årene etter 2012. Uavhengig av hvilken antagelse som legges til grunn her, blir trenden av kontantbruk den samme: bruken av kontanter som betalingsinstrument i Norge faller.

### **2.3.2 Beredskap og sikkerhet**

Til tross for at betydningen av kontanter som betalingsmiddel i Norge faller, kan kontantene ha en viktig funksjon i samfunnet dersom en krisesituasjon skulle oppstå. De fleste nye betalingsløsningene er avhengig av at kritisk samfunnsinfrastruktur som nettilgang og strømforsyning fungerer (Forbrukerrådet, 2017). Da det ikke finnes elektroniske betalingsløsninger som er uavhengige av de ordinære betalingsløsningene er det kontantene som skal være redningen i en eventuell krisesituasjon.

En krisesituasjon kan oppstå av ulike årsaker og kan føre til svikt i det elektroniske betalingssystemet, svikt i bankenes forsyningssystem for kontanter og/eller en vesentlig etterspørsel etter kontanter.

---

<sup>5</sup> Bolig, lyd og brensel, post og teletjenester, utdanning samt deler av transport anses å være lite sannsynlig til å bli betalt med kort eller kontant. SSB anslår at kjøp av biler utgjør rundt halvparten av utgiftene til transport (Statistisk sentralbyrå, 2015). Halvparten av denne posten er dermed tatt bort og anses å være betalt med giro.

---

På bakgrunn av et felles tilsyn gjennomført av Finanstilsynet og Norges Bank i 2013 kom det frem at ingen av bankene som ble undersøkt hadde en tilfredsstillende beredskap for distribusjon av kontanter, dersom en krisesituasjon skulle oppstå (Forbrukerrådet, 2018).

En svikt i, for eksempel, strømtilførselen vil imidlertid også påvirke tilgangen til kontantene. Minibankene er avhengig av kommunikasjon med bankenes systemer slik at uttakene kan autoriseres. Bankene vil heller ikke få tilgang til penger fra depotene, da Norges Bank må autorisere transaksjoner for å overføre kontanter til kontraktørene. Videre vil ikke kontantkasseløsningene fungere dersom det oppstår en svikt i strømtilførselen (Finans Norge, 2017).

Finans Norge (2017) skriver at det elektroniske betalingssystemet er robust i mindre eller kortvarige krisesituasjoner. Det er etablert reserveløsninger, slik at betalinger fremdeles kan gjennomføres, dersom det skulle oppstå en svikt i det elektroniske betalingssystemet. At kontantene kan erstatte de elektroniske betalingene i en krisesituasjon av langvarig karakter anses å være lite sannsynlig. Videre vil en større kontantbeholdning, som sikkerhet i krisetider, representere et sikkerhetsproblem.

Det er ikke bare det elektroniske betalingssystemet som kan settes ut av spill i en krisesituasjon, men også tilgangen til kontantene. Ettersom kontantbruken i Norge stadig reduseres, og mest sannsynlig vil fases ut på sikt, virker det mest formålstjenlig å gjøre de elektroniske betalingsløsningene enda mer robuste.

### **2.3.3 Svart økonomi**

Svart økonomi er en betegnelse på alle økonomiske aktiviteter som påvirker BNP, men som ikke blir registrerte (Schneider & Enste, 2000). Varer og tjenester kan kjøpes til en lavere pris og selgere ender opp med en høyere fortjeneste. Dette fører til at skatteinntektene til staten reduseres. Betalinger i dette markedet utføres ofte ved bruk av kontanter da det reduserer sannsynligheten for å bli tatt. Størrelsen på den svarte økonomien er dermed en av faktorene som påvirker etterspørselen etter kontanter.

I en undersøkelse fra 2013 ble det estimert at størrelsen på den svarte økonomien<sup>6</sup> i Norge i 2015 var på 13 prosent av BNP (Schneider, 2015). Den svarte økonomien i form av skattetap

---

<sup>6</sup> Ekskludert kriminell aktivitet som narkotikahandling, smugling, hvitvasking av penger og underslag.

er estimert til å være rundt 40 milliarder kroner årlig (Holte, 2017). Dette skaper ineffektivitet ettersom lovlige bedrifter blir utkonkurrert av bedrifter som jobber svart.

Graden av kompleksitet i skattesystemet er en faktor som avgjør hvor mange mennesker som velger å betale skatt (Kopczuk, 2006). Hvis digitale sentralbankpenger kan redusere kompleksiteten i skattesystemet kan det føre til en reduksjon i skattetafet.

En annen faktor som påvirker størrelsen på skattetafet er risikoen for å bli tatt. Digitale betalingstjenester gir en lavere grad av anonymitet som bidrar til høyere bruk av kontanter i en svart økonomi. Dersom digitale sentralbankpenger erstatter kontantene vil motivasjonen for skatteunndragelse reduseres.

## 2.4 Kontopenger

Kontopenger er et alminnelig godtatt betalingsmiddel. Kontopenger er kontanter stående på konto i banken. Ettersom kontanter og kontopenger måles i norske kroner og øre tilsvarer et beløp i kontanter akkurat det samme beløpet i kontopenger.

Når bankene gir ut lån skapes det kontopenger som settes inn på låntakers konto, som deretter kan ta i bruk kontopengene (Forbrukerrådet, 2018). Kontopengene disponeres av forbruker gjennom ulike betalingsinstrument, som betalingskort, sjekker eller betalinger direkte i nettbanken<sup>7</sup>. Nettbank er svært populært i Norge, da 9 av 10 nordmenn benytter seg av denne tjenesten (Håkonsen & Westby, 2016).

Kortbetalinger er det mest utbredte betalingsinstrumentet i Norge (DIBS, 2017). Denne løsningen tilbys av selskaper som blant annet Visa og Mastercard. For å benytte seg av tjenesten må kortholderen som regel betale en årsavgift for kortet og i noen tilfeller transaksjonsgebyrer. Når det gjelder kredittkort må kredittkortholdere også ta i betraktning eventuelle renter som påløper ved terminforfall. Brukerstedene må ofte betale en prosentandel av kjøpesummen hver gang en kunde betaler med kort (Oslo Economics, 2014).

Kortene kan benyttes til netthandel og er relativt sikre. Sikkerheten avhenger av hvilke sikkerhetsverktøy brukersteder velger å benytte. 3D-secure, som brukes til autentisering, er

---

<sup>7</sup> Betalinger direkte i nettbanken er girobetalinger, direkte debiteringer (Avtalegiro) eller eFaktura.

en av de mest brukte sikkerhetsverktøyene. Denne løsningen kan imidlertid oppfattes å være en tungvint variant av forbrukerne, da man må ha andre enheter tilgjengelige ved gjennomføring av transaksjoner. Dette gjelder særlig for små beløp.

I den senere tid har kontopengene blitt tilgjengelige gjennom ulike applikasjoner på mobiltelefoner. Da kortinformasjonen legges inn i mobiltelefonen kan mobiltelefonen benyttes for å gjennomføre kjøp på internett, fysisk på brukersteder eller ved betalinger fra en person til en annen (Norges Bank, 2017).

Vipps som er utviklet av DNB er den mest populære betalingsapplikasjonen i Norge og brukes av 2,9 millioner nordmenn (Vipps, u.d.). Da kortet ikke fysisk benyttes, vil det være raskere å utføre betalinger ved bruk av denne metoden. Det forutsetter imidlertid at betaler har strøm på mobiltelefonen, samt internettforbindelse når betalingen utføres.

Begrepet «tradisjonelle penger» vil heretter benyttes i oppgaven som en betegnelse på både kontanter og kontopenger.

## 2.5 Elektroniske penger

Elektroniske penger er definert i Finansforetaksloven (2015, § 2-4, annet ledd) som: «en elektronisk lagret pengeverdi, representert ved en fordring på utstederen, som er utstedt etter mottak av midler for å utføre betalingstransaksjonen og som er anerkjent som betalingsmiddel av andre foretak enn utstederen».

Elektroniske penger kjøpes ved hjelp av tradisjonelle penger av et e-pengeforetak som deretter gir kjøper tilsvarende verdi i elektroniske penger. Kjøper vil dermed ha en fordring på e-pengeforetaket for det innskutte beløpet. De elektroniske pengene lagres på en elektronisk innretning, som kort, datamaskin eller på en internettbasert konto og kan benyttes hos brukersteder som aksepterer betaling med elektroniske penger. Kjøper av elektroniske penger kan innløse verdien av elektroniske penger til pålydende verdi i tradisjonelle penger. Utviklingen i verdien på de elektroniske pengene vil således følge utviklingen til de tradisjonelle pengene (Finansdepartementet, 2002).

PayPal er det mest kjente og utbredte e-pengeforetaket i våre dager. Bruk av PayPal, forutsetter tilgang til en datamaskin eller smarttelefon og internettkobling. Ved opprettelse av en internettbasert PayPal-konto er det mulig å overføre penger til kontoen manuelt eller

via debet/kredittkort. Ved bruk av en PayPal konto kan både privatpersoner og bedrifter overføre og motta penger via internett. Det er over tusenvis av nettbutikker som tilbyr betaling via PayPal, som ligger i begrepets definisjon; anerkjennes som betalingsmiddel av andre foretak enn utstederen.

Å registrere en konto er gratis, men enkelte transaksjoner og handel i utenlandsk valuta tillegges ekstra gebyr. Nettbutikker påføres også et gebyr per transaksjon. PayPal er mindre sikkert enn betalinger gjennomført med bankkort eller nettbank, men oppfattes likevel som det sikreste alternativet av de som handler på internett (DIBS, 2017).

## 2.6 Virtuell valuta

Virtuell valuta er en digital valuta, som i utgangspunktet brukes for betalinger over internett, særlig i såkalte virtuelle samfunn<sup>8</sup>. Virtuelle valutaer oppstår når de virtuelle samfunnene utsteder sine egne digitale valutaer for handel av virtuelle varer og tjenester som tilbys innenfor det virtuelle samfunnet (European Central Bank, 2012).

En virtuell valuta er ikke utstedt av en sentralbank; den er normalt utstedt og kontrollert av dens utvikler. Dette kan være bedrifter, private organisasjoner, eller til og med individuelle personer. Virtuelle valutaer reguleres ikke og utsteder er ikke underlagt finansielt tilsyn av staten (Segendorf, 2014). Sikkerheten til forbrukeren vil således være svakere enn dagens tradisjonelle penger. Videre er det stor usikkerhet til verdien, da virtuelle valutaer er svært volatile. Verdien er ikke garantert av noen sentralbank og baseres på populariteten til den virtuelle valutaen, som igjen er basert på for eksempel antall brukere, hvor lett den kan handles med, hva brukerne tror verdien er eller troen på den underliggende teknologien. På grunn av de store svingningene i verdien er investering i virtuelle valutaer ansett som svært spekulativ (Australian Securities and investment commission, 2018).

European Central Bank (2012) klassifiserer virtuelle valutaer i ulike typer ut i fra interaksjonen den har med tradisjonelle penger:

---

<sup>8</sup> Et virtuelt samfunn defineres av European Central Bank som et nettsted hvor individer samhandler og følger felles interesser og/eller mål (European Central Bank, 2012).



(1) Lukket virtuell valuta benyttes innenfor virtuelle samfunn knyttet til internettspill. Den er ulovlig å kjøpe og selge, og kan kun oppnås gjennom prestasjoner i spill. Videre kan den opptjente virtuelle valutaen kun benyttes til å kjøpe virtuelle varer og tjenester innenfor det spesifikke virtuelle samfunnet.

(2) Enveisrettet (unidirectional) virtuell valuta kan kjøpes til en satt vekslingskurs, ved hjelp av tradisjonelle penger. Den er enveisrettet, da den virtuelle valutaen ikke kan veksles tilbake til tradisjonell valuta. Den virtuelle valutaen benyttes til å kjøpe virtuelle varer eller tjenester, men kan også i noen tilfeller benyttes til å kjøpe virkelige varer eller tjenester.

(3) Toveisrettet (bidirectional flow) virtuell valuta kjøpes ved hjelp av tradisjonell penger, til en gitt vekslingskurs og kan veksles tilbake til tradisjonell valuta. Vekslingskursen er basert på en spesifikk kurs eller prisen i markedet. Kryptovaluta kan således sies å være en type toveisrettet virtuell valuta. Da digitale sentralbankpenger må kunne veksles frem og tilbake mellom tradisjonelle penger og elektroniske penger, er det en toveisrettet virtuell valuta som vil være mest aktuell i utformingen av digitale sentralbankpenger.

## 2.7 Sentralbankens ansvar

Da digitale sentralbankpenger vil være en fordring direkte på sentralbanken vil en innføring av digitale sentralbankpenger ha en påvirkning på sentralbankens likviditetsstyring. For å vurdere implikasjonene ved en innføring av digitale sentralbankpenger for sentralbankens likviditetsstyring må vi se på hvordan systemet fungerer i dag og hvilke ansvar sentralbanken har i betalingsvesenet.

### 2.7.1 Tillit og troverdighet

Da penger i moderne tid ikke er knyttet mot metaller er det utelukkende tillit og troverdighet som gir pengene verdi (Nicolaisen, 2017). Norges Bank er uavhengig og står som garantist for at pengeverdien er stabil. Oppgaven er delegert til Norges Bank av den norske stat som også i egen forskrift har tallfestet at inflasjonen over tid skal være nær 2 prosent<sup>9</sup> (Regjeringen, 2018). I et system som utelukkende er basert på tro og tillit er det viktig at

---

<sup>9</sup> Inflasjonsmålet ble innført i år 2001 og var på 2,5 prosent. Inflasjonsmålet har blitt redusert til 2 prosent i år 2018.

Norges Bank sikrer lav og stabil inflasjon, slik at penger har en stabil verdi på lang sikt. Inflasjonen i Norge har vært lav og stabil i et kvart århundre (Nicolaisen, 2017).

Kontopengene oppfattes til å være like sikre som kontantene. Ansvarlig bankdrift er en forutsetning for at vi skal ha tillit til bankene og at innskuddene våre oppleves som sikre på innskuddskonto i banken. Banksektoren er underlagt strengt tilsyn og er en av de mest regulerte sektorene i vårt samfunn. Bankenes utlån og pengeskaping, reguleres av en rekke krav til både kapitaldekning og likviditetsstyring. Ved strenge krav og tilsyn til banksektoren opprettholdes tilliten til bankene, samt tilliten til kontopengene. Videre er personlige innskudd i enhver bank, opptil 2 millioner kroner, sikret av en innskuddsgaranti (Nicolaisen, 2017).

### **2.7.2 Sentralbankens likviditetsstyring**

Bankene i Norge oppretter konto<sup>10</sup> direkte hos sentralbanken som benyttes for å gjøre opp transaksjonene seg imellom. Summen av bankenes ikke-bundne innskudd i sentralbanken omtales som bankenes reserver<sup>11</sup>. Da bankene vil ha en fordring på sentralbanken for det innskutte beløpet, vil bankinnskudd havne på gjeldssiden i sentralbankens balanse (se Figur 2.7.2-1).

Bankenes reserver kan endres på to måter; (1) på bakgrunn av autonome faktorer<sup>12</sup> eller (2) via markedsoperasjoner foretatt av sentralbanken (Syrstad, 2011).

Da kontanter er styrt av etterspørsel i samfunnet, vil kontanter være en autonom faktor for sentralbanken (Syrstad, 2011). Kontanter gir en fordring på sentralbanken, og vil ende opp som en gjeldspost i sentralbankens balanse. Når befolkningen ønsker kontanter kjøper deres respektive banker kontanter fra sentralbanken ved å trekke fra sine reserver stående hos sentralbanken. Mengden bankreserver i banksystemet vil reduseres. Posten for «Kontanter» vil øke tilsvarende reduksjonen i bankenes reserver i sentralbankens balanse.


---

<sup>10</sup> Omtales også som «foliokonto».

<sup>11</sup> Omtales også som «sentralbankreserver», «reserver» eller «bankenes likviditet».

<sup>12</sup> Forhold utenfor sentralbankens kontroll (Syrstad, 2011).

Figur 2.7.2-1. Utvalgte poster i en forenklet oppstilling av sentralbankens balanse

	<b>Sentralbankens balanse</b>	
	<b>Eiendeler</b>	<b>Gjeld</b>
	Utlån til banker	Bankinnskudd ( reserver)
	Verdipapirer	Innskudd fra staten
	Valutareserver	Kontanter

Kilde: Tabellen er inspirert av Aamodt og Lerbak (2013) sin oppstilling av sentralbankens balanse.

På gjeldssiden i sentralbankens balanse finner vi også posten «Innskudd fra staten», som er den største autonome faktoren som påvirker mengden reserver i banksystemet. Sentralbanken kan ikke styre statens høye inn -og utbetalinger. Når vi betaler skatter og avgifter til staten, overføres reserver fra bankene til statens konto i sentralbanken og mengden bankreserver reduseres. Effekten vil være motsatt når staten utbetaler penger til befolkningen (Syrstad, 2011).

Sentralbanken tilpasser mengden bankreserver i banksystemet, blant annet via markedsoperasjoner for å nå målet om å holde de kortsiktige pengemarkedsrentene nær styringsrenten<sup>13</sup> (Norges Bank, 2017). Når mengden bankreserver er for høyt tilbyr sentralbanken F-innskudd for å redusere mengden bankreserver. Sentralbanken tilbyr bankene F-lån mot sikkerhet når mengden bankreserver er under ønsket nivå for å øke mengden bankreserver. Rentene på F-innskudd og F-lån settes vanligvis på bakgrunn av en flerprisauksjon og dens løpetid varierer med bakgrunn i likviditetssituasjonen i markedet. Når det gjelder F-innskudd vil reserver trekkes fra banksystemet, ved at bankene binder innskuddet i en gitt periode og ikke kan benyttes før løpetiden er utløpt. F-lån er også bundet i løpetiden og kan ikke tilbakebetales før låneperioden er utløpt (Norges Bank, 2017).

Sentralbanken tilbyr også bankene stående fasiliteter, for å sikre at betalingsoppgjørene mellom bankene fungerer. D-lån gjennom dagen<sup>14</sup> gir bankene mulighet til å låne reserver

<sup>13</sup> Omtales også som «foliorenten».

<sup>14</sup> Omtales også som «intradagfasilitet».

mot sikkerhet, rentefritt fra sentralbanken. Bankene tilbakebetaler lånet i løpet av dagen, for at ikke lånet skal omgjøres til et D-lån over natten hvor renten ligger én prosentenheter høyere enn styringsrenten (Norges Bank, 2013).

Sikkerheten som stilles bak banklånene, både D-lån og F-lån må godkjennes av Norges Bank og være av god kvalitet. Norges Bank ønsker lavest mulig risiko bak lånene som blir gitt bankene (Norges Bank, 2016).

Vi har også inkludert postene «Verdipapirer» og «Valutareserver» i sentralbankens balanse. Sentralbanken kan også justere mengden bankreserver ved å kjøpe/selge verdipapirer og valutaer. Da vil posten for «Bankinnskudd» justeres tilsvarende postene for henholdsvis «Verdipapirer» og «Valutareserver» (Syrstad, 2011).

Sentralbankens likviditetsstyring er bygget på et kvotesystem hvor bankene får forrentet en andel av sine innskudd til styringsrenten<sup>15</sup>. Innskudd utover denne kvoten, som settes av sentralbanken, forrentes til en såkalt «reserverente» som ligger én prosentenheter under styringsrenten (Syrstad, 2011). Siden september 2015 har reserverenten vært negativ og er nå på minus 0,5 prosent (Norges Bank, 2018). Bankene som har innskudd utover kvoten vil heller låne sine reserver til andre banker, fremfor å ha reservene stående til en negativ reserverente i sentralbanken. Banker med innskudd under sin kvote, vil heller låne penger av andre banker, for å fylle opp sin kvote, til en lavere markedsrente enn utlånsrenten til sentralbanken. Kvotesystemet gjør det mindre attraktivt for bankene å ha store reserver stående på konto hos sentralbanken, på grunn av den lave reserverenten.

### **2.7.3 Betalingssystemet**

Det gjennomføres transaksjoner hver dag, ved at befolkningen tar i bruk kortene sine eller registrerer regninger i nettbanken. Når betalingsavsender og betalingsmottaker har konto i samme bank, vil oppgjøret gjennomføres umiddelbart ved at banken belaster betalingsavsender sin konto og godskrifer betalingsmottaker sin konto.

Når betalingsavsender og betalingsmottaker har konto i ulike banker oppstår det et fordrings- og gjeldsforhold mellom bankene. Da går betalingen gjennom et system for avregning og

---

<sup>15</sup> Frem til oktober 2011 var likviditetsstyringen basert på et gulvsystem hvor ethvert innskudd i sentralbanken ble forrentet til styringsrenten (Syrstad, 2011).

oppgjør mellom bankene<sup>16</sup> hvor nettoposisjonen til bankene posteres i en oppgjørsbank. De mindre bankene kan benytte en privat bank som oppgjørsbank, som igjen har sentralbanken som sin oppgjørsbank. De fleste betalinger mellom bankene går gjennom bankenes daglige avregningssystem, NICS. Avregningene fra NICS sendes til sentralbankens oppgjørssystem (NBO) fire ganger om dagen<sup>17</sup> som bekrefter avregningen som er foretatt og posterer bankenes kontoer i sentralbanken (Norges Bank, 2016).

For at en betaling skal gjøres opp må banken ha dekning for betalingen på sin konto i sentralbanken. Dersom banken ikke har dekning for beløpet, må banken benytte seg av sentralbankens stående fasiliteter for å øke innskuddet sitt i sentralbanken.

Betalingsoppdraget vil ikke gjennomføres dersom det ikke er dekning for betalingen på kontoen i sentralbanken. Da vil betalingsoppdraget legges i kø i NBO, frem til det er dekning på kontoen igjen. Det er imidlertid en funksjon i systemet som lar betalingsoppdraget gå gjennom dersom summen av inngående betalinger i kø er større enn summen av de utgående betalingene i kø for avsenderbanken (Norges Bank, 2016).

Overføringer mellom banker ikke vil påvirke mengden bankreserver i balansen til sentralbanken. Overføringer mellom banker vil bare påvirke hvordan bankreservene er fordelt mellom de ulike bankene.

---

<sup>16</sup> Omtales som «interbanksystemer».

<sup>17</sup> Gjennomføres ikke i helger eller på helligdager.

### 3. Et effektivt betalingssystem

«Et effektivt betalingssystem kjennetegnes ved at betalinger kan gjennomføres raskt, sikkert, til lave kostnader og på måter som er tilpasset brukernes behov» (Norges Bank, 2017, s.2). Digitale sentralbankpenger kan gjøre betalingssystemet mer effektivt dersom løsningen blir tatt i bruk av befolkningen. Vi har dermed sett på digitale ferdigheter i Norge og hva som avgjør villigheten til å ta i bruk nye betalingsløsninger. Til tross for at det eksisterende betalingssystemet regnes som effektivt, eksisterer det utfordringer knyttet til blant annet cyberkriminalitet og transaksjoner mellom banker (Norges Bank, 2017).

#### 3.1 Digitale ferdigheter

En viktig forutsetning for å kunne utnytte digitaliseringens muligheter er at befolkningen er vant med å bruke digitale løsninger (Fjørtoft, 2017). En undersøkelse av digitale ferdigheter i Norge viser at 45 prosent av nordmenn mellom 16 og 74 år har gode digitale ferdigheter, 29 prosent har grunnleggende ferdigheter og 26 prosent har mangelfulle eller ingen digitale ferdigheter (Statistisk sentralbyrå, 2017). Sammenlignet med landene i resten av Europa har befolkningen i Norge gode digitale ferdigheter. Det eksisterer en risiko for at deler av samfunnet, som ikke har digitale ferdigheter, kan bli ekskludert ved en innføring av digitale sentralbankpenger. For aldersgruppen 65 til 74 år er handel på internett, bruk av nettbank og installering av programvare betydelig lavere enn for de andre aldersgruppene. Den eldre delen av befolkningen forventes å være mest utsatt ved innføring av digitale sentralbankpenger.

Undersøkelsen viser også at 91 prosent av alle nordmenn i 2017 har benyttet internett til banktjenester. Denne andelen var på 83 prosent i 2011, noe som viser at trenden har vært positiv de siste 6 årene (Statistisk sentralbyrå, 2017). Dette er en indikasjon på høyere etterspørsel etter digitale betalingsløsninger.

#### 3.2 Opptak av nye betalingsløsninger

De viktigste faktorene for brukersteder som vurderer å ta i bruk nye betalingsløsninger er: i hvilken grad løsningen bidrar til økt omsetning, kostnader som påføres ved bruk av den nye løsningen og hvor sikker den er (Oslo Economics, 2014).

---

For at en ny betalingsløsning skal øke omsetningen må det eksistere kunder som ønsker å benytte betalingsløsningen. Kunder vil ha betalingsløsninger som er praktisk og er akseptert av mange brukersteder (Oslo Economics, 2014). Desto flere brukersteder som tar i bruk en betalingsløsning, desto høyere verdi har den for kundene. Butikker vil på samme måte ha løsninger som fungerer på alle plattformer og gjør det enkelt for forbrukere å utføre en handel. Dette skaper en nettverkseffekt som fører til at en betalingsløsning har en høyere verdi når antall brukere øker. Nye betalingsløsninger vil typisk ha vanskeligheter med å etablere seg ettersom verdien av å tilby slike løsninger vil være lav i begynnelsen.

Bedrifter vil maksimere sin fortjeneste som gjør det ettertraktet å bruke betalingsløsninger som kan redusere kostnadene. Hvor mye kostnadene kan reduseres avhenger av de eksisterende betalingsløsningene. Nyere betalingsløsninger vil tilføre mindre verdi hvis effektive løsninger allerede er implementert. Digitale sentralbankpenger basert på desentralisert teknologi forventes å ha lave transaksjonskostnader, men kostnadsbesparelsene antas å bli lave da Norge har et relativt effektivt betalingssystem.

Sikkerhet er et annet kriterium som vurderes når brukerstedene vurderer nye betalingsløsninger. For nettbutikker er varianten hvor kunder registrerer kortinformasjon én gang og deretter kan handle uten ytterligere bekreftelser den mest ønskede betalingsløsningen (DIBS, 2014). Denne løsningen er praktisk, men mindre sikker. 3D-secure er et eksempel på en protokoll som gjør betalinger mer sikker. Nettbutikker forteller at de har fjernet 3D-secure for mindre transaksjoner, for å forenkle kjøpsprosessen ved korthandel på internett (Oslo Economics, 2014). Graden av sikkerhet er viktig for brukersteder opp til et hvis punkt og balanseres med kostnadene den medfører.

### 3.3 Transaksjoner mellom banker

En betaling mellom kunder i ulike banker går gjennom flere ledd som må verifisere betalingen (Nicolaisen, 2016). Transaksjonskostnadene ved betaling mellom ulike banker i Norge overføres ikke til kundene. Hvor raskt pengene godskrives mottakers konto avhenger av hvilken metode banken overfører pengene på: den «treige» metoden er at mottakerens bank godskriver mottakers konto etter at bankene har gjort opp seg imellom. Ved denne metoden utføres transaksjoner mellom ulike banker bare på virkedager, og opptil fem ganger per dag.

Den raske måten er at mottakerens bank godskrives mottakers konto før bankene har gjort opp seg imellom. Dette fører derimot til at mottakerens bank påtar seg en kredittrisiko, da pengene ikke har ankommet mottakerbanken før beløpet godskrives mottakers konto. For å redusere denne risikoen ble det etablert en infrastruktur for «straksbetalinger». Dette innebærer at bankene fordeler eventuelle tap seg imellom og begrenser det potensielle tapet for en enkelt bank. Etterspørselen etter slike løsninger vil øke i fremtiden og de eksisterende norske betalingsløsninger er ikke utformet til å tåle en slik økning (Norges Bank, 2017).

For å sende penger til utlandet må avsenderen betale transaksjonskostnader. Kostnaden varierer basert på hvilken bank både avsender og mottaker benytter, samt landet man sender penger til. En slik overføring kan ta inntil 8 dager. Betalinger gjennomført til land i EU og i euro, såkalte SEPA- betalinger, gjennomføres derimot raskere og godskrives normalt innen 2 dager. Grunnen til at internasjonale betalinger tar lenger tid og er mer kostbar, er at pengene gjerne blir sendt gjennom flere banker. Overføringer forsinkes ofte for å redusere sannsynligheten for bedrageri (Fexco u.d.).

### 3.4 Cyberkriminalitet

IT har gjort overføring av penger mellom ulike banker mer effektivt, samtidig har det skapt større utfordringer knyttet til cyberkriminalitet. Norges Bank (2017) har vurdert cyberkriminalitet som en av de største truslene mot finansiell stabilitet.

Et vellykket cyberangrep kan innebære tap av verdi, forstyrrelse av kundenes transaksjoner eller tap av sensitiv informasjon. De som utfører denne type handlinger er ofte organiserte kriminelle og/eller hackeraktivister, men kan også være innsidere. Sikkerheten avhenger i stor grad av kvaliteten på sikkerhetsløsningene, men også av ansatte i de finansielle institusjonene. En undersøkelse av norske og danske bedrifter som ble utført av PwC i 2017 viste at de ansattes ubevisste handlinger og organisert kriminalitet vil utgjøre den største cybertrusselen i fremtiden (PwC, 2017).

I følge Norges Bank (2017) skaper sentralitet i forsyningskjeden økt risiko for sikkerhetsbrudd. Store deler av IT-driften utføres av sentrale leverandører. Disse leverandørene blir ofte brukt av mange ulike banker. Sentrale aktører kan utnytte stordriftsfordeler for å lage mer robuste og sikre løsninger. Dette skaper derimot en risikabel situasjon hvor et vellykket cyberangrep mot en sentral leverandør kan påvirke hele systemet.



## 4. Desentralisert teknologi

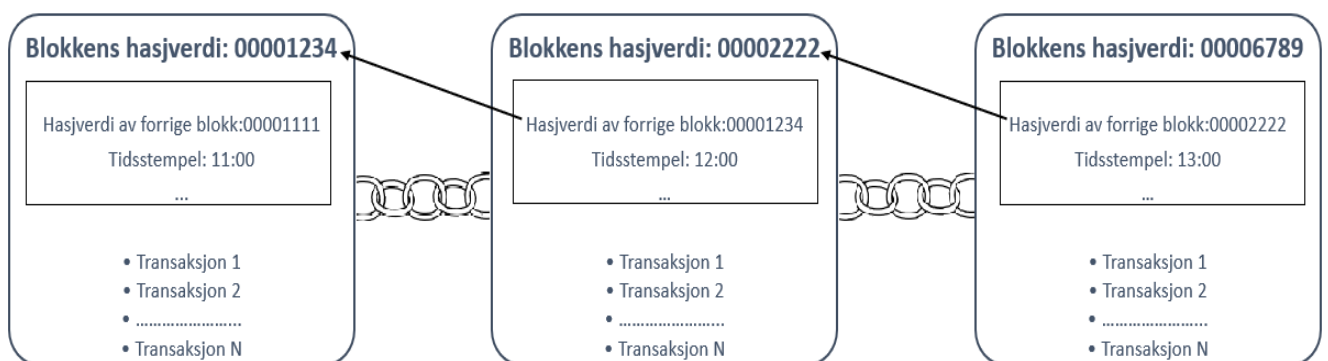
Blokkjede gjør det mulig å overføre verdi uten en sentral tredjepart som verifiserer transaksjonen. I en blokkjede kan et nettverk av datamaskiner verifisere en transaksjon på relativt kort tid. I denne delen vil vi se på strukturen til en blokkjede, protokoller som er brukt til å oppnå konsensus, hvordan transaksjoner blir utført og desentraliserte applikasjoner. Teknologien vil påvirke hvordan digitale sentralbankpenger kan utformes. Vi vil også se på digitale lommebøker ettersom de ofte benyttes sammen med desentralisert teknologi.

### 4.1 Blokkjede

En blokkjede er en distribuert database hvor enhver node registrerer endringer i det som gjøres på de andre nodene. Databasen består av blokker hvor hver blokk bortsett fra den første refererer til den forrige. Nodene produserer blokker som eventuelt kan kobles til blokkjeden. For at blokkjeden skal inneholde gyldig informasjon blir det brukt konsensusmekanismer for å verifisere innholdet i blokkene.

Blokkene i en blokkjede er koblet ved hjelp av hashing (se Figur 4.1-1). Hver blokk inneholder en hashverdi som avhenger av innholdet i blokken. Hvis informasjonen i blokken forandres vil blokken få en annen hashverdi. Siden innholdet i alle blokker, bortsett fra den første, inkluderer hashverdien til den forrige blokken, betyr det at en forandring i en blokk vil forandre hashverdien til de påfølgende blokkene. På denne måten kan deltakere av nettverket være sikker på at innholdet i tidligere blokker ikke har blitt forandret på.

Figur 4.1-1. Hashing i blokkjeden



## 4.2 Konsensus

I et desentralisert nettverk hvor hvem som helst kan verifisere transaksjoner er det utfordrende å bli enige om hvilken versjon av blokkjeden som er korrekt. Ved hjelp av konsensusmekanismer kan noder komme til enighet om en bestemt versjon av blokkjeden uten å stole på hverandre.

I desentraliserte nettverk blir det brukt ulike versjoner av blant annet Proof-of-Work og Proof-of-Stake. Ved hjelp av disse protokollene kan noder verifisere transaksjoner og sørge for at systemet opprettholder en høy grad av sikkerhet. For å motivere noder til å verifisere transaksjoner belønnes de med transaksjonskostnader og utstedelser av valuta når de legger til blokker.

### 4.2.1 Proof-of-Work

Proof-of-Work er en protokoll hvor mengden prosesseringskraft avgjør hvor stor innflytelse en utvinner<sup>18</sup> har. I denne protokollen må utvinnere finne en løsning på en matematisk oppgave. Denne løsningen kan forvandles til en hashverdi. For at en blokk skal regnes som gyldig kan ikke hashverdien overstige en viss grense (BitFury Group, 2015). Gjetting er den mest effektive måten å finne løsningen på og et stort utfallsrom gjør at en stor mengde prosesseringskraft må benyttes. Desto mer prosesseringskraft en node har, desto større sannsynlighet har den for å finne løsningen. En utvinner som finner løsningen deler blokken med resten av nettverket. Andre utvinnere kan dermed sjekke om transaksjonene i blokken er gyldige og begynne å bygge neste blokk basert på den nye hashverdien (Nakamoto, 2008).

Vanskelighetsgraden på oppgaven tilpasses basert på graden av sikkerhet man vil opprettholde i blokkjeden. Proof-of-Work sørger for at innholdet i en blokk ikke kan forandres på uten å løse oppgaven igjen (Nakamoto, 2008). En høyere vanskelighetsgrad fører til at en potensiell angriper må bruke mer prosesseringskraft for å lykkes. Bitcoin, for eksempel, øker vanskelighetsgraden annenhver uke (Meshkov, Chepurnoy, & Jansen, 2017). Dette fører til høye verifiseringskostnader, men også høy grad av sikkerhet.

---

<sup>18</sup> Utvinnere i Proof-of-Work omtales som «miners», mens utvinnere i Proof-of-Stake omtales som «forgers». Vi bruker begrepet «utvinnere» i begge protokollene.

---

## 4.2.2 Proof-of-Stake

Proof-of-Stake er en protokoll hvor innflytelsen til en node bestemmes ut ifra andelen av den totale pengemengden i systemet noden eier. En utvinner som har en høy grad av eierskap vil ha en større sannsynlighet for å produsere en blokk. Utvinnere som har akkumulert mest verdi vil være mest interessert i å opprettholde en høy grad av sikkerhet i nettverket, da de vil ha mest å tape hvis kursen til valutaen reduseres (BitFury Group, 2015).

I denne protokollen må utvinnerne på samme måte som i Proof-of-Work finne en løsning på den matematiske oppgaven. Den største forskjellen er at utfallsrommet avhenger av eierskapet til utvinneren i Proof-of-Stake istedenfor innholdet<sup>19</sup> i blokken som i Proof-of-Work (BitFury Group, 2015). Ved Proof-of-Stake reduseres antall verdier utvinneren må undersøke betraktelig og fører til lave verifiseringskostnader.

En klassisk versjon av Proof-of-Stake er problematisk å bruke i et desentralisert nettverk fordi graden av sikkerhet er lavere enn i Proof-of-Work. Det har blitt laget nye versjoner av protokollen som løser noen av utfordringene forbundet med lavere sikkerhet. Algoritmer som «Slasher» og «Tendermint» er basert på at blokker lages av forutbestemte brukere. Disse brukerne belønnes for å lage gyldige blokker og straffes for å gjøre det motsatte. På denne måten kan graden av sikkerhet opprettholdes på et relativt høyt nivå uten en stor økning i verifiseringskostnadene. Protokollen er i større grad basert på insentiver enn Proof-of-Work.

## 4.3 Transaksjoner

Hver bruker har en privat og en offentlig nøkkel. Den offentlige nøkkelen brukes til å verifisere at en bruker er eieren av en offentlig adresse<sup>20</sup>, mens den private nøkkelen brukes til å overføre verdi. Det er nesten umulig å finne ut hva den private nøkkelen er ved å analysere den offentlige, selv om den offentlige nøkkelen er et produkt av den private nøkkelen (Krishnan, 2004). Når en bruker utfører en transaksjon kombineres den private nøkkelen sammen med transaksjonsinformasjonen som danner en digital signatur. Den

---

<sup>19</sup> Innholdet i en blokk består av blant annet vanskelighetsgraden på den matematiske oppgaven.

<sup>20</sup> Offentlig adresse er et produkt av den offentlige nøkkelen.

digitale signaturen er unik og gjør at forandringer i transaksjonen fører til en helt annen signatur. Transaksjonen spres gjennom nettverket hvor noder kan legge den til i en blokk sammen med andre transaksjoner. Signaturen brukes dermed av noder til å verifisere at en bestemt bruker har utført en transaksjon uten at den private nøkkelen avsløres. Etter at blokken har blitt verifisert legges den til i blokkjeden. Når en tilstrekkelig mengde blokker har blitt lagt til er transaksjonen akseptert som gyldig (Antonopoulos, 2014). Denne informasjonen blir som regel publisert slik at alle brukere kan se hvor mye verdi som har blitt overført fra en offentlig adresse til en annen. Til tross for at de offentlige adressene regnes å være pseudonyme er det mulig å benytte teknikker basert på langvarige transaksjonsmønstre til å identifisere individuelle aktører (Monaco, 2015).

## 4.4 Smart contracts

Smart contracts er kontrakter i form av kode på en blokkjede som gjør det mulig å gjennomføre en avtale mellom to parter som ikke stoler på hverandre uten en betrodd tredjepart (Alharby & Moorsel, 2017). Når to parter inngår kontrakten går programmet gjennom koden og avgjør basert på kontraktsbetingelsene om verdi skal overføres til en bruker, sendes tilbake til den originale brukeren, eller en kombinasjon av disse (Buterin, 2017). Dette skjer basert på en utløsende faktor som for eksempel når kontrakten utløper eller prisen på en aksje.

Fordelen ved å bruke slike applikasjoner er at man slipper å bruke mellompersoner som for eksempel en advokat eller en megler. Dette kan være en billigere løsning ettersom man blir kvitt en del av transaksjonskostnadene. Kontraktene blir lagret i en hovedbok som alle har tilgang til. På denne måten er kontrakten lagret på en sikker måte, da alle har en kopi av den.

Det eksisterer enkelte ulemper ved bruk av smart contracts. Implementering av slike kontrakter kan være kostbar siden mye av kodingen må gjøres manuelt i begynnelsen. Det gir også høyere sannsynlighet for at de kan inneholde feil. Kontraktene må også reguleres, noe som skaper utfordringer på grunn av blokkjedens grad av anonymitet.

## 4.5 Digitale lommebøker

Digitale lommebøker kan brukes sammen med desentralisert teknologi til oppbevaring og overføring av verdi mellom brukere. En slik lommebok inneholder en eller flere private

nøkler (Guri, 2018). Lommeboken kan være i form av et program på en PC, på internett, på mobilen, på en USB eller i papirform.

Å bruke en digital lommebok på internett er en av de enkleste alternativene. Man lager en egen konto og får muligheten til å bruke verdien i lommeboken så lenge man har tilgang til internett. Svakheten med denne type lommebok er at den personlige nøkkelen lagres på en server. Av denne årsaken er det en av de minst sikre alternativene og brukes derfor ofte til lagring av små mengder kryptovaluta.

En digital lommebok i form av et program på en mobil/pc regnes som en sikrere løsning. Denne lommeboken kan bare brukes på den enheten hvor den ble lastet ned. Svakheten med denne typen lommebok er at slike enheter ofte er koblet til internett, selv når transaksjoner ikke utføres. Det øker risikoen knyttet til virusangrep. Innholdet i lommeboken vil forsvinne dersom enheten blir ødelagt.

En lommebok i form av en USB tilbyr relativ høy grad av sikkerhet. Man kan laste ned et program og overføre programmet til en USB. Alternativt kan man kjøpe en USB som allerede har programmet installert. Denne er sikrere da verdien er lagret på en USB som ikke er koblet til internett. Lommeboken må imidlertid ha internettilgang når en transaksjon skal gjennomføres.

Det sikreste alternativet er å benytte en lommebok i form av papir. Dette gjøres ved å laste ned et program som genererer en privat og offentlig nøkkel i form av en QR-kode. Denne koden lagres på papir og oppbevares på et sikkert sted. Denne metoden brukes vanligvis til å lagre store summer kryptovaluta, men er lite praktisk å bruke til noe annet enn verdioppbevaring. Verdien vil være tapt dersom papiret ødelegges eller mistes.

## 5. Implikasjoner av desentralisert teknologi

Digitale sentralbankpenger basert på desentralisert teknologi vil skape forandringer i det eksisterende betalingssystemet. Vi vil benytte desentraliserte kryptovalutaer for å danne et bilde av implikasjonene ved en desentralisert struktur. Vi vil se på mulige tilpasninger som kan gjennomføres for at teknologien på en hensiktsmessig måte kan tas i bruk av Norges Bank.

### 5.1 Anonymitet

Anonym er et ord som brukes til å beskrive situasjoner der navnet til personen er ukjent. En del av de som bruker desentraliserte kryptovalutaer som et betalingsmiddel gjør det på grunn av høyere grad av anonymitet. Elektroniske betalingsmetoder legger igjen opplysninger om forbrukeren, som gir økte muligheter til å kartlegge den enkelte forbruker og den enkeltes handlingsmønster. Ved en transaksjon gjennomført med kort, er det stort sett mulig å slå fast hva som faktisk er kjøpt, da både brukersted, tid og beløp registreres. Hver transaksjon isolert gir ikke mye informasjon, men det er alle transaksjonene samlet som gir et klart bilde av forbrukeren.

Blokkjede i seg selv gjør ikke transaksjoner anonym. Kombinert med kryptografiske verktøy kan brukere verifisere transaksjoner uten å vite hvem som har sendt verdi til hvem. I dette tilfellet er brukeren pseudonym som gir en høyere grad av anonymitet enn det som tilbys av andre elektroniske betalingsmetoder.

#### 5.1.1 Etterspørsel etter anonymitet

De fleste elektroniske transaksjonene i dag utføres gjennom en bank. Dette fører til at overføringer av penger er avhengig av en tredjepart som overser transaksjonene. Det eneste betalingsmiddelet i våre dager som gir fullstendig anonymitet er kontanter. Kontanter gir friheten til å velge selv hvorvidt man ønsker å gjennomføre anonyme betalinger. En eliminering av kontantene kan således dra oss i en retning av et overvåkingssamfunn, hvor enhver transaksjon kan spores og lagres hos de ulike finansinstitusjonene.

Det er åpenbart at det finnes kriminelle aktører som foretrekker anonyme transaksjoner ettersom det gjør kjøp av ulovlige varer og hvitvasking av penger lettere. På en annen side er

---

det rimelig å anta at lovlidige mennesker også vil ha et privatliv og rett til å bestemme over egne personopplysninger. Digitale sentralbankpenger må dermed opprettholde en viss grad av anonymitet.

### 5.1.2 Utfordringer ved anonymitet

Monero er en av de kryptovalutaene som tilbyr høy grad av anonymitet. Det er ikke mulig å se hvem som overfører penger til hvem og heller ikke hvor mye som blir overført. For å få til dette benytter Monero kryptografi som gjør at transaksjonene tar mer lagringsplass og påfører høyere transaksjonskostnader (Kumar, Tople, Fischer, & Saxena, 2017). Transaksjonene er ikke synlig for noen med mindre de som utfører transaksjonene velger å dele informasjonen med andre. Alle brukere har en personlig nøkkel som kan brukes til å gjøre transaksjonene synlige. En slik løsning passer for mennesker som vil ha en høyere grad av anonymitet. At transaksjoner tar større lagringsplass gjør blokkjeden vanskeligere å skalere.

Ved Bitcoin kan ikke en person identifiseres på én transaksjon. Hvis personen bruker den samme offentlige nøkkelen til alle transaksjoner finnes det teknikker, ved å analysere transaksjonshistorikken, som gjør personen identifiserbar (Androullaki, Karame, Roeschlin, Scherer, & Srdjan, 2012). Da alle brukere i nettverket har tilgang til transaksjonshistorikken kan slike identifiseringer være problematisk for individer som vil forbli anonym. Hvis man klarer å koble en person sammen med en offentlig adresse blir det mulig å se gjennom alle transaksjonene som personen har utført. Informasjon som lagres på blokkjeden kan være nærmest umulig å forandre på. Ettersom store mengder kryptering gjør en kryptovaluta mindre skalerbar kan det være en bedre løsning å begrense adgangen til denne informasjonen.

## 5.2 Skalerbarhet

En av de største ulempene ved eksisterende blokkjedeteknologi er skalerbarhet. Desentraliserte kryptovalutaer har blitt mer populær i det siste som har ført til en økning i antall transaksjoner. For noen kryptovalutaer er dette problematisk siden antallet transaksjoner er større enn det blokkjeden kan behandle og kostnadene forbundet med verifisering av transaksjoner øker betraktelig. Sentraliserte betalingssystemer har langt større prosesseringskapasitet enn teknologien som benyttes av desentraliserte kryptovalutaer

(Norges Bank, 2018). For at digitale sentralbankpenger skal kunne baseres på desentralisert teknologi må den kunne skaleres godt. Vi vil dermed se på hva som avgjør skalerbarheten til blokkjeden og hvilke løsninger som kan implementeres.

### 5.2.1 Transaksjonsvolum

Transaksjonsvolumet en blokkjede kan behandle avhenger direkte av blokkstørrelse og tiden det tar for systemet å produsere en blokk (Klarman, Basu, Kuzmanovic, & Sirer, 2018). Disse innstillingene bestemmes i stor grad av hvor mye prosesseringskraft man er villig til å «sløse» og sikkerheten man ønsker å opprettholde i nettverket. Det er utfordrende å forandre disse innstillingene i ettertid da store forandringer i protokollen kan resultere i en «hard fork», som kan gjøre ugyldige transaksjoner gyldig eller motsatt (Zamyatin, et al., 2018). Noder i Bitcoin-nettverket bruker for eksempel 10 minutter på å produsere én blokk (Mauro, Sandeep, Chhagan, & Ruj, 2017). Dette begrenser valutaen til 7 transaksjoner per sekund.

Blokkstørrelsen avgjør antall transaksjoner som kan lagres i en blokk. Dette har også en effekt på tiden det tar for en blokk å forplante seg i nettverket. Økt størrelse til en blokk har en lineær effekt på forplantningstiden<sup>21</sup> (Klarman, Basu, Kuzmanovic, & Sirer, 2018). Høyere forplantningstid øker risikoen for at transaksjoner ikke blir inkludert i blokkjeden. Når en transaksjon blir inkludert i en blokk som ikke refererer til den nyligste blokken vil blokken være en del av side-kjeden (Klarman, Basu, Kuzmanovic, & Sirer, 2018). På grunn av dette må brukere ofte vente til flere blokker har blitt lagt til i kjeden for å være sikker på at transaksjonen ikke vil bli fjernet fra blokkjeden. Dette kan gjøre den teknologiske løsningen lite praktisk som et betalingsmiddel. Ved en innføring av digitale sentralbankpenger må teknologien tilrettelegge for et umiddelbart oppgjør.

En høyere forplantningstid fører til at flere noder blir ekskludert fra nettverket. Noder må kunne motta blokker fort slik at de kan bruke den nyeste versjonen av blokkjeden. Høyere forplantningstid fører til at flere noder jobber med en utdatert versjon av blokkjeden og lager ugyldige blokker som sløser prosesseringskraft. Basert på dette vil en økning i blokkstørrelse eller reduksjon av tiden det tar å produsere en blokk være ineffektive løsninger for skalering av blokkjeden.

---

<sup>21</sup> Begrepet forplantningstid er oversatt fra det engelske begrepet «Propagation time».

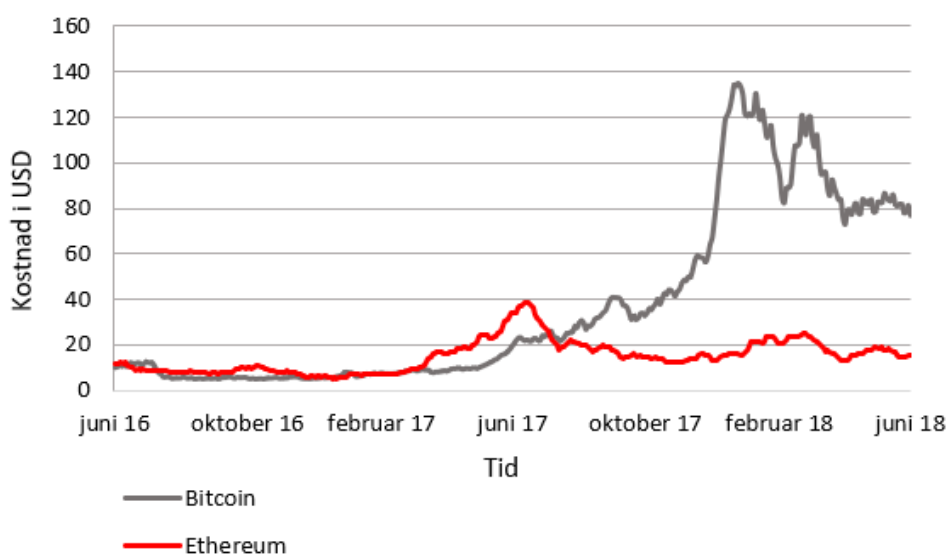


Det eksisterer flere metoder som benyttes til å øke antall transaksjoner en blokkjede kan prosessere, men de skaper andre svakheter. Ethereum for eksempel bruker «sharding» som gjør det mulig for utvinnere å verifisere transaksjoner ved å bruke mindre deler av blokkjeden; noder bruker deler av hovedboken og godkjenner transaksjoner som tilhører den delen (Gao & Nobuhara, 2017). Svakheten er at man må stole på andre noder. Dette er utfordrende for desentraliserte kryptovalutaer da det er risikabelt å stole på de andre nodene i nettverket.

## 5.2.2 Verifiseringskostnader

Kryptovalutaer som Bitcoin og Ethereum bruker Proof-of-Work til verifisering av transaksjoner. Når teknologien forbedres tar det kortere tid å komme frem til en løsning på den matematiske oppgaven. Ettersom teknologien stadig forbedres må vanskelighetsgraden øke for å gjøre det vanskelig å angripe systemet. Dette fører til en økning i verifiseringskostnader som følge av høy forbruk av elektrisitet.

Figur 5.2.2-1<sup>22</sup>. Verifiseringskostnad per transaksjon



Grafen (se Figur 5.2.2-1) viser at verifiseringskostnadene per transaksjon har vært høye de to siste årene for både Ethereum og Bitcoin. For Ethereum ligger nå kostnaden per transaksjon

<sup>22</sup> Tallene for Bitcoin er hentet fra Blockchain (2018), mens tallene for Ethereum er hentet fra Etherscan (2018) og er generert ved å ta utstedelse av valuta og transaksjonsgebyrer delt på antall transaksjoner. Det er benyttet 5-dagers glidende gjennomsnitt.

på rundt 18 USD, som er høyt i forhold til eksisterende betalingsløsninger. Bitcoins verifiseringskostnadene har økt betraktelig det siste halvåret som skyldes i stor grad dårlig skalerbarhet. Når antallet transaksjoner i nettverket overstiger prosesseringskapasiteten vil noder prioritere transaksjoner som gir størst belønning. For å få transaksjonene sine verifisert måtte brukere betale større verdier, som resulterte i at noder ble belønnet med betydelige transaksjonskostnader i tillegg til valutautstedelser. Kostnaden per transaksjon for Bitcoin har blitt mindre som forventes å være på grunn av implementering av «Lightning Network». Verifiseringskostnadene til Ethereum har vært mer stabil som antas å være på grunn av bedre prosesseringskapasitet enn Bitcoin.

For digitale sentralbankpenger er det mer gunstig å gjøre verifiseringen mer sentralisert. Hvis verifiseringen begrenses til noen bestemte institusjoner kan verifiseringskostnader reduseres betraktelig foruten en kraftig økning i risikoen for sikkerhetsbrudd. Dette forutsetter at man kan stole på slike institusjoner og holde dem ansvarlige for eventuelle brudd på retningslinjene. Dette er langt mer utfordrende for desentraliserte kryptovalutaer.

## 5.3 Kostnader

Lavere transaksjonskostnader er en av fordelene som desentraliserte kryptovalutaer hevder å ha. Dette oppnås ved eliminering av en sentral tredjepart som verifiserer transaksjonene. Det betyr ikke nødvendigvis at denne måten å utføre transaksjoner på er billigere totalt sett, ettersom vi har sett at verifiseringskostnadene til desentraliserte kryptovalutaer kan være høy. Vi vil dermed se på kostnader for ulike deler av samfunnet ved ulike betalingsmetoder og ved desentralisert teknologi.

### 5.3.1 Bedriftenes kostnader

En av de mest populære betalingsmetodene i Norge er kortbetaling. De samlede kostnadene for bedrifter som brukte kortbetalinger i 2013 utgjorde 3 milliarder kroner (Norges Bank, 2014). Bedrifter som ønsker å motta kortbetalinger må inngå en avtale med en innløser. For å inngå en slik avtale må bedriften tilfredsstillе alle krav som er satt i kjøpsloven. Kostnaden som påføres bedriften ved bruk av NETS sine betalingsløsninger, varierer mellom 1,5 til 1,8 prosent av alle transaksjonene (Nets, u.d.). Noen innløser krever også et etableringsgebyr. I tillegg må bedrifter inngå en avtale med en leverandør som lager kortbetalingsløsninger. Dette er aktører som DIBS, NETS og PayPal. Prisen bedrifter må betale for denne tjenesten

---

varierer basert på faktorer som for eksempel antall transaksjoner per måned, prisen per transaksjon og samlet omsetning.

I en undersøkelse gjennomført av Norges Bank i 2013 utgjorde kostnadene ved kontantbetalinger for bedrifter i Norge 348 millioner kroner (Norges Bank, 2014). Dette er kostnader som innebærer klargjøring og avstemming av kasser, håndtering/transport av kontanter, innskudd og uttak i bank og tidskostnader. Selv om de totale kostnadene var mindre enn ved kortbetalinger (3 milliarder) hadde kontanter en høyere kostnad per enhet ifølge undersøkelsen.

Mobilbetaling er en annen form for betaling som har blitt populær de siste årene. Vipps tilbyr bedrifter betalingsløsninger hvor transaksjonskostnadene er på rundt 1,75 prosent av kjøpsbeløpet og mellom 2 til 3,5 prosent ved handel på internett (Vipps, u.d.). Transaksjonskostnadene for nettbutikkene settes på bakgrunn av omsetningen til nettbutikken. Desto høyere omsetning, desto lavere transaksjonskostnader. Siden Vipps er en kostbar applikasjon for banker, forventes det at kunder vil belastes for tjenesten i fremtiden.

Desentraliserte kryptovalutaer påfører bedrifter lave transaksjonskostnader som følge av at kostnadene dekkes direkte av forbrukerne. For å unngå volatiliteten til desentraliserte kryptovalutaer brukes aktører som BitPay til å konvertere kryptovaluta til tradisjonelle penger umiddelbart. Det er en betalingsløsning som gjør det mulig for bedrifter å ta betalt med Bitcoin og Bitcoin Cash. Denne tjenesten påfører bedrifter en transaksjonskostnad som tilsvarer 1 prosent av kjøpsverdien (BitPay, u.d.). Digitale sentralbankpenger som utformes på desentralisert teknologi kan dermed være et billigere alternativ *for bedrifter*.

### **5.3.2 Bankenes kostnader**

I 2013 var bankenes kostnader tilknyttet betalinger på rundt 8,5 milliarder kroner (Norges Bank, 2014). Disse kostnadene er forbundet med kontantrelaterte tjenester, kortbetalinger og girobetalinger. De største kostnadene for banker ved bruk av desentralisert teknologi forventes å være kostnader forbundet med verifisering av transaksjoner.

Kontantrelaterte tjenester stod for 1,8 milliarder kroner av bankenes samlede kostnader i 2013 (Norges Bank, 2014). Dette er kostnader tilknyttet vedlikehold/drift av minibanker, manuelle innskudd og uttak i skranke, nattsafer, automatiserte innskudds- og uttaksautomater og vekslinger. Etersom kontanter utgjør en liten del av pengene våre gir det en høy

enhetskostnad. Det kan dermed sies at Norge betaler en høy pris for de kontantrelaterte tjenestene.

Girobetalinger utgjorde 3,6 milliarder kroner av bankenes kostnader i 2013 (Norges Bank, 2014). Den største delen av disse kostnadene er knyttet til behandling av elektroniske giroer. Dette inkluderer kostnader som betalinger til leverandører, prosessering og avregning av transaksjoner, vedlikehold av betalingsprodukter, rådgivning og andre faste kostnader. Girobetalinger hadde en betydelig lavere enhetskostnad for banker enn kontantrelaterte tjenester.

Kostnader forbundet med kortbetalinger var på 3,1 milliarder kroner i 2013 (Norges Bank, 2014). Mesteparten av disse kostnadene tilknyttes internasjonale kortleverandører som VISA og Mastercard. Banker må betale gebyrer til kortselskaper basert på antall utstedte kort, korttype og hvor mange kortbetalinger som blir utført. Betalingsapplikasjoner er basert på internasjonale betalingskort som underliggende betalingsinstrument som gjør betalingsapplikasjoner dyre for banker (Norges Bank, 2017). Vipps, for eksempel, kan være en billig løsning for kundene men bankene tapte penger på den i 2017 (Hoemsnes & Eriksen, 2017).

Kortbetalinger hadde den laveste kostnaden per transaksjon. For at desentralisert teknologi skal være et billigere alternativ for banker kan ikke kostnaden per transaksjon overstige 2,05 kr. De største desentraliserte kryptovalutaene i dag bruker konsensusprotokoller som er basert på prosesseringskraft. Dette fører til at kostnaden per transaksjon blir langt høyere enn ved kortbetalinger. Slike konsensusprotokoller er dårlig egnet for digitale sentralbankpenger.

### **5.3.3 Brukernes transaksjonskostnader**

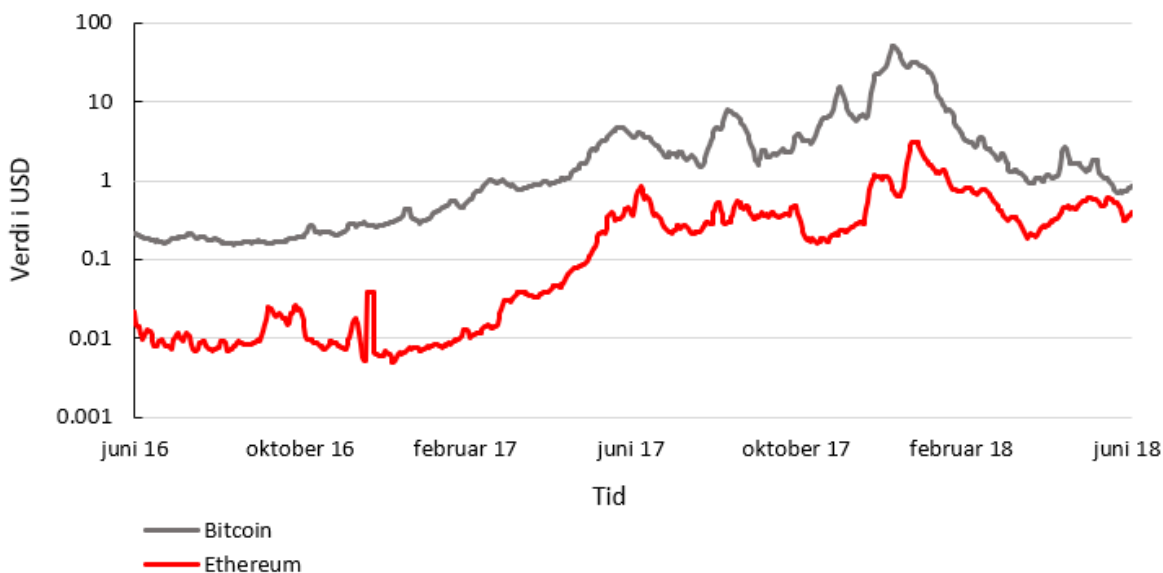
Den mest populære betalingsapplikasjonen i Norge er Vipps. Overføringer som er under 5000 kr påfører ingen transaksjonsgebyr, mens beløp over 5000 kr koster 1 prosent av beløpet (Vipps, u.d.). For å unngå kostnader ved større innenlands betalinger benyttes nettbanken. En overføring av penger mellom kunder i samme bank er gratis og umiddelbar, mens overføring til kunder i andre banker tar lenger tid, med mindre «straksbetaling» er benyttet. Beløpet som kan overføres ved denne type betaling er begrenset og noen banker tar betalt for tjenesten (Sparebanken Møre, 2018). Det er dermed lite sannsynlig at desentralisert teknologi vil tilføre fordeler i form av lavere transaksjonskostnader for brukerne. Det kan ha

en indirekte påvirkning hvor varer koster mindre som følge av lavere transaksjonskostnader for butikker eller lavere kortgebyr/walletgebyr som følge av lavere kostnader for bankene.

Overføring av penger til utlandet er mindre effektivt. En bruker betaler transaksjonskostnader basert på hvilken bank pengene sendes til og fra. Ventetiden avhenger av hvilke banker som samarbeider med banken pengene sendes fra. Pengene går ofte gjennom flere korresponderende banker som øker transaksjonskostnaden. Ventetiden kan være opptil 8 dager som er langt tregere enn ved bruk av desentralisert teknologi. Videre kan kostnadene reduseres dersom desentralisert teknologi tas i bruk. Dette avhenger av at andre land tar i bruk tilsvarende teknologi.

Transaksjonstiden til Bitcoin avhenger av hvor høye transaksjonskostnader brukeren er villig til å betale og hvor mye aktivitet det er i nettverket. Selv om Bitcoin er den mest utbredte kryptovalutaen er transaksjonene ineffektiv i forhold til andre store kryptovalutaer. Bitcoin-transaksjoner tar 1 time å gjennomføre og kostnaden pleier å ligge rundt 1 USD. Ethereum har forbedret på deler av teknologien som blir brukt av Bitcoin. Transaksjonstiden og transaksjonskostnadene pleier å være lavere og ligger på rundt 1 minutt og 0,5 USD (se Figur 5.3.3-1).

Figur 5.3.3-1<sup>23</sup>. Gjennomsnittlig gebyr per transaksjon



<sup>23</sup> Tall for Bitcoin er hentet fra Blockchain (2018) og generert ved å ta verdien av totale transaksjonskostnader og dele på antall transaksjoner. Tall for Ethereum er hentet fra Etherscan (2018) og generert ved å ta verdien av totale transaksjonskostnader og dele på antall transaksjoner. Det er benyttet 5-dagers glidende gjennomsnitt.

Transaksjonskostnadene for de to valutaene har variert mye det siste året. Stor økning i transaksjonsvolum har ført til at brukere har betalt mer for å få transaksjonene sine verifisert. Siden desentraliserte kryptovalutaer hadde begrensninger på hvor mange transaksjoner som kunne gjennomføres per sekund førte det til at utvinnere inkluderte transaksjonene som førte til størst belønning. Brukere måtte dermed betale mer for at transaksjonene skulle utføres raskt.

### **5.3.4 Samfunnets transaksjonskostnader**

Noen av tjenestene i samfunnet kan effektiviseres ved hjelp av desentraliserte applikasjoner. En fordel med blokkjedeteknologi er at transaksjoner kan utføres uten en tredjepart og lagres på en måte som gjør de vanskelig å forandre i ettertid. I følge Norges Bank (2016) har det blitt foreslått å bruke teknologien til registrering av eiendommer, verdifulle gjenstander og til å gjennomføre valg.

Smart contracts er en desentralisert applikasjon som har fått mye oppmerksomhet. Når en kontrakt blir inngått mellom to parter er den irreversibel. En slik kontrakt er automatisert og kan gjøre det mulig å programmere hvordan penger brukes i samfunnet. Kostnadene forbundet med beskatning kan reduseres ved å bruke smart contracts til å automatisere beskatningen og forbedre overholdelse av regler (Csiro, 2017). Da størrelsen på den svarte økonomien i Norge er vesentlig kan det føre til betydelige inntekter for staten. Dette vil avhenge av i hvilken grad myndighetene har tilgang til informasjonen lagret på en blokkjede.

Implementering av smart contracts har vekt stor interesse ved aksjehandel. Ved bruk av desentraliserte applikasjoner kan aksjetransaksjoner foregå nesten umiddelbart. På denne måten kan man bli kvitt mellommenn som for eksempel meglerhus. I dag blir dette utviklet av blant annet Australian Securities Exchange (ASX, 2018).

## **5.4 Volatilitet**

Volatilitet er et begrep som brukes til å beskrive hvor mye verdien på et finansielt aktivum varierer over tid sammenlignet med en annen indeks. Desto mer et finansielt aktivums verdi varierer, desto høyere volatilitet har den. Foreløpig har valutaer som bruker desentralisert teknologi en høy volatilitet som skaper flere utfordringer knyttet til klassifisering av penger. For at en valuta skal klassifiseres som penger må den oppfylle tre krav: Den skal kunne

---

brukes som et verdimål, et byttemiddel og et verdioppbevaringsmiddel. Høy volatilitet til en valuta fører til at disse kravene ikke opprettholdes. Digitale sentralbankpenger vil dermed ikke regnes som valuta hvis de innehar samme grad av volatilitet.

### 5.4.1 Pengenes egenskaper

En av pengenes egenskaper er dens funksjon som verdioppbevaringsmiddel. Dette gjør det mulig å oppbevare penger uten at de mister verdi. En av grunnene til at kryptovalutaene har blitt så populære er fordi de er veldig volatile, noe som kan føre til store fortjenester. Kryptovalutaer brukes av de fleste nordmenn som et investeringsmiddel. Av de 200 000 som eier den er det bare 16 prosent som har benyttet den til betaling eller pengeoverføring (Menon Economics, 2018). Risikoen for et stort fall i valutaens verdi er betydelig større enn for tradisjonelle valutaer. Videre må valutaen kunne brukes som betalingsmiddel i fremtiden. Hvis man forventer at ingen vil akseptere en valuta som betalingsmiddel i fremtiden vil det redusere dens funksjon som verdioppbevaringsmiddel.

Penger fungerer som byttemiddel. Dette reduserer kostnader forbundet med bytte av varer og tjenester. For at en betalingsløsning skal være et effektivt byttemiddel må betalingsmiddelet være akseptert av alle. Kryptovalutaer er lite effektiv ettersom bare en liten andel av butikker godtar betalinger i form av kryptovaluta. Selv om transaksjonskostnadene kan være mindre kan det være risikabelt for butikker å akseptere slike betalinger. På grunn av høy volatilitet vil butikker som mottar betalinger med kryptovaluta utsettes for en risiko ved at verdien til mottatte betalinger reduseres.

For at en valuta skal klassifiseres som penger må den også fungere som et verdimål. Et verdimål brukes som en numerisk måleenhet av markedets varer, transaksjoner og andre tjenester. For at et betalingsmiddel skal fungere som et godt verdimål må det være delelig, ombyttelig og tellbart (Vavrinec, 2017). Kryptovalutaer som Bitcoin er fullstendig delelig og tellbar, men ikke helt ombyttelig. En valuta som gjør transaksjoner synlig for andre gjør det mulig å se hvor pengene kommer fra. Noen utvekslingstjenester blokkerer for eksempel brukere som har anskaffet Bitcoin på en tvilsom måte. På denne måten kan noen BTC<sup>24</sup> ha lavere verdi basert på hvordan de ble anskaffet.

---

<sup>24</sup> Den monetære verdien til Bitcoin.

## 5.4.2 Tilbud

Volatiliteten til desentraliserte kryptovalutaer avhenger av tilbud og etterspørsel. Høy volatilitet skyldes i stor grad eksterne faktorer som for eksempel omtale i medier og reguleringer.

Tilbudet av digitale valutaer er annerledes enn ved tradisjonelle valutaer. Valutaer som Bitcoin, utsteder nye valutaer bare når blokker legges til i blokkjeden. Det maksimale antallet BTC i nettverket er begrenset som fører til at utvinnere på et tidspunkt bare vil belønnes med transaksjonskostnader. Ethereum utsteder valuta på samme måte, men det maksimale antallet ETH<sup>25</sup> er ikke begrenset.

Lavere volatilitet kan føre til at digitale sentralbankpenger får de samme egenskapene som tradisjonelle penger. Det er imidlertid lite sannsynlig at digitale sentralbankpenger kan baseres på samme teknologi som Bitcoin og Ethereum benytter. Da nye kryptovaluta bare utstedes når blokker tilføres kjeden er systemet veldig rigid. Det ville ha redusert sentralbankens muligheter til å styre konjunktorene i landet. Digitale sentralbankpenger basert på blokkjedeteknologi må dermed tilpasses slik at sentralbanken har minst like mye fleksibilitet i forhold til utøvelse av pengepolitikken.

## 5.5 Sikkerhet

Stadig flere transaksjoner blir utført ved hjelp av digitale betalingsløsninger. Dette har gjort overføringer og betalinger mer praktisk og redusert kostnader forbundet med kontanter. Samtidig har dette skapt utfordringer knyttet til cyberkriminalitet. En undersøkelse fra 2017 viser at den finansielle industrien har høyest gjennomsnittlig kostnad per selskap forbundet med cyberkriminalitet (Accenture, 2017). I tillegg er det forventet at antall cyberangrep vil øke i fremtiden. Kriminelle aktører kan også angripe forbrukerne som gjør det viktig å lage sikre verktøy for betaling og verdioppbevaring. Vi vil dermed se på sikkerheten til eksisterende løsninger og sammenligne de med løsninger som kan oppnås ved bruk av desentralisert teknologi.

---

<sup>25</sup> Den monetære verdien til Ethereum.



---

### 5.5.1 Tradisjonell infrastruktur

I et sentralisert system er transaksjoner godkjent av en sentral tredjepart. Et slikt system praktiseres av Norge. Den finansielle infrastrukturen er tett sammenvevd og et angrep som blir utført på et medlem av systemet kan ha konsekvenser for hele systemet. Et godt eksempel på sikkerhetsbrudd som følge av et sentralisert system er cyberangrepet i 2016 som resulterte i et tap på 81 millioner dollar for Bangladesh sin sentralbank. Dette ble gjort ved å angripe noen av de mindre bankene først og bruke legitimasjonen deres til å sende SWIFT forespørsler til større banker i utlandet (Lewis, 2018). Noen av disse forespørslene ble godkjent som resulterte i store gevinster for hackere.

Sikkerheten til en finansiell institusjon avhenger også av ansatte som jobber der. En av de siste trendene innenfor cyberkriminalitet er å skaffe påloggingsinformasjonen til de ansatte ved å bruke verktøy som «phishing email», «keystroke loggers» og «remote access trojans». (Symantec, 2012). Selv om det er mulig å informere de ansatte om disse trendene vil kriminelle aktører finne nye metoder å skaffe sensitiv informasjon på. I tillegg kan sikkerhetsbrudd forekomme av ansattes bevisste handlinger.

På samme måte som i desentraliserte systemer må man betale en pris for cybersikkerhet. Banker bruker tre ganger så mye penger på sikkerhet enn selskaper i andre industrier (Lewis, 2018). En av grunnene er økt antall angrep rettet mot finansielle institusjoner og fare for store økonomiske tap. Faren for store tap fører til økte investeringer i cybersikkerhet. En annen grunn til at det investeres i cybersikkerhet er nye reguleringer. EUs nye personvernforordning stiller for eksempel nye sikkerhetskrav til virksomheter som behandler personopplysninger. Hvis kravene ikke overholdes kan virksomheter risikere å måtte betale opptil 4 prosent av omsetningen eller 20 millioner euro (PwC, 2017). Sikkerhetskravene blir høyere med tiden, men hackere blir også mer sofistikerte og antall angrep forventes å øke i fremtiden. Det har også blitt estimert at kostnadene av å implementere og opprettholde cybersikker infrastruktur vil øke med over 40 prosent innen 2025 (BDO, 2017). Dette kan gjøre sikkerhetstiltak som praktiseres av desentraliserte kryptovalutaer enda mer nyttig i fremtiden.

### 5.5.2 Desentralisert infrastruktur

De to største kryptovalutaene i dag bruker kryptografi kombinert med blokkjede for å gjøre transaksjonene sikker. Valutaer som Bitcoin og Ethereum bruker en desentralisert struktur

som lar alle brukere verifisere og lagre transaksjoner utført av andre. Det som gjør infrastrukturen til desentraliserte valutaer sikker er protokollene som brukes til verifisering av transaksjonene.

Protokollen som brukes til verifisering av Ethereum og Bitcoin er Proof-of-Work. Den sørger for at en person som har godkjent transaksjoner har bevis for at han har utført mye arbeid. Den eneste måten å skaffe et slikt bevis på er å bruke store mengder prosesseringskraft. Dersom en aktør lykkes i å skaffe mer enn 50 prosent av prosesseringskraften i systemet kan han utføre et vellykket angrep. Selv om Proof-of-Work er en sikker løsning har den svakheter knyttet til kostnader og skalering. Siden verifisering avhenger av prosesseringskraft resulterer det i store elektrisitetskostnader. I 2018 var Bitcoins estimerte årlige kostnader av utvinning på over \$3 milliarder (Digiconomist, 2018). Mengden prosesseringskraft brukt må øke for å opprettholde samme nivå av sikkerhet. Dette fører til at kostnadene øker betraktelig. På grunn av dette har noen valutaer implementert løsninger som i mindre grad er basert på prosesseringskraft.

Proof-of-Stake er en protokoll som har fått mye oppmerksomhet på grunn av dens sikkerhet og lave kostnader. Ethereum vil bytte til Proof-of-Stake som følge av høye elektrisitetskostnader forbundet med Proof-of-Work. Da det finnes mange varianter av Proof-of-Stake er det også variasjon i graden av sikkerhet og prosesseringskostnader. Proof-of-Stake benyttes allerede av mindre valutaer som Peercoin og Blackcoin. I motsetning til Proof-of-Work er prosessen i en større grad basert på insentiver. Proof-of-Stake belønner brukere for å godkjenne gyldige transaksjoner og straffer dem for å godkjenne ugyldige transaksjoner. Dette gjør at man kan redusere prosesseringskostnadene betraktelig. I følge Ethereums grunnlegger Vitalik Buterin (2017) vil utføring av et angrep være for kostbart til å vinne noe på det. En slik protokoll er mye bedre egnet for digitale sentralbankpenger siden kostnadene ved å opprettholde protokollen vil være betydelig mindre. Hvis tilgangen til verifisering av transaksjonene begrenses, kan kostnadene reduseres ytterligere, men graden av sikkerhet vil være noe lavere.

### **5.5.3 Verdioppbevaring**

Digitale lommebøker og vekslingstjenester har en betydelig lavere sikkerhet enn infrastrukturen til desentraliserte kryptovalutaer. Ved flere anledninger har brukere mistet store verdier av Bitcoin som følge av hackerangrep. Som vi har sett på tidligere finnes det

ulike typer digitale lommebøker som tilbyr ulik grad av sikkerhet. Graden av sikkerhet avhenger mye av hvor den private nøkkelen oppbevares. Hvis den digitale lommeboken er i form av program på en pc, på nett eller på mobilen kan graden av sikkerhet være lavere ettersom slike gjenstander ofte er koblet til internett. Digitale lommebøker i form av papir eller USB kan oppbevares uten å være koblet til internett og er et sikrere alternativ.

På samme måte som med eksisterende løsninger er graden av sikkerhet avhengig av brukeren. Hvis brukeren ikke er forsiktig vil det føre til lav sikkerhet uansett hvilket verdioppbevaringsmiddel man bruker. En ulempe med digitale lommebøker er at brukeren mister verdien lagret i lommeboken dersom den private nøkkelen går tapt. Ved de eksisterende digitale løsningene, som nettbank og bankkort er det opprettet løsninger slik at forbrukerne fremdeles får tilgang til verdien på kontoen dersom innloggingspassordet eller PIN-koden er glemt.

Innholdet i digitale lommebøker er sikret ved hjelp av kryptografi og kan være et sikkert alternativ hvis det oppbevares et sikkert sted. I følge rapporten til Norges Bank (2018) er lavere sikkerhet ved digitale lommebøker en av utfordringene som gjør desentralisert teknologi lite egnet for digitale sentralbankpenger. Det finnes ulike digitale lommebøker som kan brukes basert på graden av sikkerhet man vil opprettholde. Det er ingen grunn til å tro at lommebøker i form av papir eller USB gir lavere sikkerhet enn bankkort hvis de oppbevares på en forsvarlig måte.

## 6. Utforming av norsk digital valuta

Vi vil i denne delen ta for oss hvordan en norsk digital valuta kan se ut. Vi vil ta i bruk alle de foregående delene for å konkludere med hvem som bør utstede digitale sentralbankpenger, hvilke implikasjoner den vil ha for sentralbankens likviditetsstyring og hvilken teknologisk utforming vi anbefaler.

### 6.1 Sentralbankens oppgaver

Da nasjonal digital valuta gjerne omtales som «digitale sentralbankpenger<sup>26</sup>» er det tilsynelatende allerede slått fast at det er sentralbanken som eventuelt skal utstede den nasjonale digitale valutaen. Prinsipielt kunne oppgaven også vært delegert til private aktører.

Sentralbanken har imidlertid høy tillit og troverdighet i samfunnet, som er bygget opp igjennom flere hundretalls av år. Dette fører til at sentralbanken står i en særskilt posisjon og lettere kan bygge troverdighet og tillit til en ny norsk digital valuta.

For å sikre troverdighet og tillit til digitale sentralbankpenger må vi ha tro og tillit til at utstederen vil opptre forsvarlig i fremtiden. Sentralbanken antas å vektlegge fremtiden i større grad enn private aktører, og ta i betraktning hvilke ringvirkninger ulike bestemmelser vil ha på pengepolitikken på både kort og lang sikt. En privat aktør antas å ha større insentiver til å fravike optimal pengepolitikk og legge mindre vekt på eventuelle ringvirkninger for å sikre en høyere kortsiktig gevinst.

En innføring av digitale sentralbankpenger vil føre til at sentralbanken må opprette nye avdelinger og funksjoner som den ikke innehar i dag. Hvor stor denne endringen vil være avhenger av hvordan digitale sentralbankpenger settes opp og hvordan de utformes. Det antas å være lite sannsynlig at sentralbanken vil ønske å ta på seg store administrative oppgaver knyttet direkte til forbruker, som kundeservice, utvikling av betalingsløsninger, osv. Det vil endre sentralbankens rolle i samfunnet og således endre samfunnets oppfatning av hva sentralbanken er. Videre kan det føre til uønskede effekter knyttet til sentralbankens omdømme, dersom det skulle oppstå problemer med enkelte av deres tjenester. Vi kan ikke

---

<sup>26</sup> Omtales også som «elektroniske sentralbankpenger».

risikere at tilliten og troverdigheten til sentralbanken reduseres. Vi vil dermed anbefale at forbrukerne vil ha en indirekte kobling til sentralbanken, som vil føre til at sentralbanken i større grad kan konsentrere seg om dens hovedoppgave: å sikre den økonomiske stabiliteten i Norge.

Sveriges Riksbank (2017) anser i hovedsak to modeller til å være relevante for utformingen av digitale sentralbankpenger: (1) en verdibasert modell<sup>27</sup> og/eller (2) en registrerbar modell<sup>28</sup>. Rapporten til Norges Bank (2018) deler den Svenske Riksbanken sine tanker om to tenkbare modeller for digitale sentralbankpenger. Både rapporten til Sveriges Riksbank og Norges Bank påpeker at administrering av digitale sentralbankpenger i større eller mindre grad kan overlates til private aktører.

### **6.1.1 Likviditetsstyring ved innføring av digitale sentralbankpenger**


Vi har tidligere i oppgaven sett på sentralbankens likviditetsstyring. Vi vil ta et tilbakeblikk og vurdere hvordan innføring av digitale sentralbankpenger vil påvirke likviditetsstyringen til sentralbanken.

Innehaverne av digitale sentralbankpenger vil ha en fordring direkte på sentralbanken. Digitale sentralbankpenger vil således ende opp som en gjeldspost i sentralbankens balanse (se Figur 6.1.1-1).

---

<sup>27,28</sup> Se rapport fra Norges Bank og Sveriges Riksbank for en nærmere beskrivelse av disse to modellene.

Figur 6.1.1-1. Utvalgte poster i en forenklet oppstilling av sentralbankens balanse (inkludert ny post for digitale sentralbankpenger)

	Sentralbankens balanse	
	Eiendeler	Gjeld
	Utlån til banker	Bankinnskudd ( reserver)
	Verdipapirer	Innskudd fra staten
	Valutareserver	Kontanter
		Digitale sentralbankpenger

Kilde: Tabellen er inspirert av Aamodt og Lerbak (2013) sin oppstilling av sentralbankens balanse.

Dersom en kunde ønsker å flytte penger fra innskuddskonto i banken til digitale sentralbankpenger, vil reserver på bankenes foliokontoer reduseres og posten «Digitale sentralbankpenger» vil økes. Vi får samme effekt som for kontantene; at mengden bankreserver reduseres.

Dersom bankene ikke har nok reserver på foliokonto i sentralbanken til å dekke etterspørselen etter digitale sentralbankpenger, vil banken måtte låne reserver av sentralbanken (Sveriges Riksbank, 2017). Dette er helt tilsvarende med at banken må låne reserver hvis de ikke har dekning på foliokontoen for å gjennomføre betalingstransaksjoner i våre dager. Alternativt må banken selge eventuelle investeringer slik at etterspørselen etter digitale sentralbankpenger kan tilfredsstilles.

Dersom bankene må låne reserver av sentralbanken vil posten «Utlån til banker» økes i samme størrelse som økningen i posten «Digitale sentralbankpenger». For bankenes balanse vil innskuddet fra kundene reduseres og erstattes med lån fra sentralbanken.

Dersom banken har tilstrekkelig med reserver hos sentralbanken vil ikke sentralbankens balanse endres i stor grad. Endringen i sentralbankens balanse vil komme av at posten «Bankinnskudd» vil reduseres og posten «digitale sentralbankpenger» vil økes. Verdien som overføres til digitale sentralbankpenger vil dermed gå fra å være en fordring mot banken til å bli en fordring mot eier av digitale sentralbankpenger.

---

Sentralbanken styrer blant annet mengden bankreserver for å nå målet med å holde de kortsiktige pengemarkedsrentene nær styringsrenten. Da etterspørselen etter digitale sentralbankpenger vil påvirke mengden bankreserver i banksystemet, må sentralbanken ha gode prognoser for hvor stor etterspørselen etter digitale sentralbankpenger vil bli. Digitale sentralbankpenger vil på samme måte som kontantene og innskudd fra staten være en autonom faktor, som sentralbanken ikke kan kontrollere (Sveriges Riksbank, 2017). Da digitale sentralbankpenger antas å kunne lett forflyttes mellom banker og sentralbanken, kan det bli vanskeligere for sentralbanken å finne gode prognoser for etterspørselen etter digitale sentralbankpenger. Denne slutningen stemmer godt overens med slutningen Norges Bank har trukket i sin rapport om digitale sentralbankpenger.

### **Normale tider**

I normale tider antar vi at etterspørselen etter digitale sentralbankpenger vil bestemmes ut ifra hvilke fordeler digitale sentralbankpenger gir sammenlignet med å ha pengene stående på konto i banken. Da bankinnskudd er en viktig finansieringskilde for bankene er det rimelig å anta at bankene vil forsøke å gjøre det mer attraktivt å ha pengene stående på konto i banken, for å hindre store overføringer til digitale sentralbankpenger. Da vil påvirkningen på den finansielle stabiliteten antas å være relativt liten. Denne slutningen underbygges av Sveriges Riksbank (2017) som forklarer at bankene vil være villige til å øke sine innskuddsrenter for å hindre overføringer til digitale sentralbankpenger i større utstrekning.

### **Urolige tider**

Ved innføring av digitale sentralbankpenger vil samfunnet ha enda et valg i urolige tider; pengene stående på konto kan overføres til digitale sentralbankpenger og plasseres sikkert hos sentralbanken.

Alternativet i våre dager, ved finansiell uro, er å overføre pengene til den banken vedkommende har størst tillit til. Pengene kan i prinsippet også tas ut i kontanter. De praktiske konsekvensene ved å håndtere store mengder kontanter er imidlertid lite attraktivt. Videre vil det ta tid før bankene klarer å tilrettelegge for at store pengemengder kan tas ut i kontanter, samt at det vil være risiko knyttet til sikkerheten ved å ha store kontantbeholdninger. I urolige tider vil mennesker overføre penger fra konto i banken over til digitale sentralbankpenger hvor pengene er sikkert plassert hos sentralbanken.

Ved store pengeoverføringer fra innskuddskontoene i bankene over til digitale sentralbankpenger vil bankene antageligvis tvinges til å ta opp lån fra sentralbanken. Da bankene må stille god sikkerhet bak lånene, er det en fare for at sentralbanken må utvide hva som klassifiseres som god sikkerhet i urolige tider når behovet for banklån er stort. Denne faren samsvarer med den publiserte rapporten til Norges Bank (2018).

Dyson og Hodgson (2016) påpeker at det er en risiko ved at kundene ønsker å overføre penger over til digitale sentralbankpenger også ved mindre uro i markedet. Pengene kan heller føres tilbake til konto i banken når uroen har lagt seg igjen. På den måten kan mindre uro i markedet forverres og lede til en større risiko for «bank runs» også i tider med mindre uro i markedet.

## 6.2 Teknologisk utforming

Digitale sentralbankpenger utformes basert på ønskede egenskaper. Vi har sett at skalerbarhet og kostnader er viktige faktorer i vurderingen av digitale sentralbankpenger. Vi vil foreslå en mindre desentralisert struktur, slik at digitale sentralbankpenger har en høy grad av skalerbarhet. Ved bruk av en mindre desentralisert struktur og ved å ta i bruk en verifiseringsprotokoll som ikke er drevet av prosesseringskraft, ender vi opp med digitale sentralbankpenger som har en langt lavere kostnad enn de eksisterende desentraliserte kryptovalutaene.

### 6.2.1 Verifisering

Digitale sentralbankpenger må ha en høy grad av skalerbarhet, slik at systemet kan tilpasses endringer i for eksempel antall transaksjoner som gjennomføres eller antall brukere. Ifølge Danezis & Meiklejohn (2015) er det mulig å lage en mer skalerbar valuta ved å gjøre verifiseringen av transaksjonene mer sentralisert.

Metoden som benyttes mest av desentraliserte kryptovalutaer er Proof-of-Work. Denne protokollen brukes i stor grad fordi det er ukjent hvem som faktisk produserer blokkene og om de kan stoles på. Denne løsningen bidrar til en høy grad av sikkerhet i systemet, men de høye kostnadene gjør den lite attraktiv. Vi foreslår å bruke en mindre desentralisert teknologi hvor et distribuert sett av banker eller andre finansielle aktører, heretter benevnt «finansielle utvinnere», kan verifisere transaksjoner som gjennomføres. Ettersom verifiseringen av



---

transaksjoner begrenses til disse aktørene vil det være mulig å bruke andre protokoller uten betydelige tap av sikkerhet. Ved å bruke en versjon av Proof-of-Stake hvor finansielle utvinnere er kjente, reduseres verifiseringskostnadene betraktelig. En slik protokoll er i større grad basert på insentiver og vil fungere bedre i et system hvor finansielle utvinnere kan holdes ansvarlig.

En årsak til lav prosesseringskapasitet ved blokkjeder er blant annet at noder bruker en fullstendig versjon av blokkjeden og prosesserer alle transaksjonene i den. Ved å gi finansielle utvinnere ansvar for deler av blokkjeden som de må opprettholde, kan skaleringen være enklere å oppnå (Gao & Nobuhara, 2017). Finansielle utvinnere vil deretter samle transaksjoner i delblokker og verifisere egne og noen av transaksjonene til andre finansielle utvinnere (Se Figur 6.2.2-1). Dette er vanskelig å oppnå i et fullstendig desentralisert system ettersom noder må til en viss grad stole på andre noder, hvis de ikke går gjennom alle transaksjonene i blokkjeden selv. I en undersøkelse av et lignende system hvor det ble brukt en variasjon av «Two-Phase Commit» kunne blokkjeden prosessere over 2000 transaksjoner per sekund og det tok mindre enn et sekund å bekrefte transaksjonene (Danezis & Meiklejohn, 2015). Det ble brukt 30 finansielle utvinnere i undersøkelsen og antall transaksjoner som kunne prosesseres økte lineært med antall finansielle utvinnere i systemet. Sentralbanken kan dermed tilpasse antallet finansielle utvinnere etter brukernes behov. På denne måten kan banker også overføre penger til hverandre umiddelbart uten å utsettes for kredittrisikoen som er forbundet med «straksbetalinger».

Sentralbanken må stille strenge krav til de finansielle utvinnerne for å forsikre seg om at de finansielle utvinnerne er ærlige og kan stoles på. Ved at finansielle utvinnere er autorisert av sentralbanken forutsettes det at finansielle utvinnere er troverdige og ærlige i sine godkjenninger av gyldige transaksjoner. Utvinnerne autoriseres ved å motta en digital nøkkel som signeres av sentralbanken. For at sentralbanken skal inkludere en delblokk i hovedblokken må den inneholde den digitale signaturen av den finansielle utvinneren (Danezis & Meiklejohn, 2015).

En slik protokoll er avhengig av at mesteparten av finansielle utvinnere som verifiserer en bestemt del<sup>29</sup> av blokkjeden er ærlige. Siden finansielle utvinnere vil verifisere noen av

---

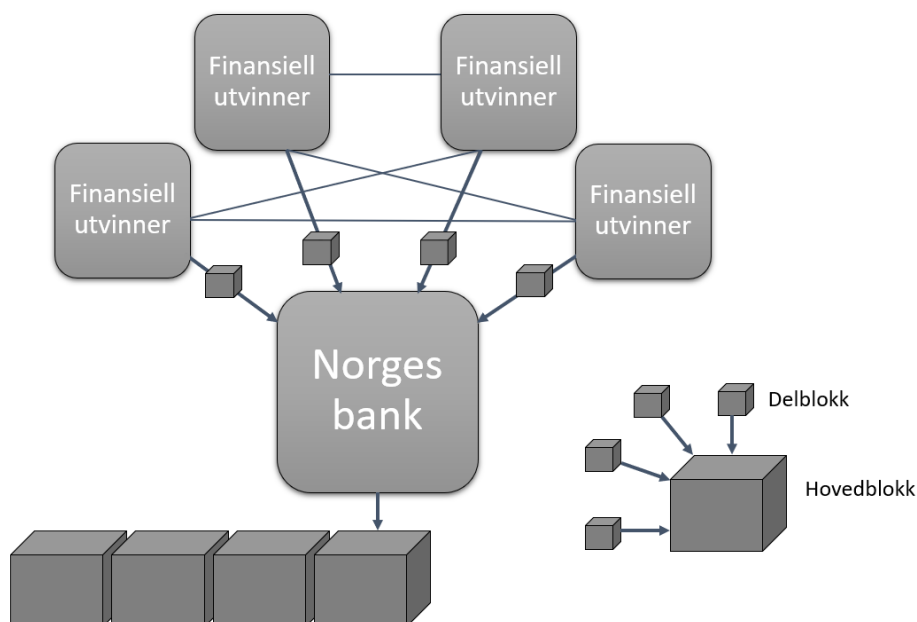
<sup>29</sup> Er ikke det samme som mesteparten av finansielle utvinnere i nettverket er ærlige.

delblokkene til de andre, kan ugyldige transaksjoner som har blitt verifisert bli oppdaget av andre utvinnere før de sendes til sentralbanken. I så fall vil den finansielle utvinneren straffes ut ifra retningslinjene som er satt av Proof-of-Stake, men også eventuelle retningslinjer som settes av sentralbanken. Utvinnere vil således ha et sterkere insentiv til å utelukkende verifisere gyldige transaksjoner. Dette vil føre til lavere verifiseringskostnader sammenlignet med de eksisterende desentraliserte kryptovalutaene.

## 6.2.2 Struktur

Finansielle utvinnere legger til transaksjoner i delblokker. Når delblokkene er revidert sendes de til sentralbanken som lager en hovedblokk ut av disse delblokkene og legger den til i blokkjeden. Denne blokkjeden inneholder alle transaksjonene og er tilgjengelig for de finansielle utvinnerne. Basert på dette er det mulig for interne brukere å bekrefte at alle transaksjonene i blokkjeden er gyldige.

Figur 6.2.2-1. Verifiseringsprotokoll for digitale sentralbankpenger



Kilde: Inspirert av Danezis og Meiklejohn (2015)

Danezis og Meiklejohn (2015) forklarer at det er mulig å opprette digitale sentralbankpenger hvor sentralbanken har full kontroll over utstedelsen av digitale sentralbankpenger. At sentralbanken har enerett til å utstede digitale sentralbankpenger sikrer en stabil pengeverdi.

---

### 6.2.3 Sikkerhet og anonymitet

Rapporten publisert av Norges Bank (2018) påpeker at en desentralisert teknologi vil gi en rekke sikkerhetsutfordringer, på bakgrunn av at digitale lommebøker kan bli stjålet eller tapt på grunn av tekniske problemer. Vi har sett at digitale lommebøker hos de eksisterende kryptovalutaene har utfordringer knyttet til tap av digitale lommebøker; dersom den digitale lommeboken går tapt, vil også verdien på den digitale lommeboken være tapt. De mest etablerte kryptovalutaene gir oversikt over alle transaksjonene på blokkjeden til eksterne brukere. Siden transaksjonene regnes som pseudonym er det umulig<sup>30</sup> for innehaveren av en tapt digital lommebok å bevise at vedkommende er den rettmessige eier av verdien. Ved å lage en kobling mellom en person og den offentlige adressen som benyttes av personen på blokkjeden kan gjøre det mulig å gjenopprette verdien dersom lommeboken mistes eller blir ødelagt. Ved at transaksjonene gjennomført med digitale sentralbankpenger lagres sentralt på blokkjeden i sentralbanken, vil sentralbanken kunne slå fast verdien som stod på den digitale lommeboken dersom den skulle gå tapt. I dette tilfellet vil en digital lommebok være like praktisk som for eksempel et bankkort. Det er mulig å gi brukere et valg om å ikke etablere en slik referanse til en offentlig adresse, som vil føre til høyere grad av anonymitet, men da må de forvente at verdien av en tapt/ødelagt digital lommebok ikke kan gjenopprettes.

Vi har imidlertid sett at det virker lite sannsynlig med digitale sentralbankpenger som er fullstendig anonym. En av fordelene ved lavere grad av anonymitet er at myndighetene får bedre oversikt over hvordan pengene brukes og bedre muligheter til skattelegging. Det svarte markedet utgjør en betydelig andel av Norges BNP (Se Svart økonomi). Hvis det blir mulig å redusere størrelsen på det svarte markedet ved introduksjon av digitale sentralbankpenger kan det føre til høyere inntekter for staten og et mer rettferdig marked for lovlydige bedrifter.

Foruten sikkerhet tilknyttet den digitale lommeboken, vil digitale sentralbankpenger forsterke sikkerheten til betalingssystemet i sin helhet. Digitale sentralbankpenger vil være mer robust og sikker enn de eksisterende betalingsløsningene som er knyttet opp mot et fåtall sentrale aktører. Ved at de finansielle utvinne vil stå for verifiseringen av transaksjonene, må en potensiell angriper lykkes i å angripe flere finansielle utvinnere på samme tid. De

---

<sup>30</sup> Det er mulig hvis den private og offentlige nøkkelen oppbevares flere steder enn i den digitale lommeboken.

desentraliserte løsningene kan dermed redusere faren ved cyberkriminalitet og kan bidra til et mer effektivt betalingssystem.

## 6.3 Sluttkommentarer

En viktig faktor som er utelatt i oppgaven, er diskusjonen rundt hvorvidt den nasjonale digitale valutaen bør gi renter eller ikke. Ut i fra vår forståelse av teknologien og vårt forslag til hvordan teknologien kan benyttes i utforming av digitale sentralbankpenger, vil det være vanskelig å sette opp et system hvor digitale sentralbankpenger gir renter<sup>31</sup>. Vi har ikke funnet en god tenkbar metode for hvordan det praktisk vil være mulig å gi rente på digitale sentralbankpenger med vår utforming basert på en mindre desentralisert teknologi. Slutningen hadde ikke nødvendigvis vært en annen, dersom det skulle være mulig å gi rente på den nasjonale digitale valutaen i vår utforming. Committee on Payments and Market Infrastructures (2018) forklarer at effektene tilknyttet en rente på digitale sentralbankpenger vil være svært vanskelig å forutse, da den vil avhenge av mange ulike faktorer og koblinger i den finansielle systemet.

De juridiske forholdene knyttet til en utstedelse av digitale sentralbankpenger basert på desentralisert teknologi er ikke behandlet i denne oppgaven. Disse problemstillingene ligger utenfor vår økonomiske tilnærming. I denne masterutredningen vil vi dermed nøye oss med å poengtere at juridiske problemstillinger kan oppstå og må tas høyde for ved en eventuell innføring av digitale sentralbankpenger.

---

<sup>31</sup> Sentralbanken må eventuelt utføre en transaksjon til alle brukere for å øke deres balanse med tilsvarende renteverdi.

---

## 7. Konklusjon

Målet vårt med oppgaven var å gi en innsikt i hvordan desentralisert teknologi kan benyttes i utformingen av digitale sentralbankpenger.

Innledningsvis påpekte vi at Norges Bank har publisert sin første rapport om temaet for å gi en overordnet innføring rundt digitale sentralbankpenger. Vi har derimot, i denne utredningen, rettet fokuset mot de teknologiske aspektene digitale sentralbankpenger kan bygges på. Digitale sentralbankpenger basert på en *fullstendig* desentralisert teknologi vil føre til høye verifiseringskostnader og en relativt lav prosesseringskapasitet. Vi er således enige med Norges Bank om at en fullstendig desentralisert teknologi kan sies å være «umoden» og ikke være et relevant alternativ for digitale sentralbankpenger på nåværende tidspunkt.

Vi har imidlertid sett at digitale sentralbankpenger kan uformes med en *mindre* desentralisert teknologi. Det er mulig å redusere kostnadene ved å benytte verifiseringsprotokoller som ikke er basert på prosesseringskraft, som for eksempel den såkalte protokollen «Proof-of-Stake». Ved å begrense verifisering av transaksjoner til bestemte finansielle utvinnere, som vil ha ansvar for deler av blokkjeden, ender vi opp med en mer skalerbar valuta. Samlet får vi en høy prosesseringskapasitet, som ytterligere kan økes ved å øke antallet finansielle utvinnere i systemet.

Den mindre desentraliserte strukturen vil være mer robust og sikrere enn de eksisterende betalingsløsningene som er knyttet opp mot en knippe sentrale aktører. Farene knyttet til blant annet cyberkriminalitet vil således reduseres.

Digitale sentralbankpenger vil ha samme effekt som kontantene i sentralbankens balanse. Dersom bankene ikke har dekning på sine foliokontoer kan bankene benytte seg av sentralbankens stående fasiliteter for å møte etterspørselen etter digitale sentralbankpenger. Det er i tider hvor behovet for banklån er stort, ettersom bankene må stille sikkerhet bak lånene, at sentralbanken kan havne i en situasjon hvor de må ta større risiko bak utlånene, da de må utvide hva som klassifiseres som god sikkerhet.

Digitale sentralbankpenger vil være enda en autonom faktor for sentralbanken og forbrukerne vil enkelt kunne forflytte verdier mellom konto i banken og digitale

sentralbankpenger. Denne fleksibiliteten til forbrukere gjør det vanskeligere for sentralbanken å finne gode prognoser for etterspørselen etter digitale sentralbankpenger.

Implikasjonene digitale sentralbankpenger vil ha for sentralbankens likviditetsstyring, samsvarer godt med slutningene som er trukket i rapporten til Norges Bank (2018).

## 8. Bibliografi

- Aamodt, E., & Lerbak, M. N. (2013). *Norges Banks balanse og resultat*. Hentet Juni 15, 2018 fra Norges Bank: [https://static.norges-bank.no/contentassets/429218c486614c2fb8a59d3953b4abd9/staff\\_memo\\_2013\\_09.pdf?v=03/09/2017123133&ft=.pdf](https://static.norges-bank.no/contentassets/429218c486614c2fb8a59d3953b4abd9/staff_memo_2013_09.pdf?v=03/09/2017123133&ft=.pdf)
- Accenture. (2017). *Cost of cybercrime study*. Hentet Juni 17, 2018 fra Accenture: [https://www.accenture.com/t20170926T072837Z\\_\\_w\\_/us-en/\\_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf](https://www.accenture.com/t20170926T072837Z__w_/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf)
- Alharby, M., & Moorsel, A. V. (2017, August). *Blockchain-Based Smart Contracts : A Systematic Mapping Study*. Hentet Juni 16, 2018 fra [https://www.researchgate.net/publication/319603816\\_Blockchain\\_Based\\_Smart\\_Contracts\\_A\\_Systematic\\_Mapping\\_Study](https://www.researchgate.net/publication/319603816_Blockchain_Based_Smart_Contracts_A_Systematic_Mapping_Study)
- Androullaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Srdjan, C. (2012). *Evaluating User Privacy in Bitcoin*. Hentet fra <https://eprint.iacr.org/2012/596.pdf>
- Antonopoulos, A. M. (2014, Oktober 7). *Mastering Bitcoin*. Hentet Juni 16, 2018 fra <https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf>
- ASX. (2018, September 19). *ASX's Replacement of CHES for Equity Post-Trade Services: Business Requirements*. Hentet Juni 15, 2018 fra <https://www.asx.com.au/documents/public-consultations/ASX-Consultation-Paper-CHES-Replacement-19-September-2016.pdf>
- Australian Securities and investment commision. (2018, Juni 13). *Cryptocurrencies - Bitcoin and other cryptocurrencies*. Hentet Juni 16, 2018 fra <https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies>
- BDO. (2017). *Cyber security in banking industry*. BDO.
- BitFury Group. (2015, September 13). *Proof of Stake versus Proof of Work*. Hentet Juni 16, 2018 fra <https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf>
- BitPay. (u.d.). *Why Accept Blockchain Payments?* Hentet Juni 16, 2018 fra <https://bitpay.com/tour>
- Blockchain. (2018, Juni 15). *Confirmed Transactions Per Day*. Hentet Juni 15, 2018 fra <https://blockchain.info/charts/n-transactions>
- Blockchain. (2018, Juni 15). *Cost per Transaction*. Hentet Juni 15, 2018 fra <https://blockchain.info/charts/cost-per-transaction>
- Blockchain. (2018, Juni 15). *Total Transaction Fees in USD*. Hentet Juni 15, 2018 fra <https://blockchain.info/charts/transaction-fees-usd>
- Buterin, V. (2016, Desember 31). *A Proof of Stake Design Philosophy*. Hentet Juni 18, 2018 fra <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>
- Buterin, V. (2017, November 5). *Using Blockchain for Supply Chain Transparency and Traceability*. Hentet Juni 15, 2018 fra <https://blockchainreview.io/blockchain-supply-chain/>
- Committe on Payments and Market Infrastructures. (2018, Mars). *Central bank digital currencies*. Hentet Juni 16, 2018 fra <https://www.bis.org/cpmi/publ/d174.pdf>
- Csiro. (2017, Mai). *Risks and opportunities for systems using blockchain and smart contracts*. Csiro.
- Danezis, G., & Meiklejohn, S. (2015, Desember 18). *Centrally Banked Cryptocurrencies*. Hentet 17 Juni, 2018 fra <https://arxiv.org/pdf/1505.06895.pdf>

- 
- DIBS. (2014). *Norsk E-handel*. Hentet Juni 16, 2018 fra [https://www.dibspayment.com/sites/corp/files/files/NO/DIBS\\_NEH\\_NO\\_2014\\_low.pdf](https://www.dibspayment.com/sites/corp/files/files/NO/DIBS_NEH_NO_2014_low.pdf)
- DIBS. (2017). *Norsk e-handel*. Hentet Juni 16, 2018 fra [https://cdn2.hubspot.net/hubfs/2204211/E-handel%20rapport/Norsk%20e-handel%202017/NO\\_DIBS\\_single\\_page\\_300.pdf](https://cdn2.hubspot.net/hubfs/2204211/E-handel%20rapport/Norsk%20e-handel%202017/NO_DIBS_single_page_300.pdf)
- Digiconomist. (2018, Mai 25). *Bitcoin Energy Consumption Index*. Hentet Juni 15, 2018 fra <https://digiconomist.net/bitcoin-energy-consumption>
- Dyson, B., & Hodgson, G. (2016, Januar). *Digital Cash - Why Central Banks Should Start Issuing Electronic Money*. Hentet Juni 16, 2018 fra Positive Money: [http://positivemoney.org/wp-content/uploads/2016/01/Digital\\_Cash\\_WebPrintReady\\_20160113.pdf](http://positivemoney.org/wp-content/uploads/2016/01/Digital_Cash_WebPrintReady_20160113.pdf)
- Etherscan. (2018, Juni 15). *Ether Historical Prices*. Hentet Juni 15, 2018 fra <https://etherscan.io/chart/etherprice>
- Etherscan. (2018, Juni 15). *Ethereum Daily Block Rewards Chart*. Hentet Juni 15, 2018 fra <https://etherscan.io/chart/ethersupply>
- Etherscan. (2018, Juni 15). *Ethereum Network Transaction Fees*. Hentet Juni 15, 2018 fra <https://etherscan.io/chart/transactionfee>
- Etherscan. (2018, Juni 15). *Ethereum Transaction Chart*. Hentet Juni 15, 2018 fra <https://etherscan.io/chart/tx>
- European Central Bank. (2012, Oktober). *Virtual currency schemes*. Hentet Juni 15, 2018 fra <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- Fexco. (u.d.). *How long do international bank transfers take?* Hentet Juni 16, 2018 fra <https://fexco.com/fexco/news/how-long-international-bank-transfers-take/#>
- Finans Norge. (2017, Mai 5). *Beredskap for kontandistribusjon - hørings svar*. Hentet Juni 16, 2018 fra [https://www.regjeringen.no/contentassets/56750b40480d4f4aae3d7e81b8ebce4c/finans\\_norge1.pdf](https://www.regjeringen.no/contentassets/56750b40480d4f4aae3d7e81b8ebce4c/finans_norge1.pdf)
- Finansdepartementet. (2002, juni 14). *Ot.prp. nr. 92 (2001-2002) - Om lov om e-pengeforetak*. Hentet Juni 15, 2018 fra <https://www.regjeringen.no/no/dokumenter/otprp-nr-92-2001-2002-/id125085/sec1>
- Finansforetaksloven. Lov av 10.april 2015 om finansforetak og finanskonsern
- Fjørtoft, T. O. (2017, Mai 19). *Norge i Eurotoppen på digitale ferdigheter*. Hentet Juni 16, 2018 fra Statistisk sentralbyrå: <https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/norge-i-eurotoppen-pa-digitale-ferdigheter>
- Forbrukerrådet. (2017, Mai 2). *Høring – beredskap for kontantdistribusjon*. Hentet Juni 15, 2018 fra <https://fil.forbrukerradet.no/wp-content/uploads/2017/05/horing-om-beredskap-for-kontantdistribusjon.pdf>
- Forbrukerrådet. (2018, Februar 6). *Kort og kontant*. Hentet Juni 15, 2018 fra <https://fil.forbrukerradet.no/wp-content/uploads/2018/02/kort-og-kontant-policynotat.pdf>
- Gao, Y., & Nobuhara, H. (2017). *A Proof of Stake Sharding Protocol for Scalable Blockchains*. APAN – Research Workshop.
- Guri, M. (2018, April 23). *BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets*. Hentet Juni 16, 2018 fra <https://arxiv.org/pdf/1804.08714.pdf>
- Hoemsnes, A., & Eriksen, M. R. (2017, April 18). *DNB har brukt 600 millioner på Vipps uten å ha tjent én krone*. Hentet Juni 17, 2018 fra <https://www.dn.no/nyheter/2017/01/27/1502/Finans/dnb-har-brukt-600-millioner-pa-vipps-uten-a-ha-tjent-en-krone>



- 
- Holden, S. (2004, Oktober). *Penger og kapitalmarkeder*. Hentet Juni 15, 2018 fra Universitetet i Oslo: [folk.uio.no/sholden/E1310/ECON1310-fnotat12-penger-okt04.doc](http://folk.uio.no/sholden/E1310/ECON1310-fnotat12-penger-okt04.doc)
- Holte, H. C. (2017, September 18). *Kampen mot arbeidslivskriminalitet: Sterkere sammen*. Hentet Juni 16, 2018 fra Skatteetaten: <https://beta.skatteetaten.no/tag/svart-okonomi/>
- Håkonsen, A., & Westby, T. (2016, Mars 8). *Vi blir stadig mer digitale i vår bankbruk*. Hentet Juni 16, 2018 fra Finans Norge: <https://www.finansnorge.no/aktuelt/sporreundersokelser/dagligbankundersokelsen1/dagligbankundersokelsen-2016/vi-blir-stadig-mer-digitale-i-var-bankbruk/>
- Klarman, U., Basu, S., Kuzmanovic, A., & Sirer, E. G. (2018, Mars). *A Scalable Trustless Blockchain Distribution Network Whitepaper*. Hentet Juni 16, 2018 fra <https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf>
- Kopczuk, W. (2006). *Tax simplification and tax compliance: An economic perspective*. Hentet Juni 16, 2018 fra Columbia University: <http://www.columbia.edu/~wk2110/bin/epi.pdf>
- Krishnan, K. (2004, Mars). *Computer Networks and Computer Security*. Hentet Juni 16, 2018 fra <http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture9.pdf>
- Kumar, A., Tople, S., Fischer, C., & Saxena, P. (2017, April 17). *A Traceability Analysis of Monero's Blockchain*. Hentet Juni 16, 2018 fra <http://www.comp.nus.edu.sg/~shruti90/papers/monero-analysis.pdf>
- Lewis, J. (2018, Februar). *Economic Impact of Cybercrime - No Slowing Down*. Hentet Juni 17, 2018 fra Csis: <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd>
- Mauro, C., Sandeep, K. E., Chhagan, L., & Ruj, S. (2017, Desember 25). *A Survey on Security and Privacy Issues of Bitcoin*. Hentet Juni 18, 2018 fra <https://arxiv.org/pdf/1706.00916.pdf>
- Menon Economics. (2018, Februar 1). *Hvem eier bitcoin?* Hentet Juni 16, 2018 fra <https://www.menon.no/hvem-eier-bitcoin/>
- Meshkov, D., Chepurnoy, A., & Jansen, M. (2017). *Revisiting Difficulty Control for Blockchain Systems*. Hentet Juni 16, 2016 fra <https://eprint.iacr.org/2017/731.pdf>
- Monaco, J. V. (2015, Mai 26). *Identifying Bitcoin users by transaction behavior*. Hentet Juni 16, 2018 fra [https://www.researchgate.net/publication/277248535\\_Identifying\\_Bitcoin\\_users\\_by\\_transaction\\_behavior](https://www.researchgate.net/publication/277248535_Identifying_Bitcoin_users_by_transaction_behavior)
- Nakamoto, S. (2008, Oktober 31). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Hentet Juni 16, 2018 fra <https://bitcoin.org/bitcoin.pdf>
- Nets. (u.d.). *Select Merchant Agreement*. Hentet Juni 18, 2018 fra [https://my.nets.eu/landingpage?landingPageId=NETSPAYNO&\\_ga=2.81166356.2042385204.1529379000-458300983.1529379000](https://my.nets.eu/landingpage?landingPageId=NETSPAYNO&_ga=2.81166356.2042385204.1529379000-458300983.1529379000)
- Nicolaisen, J. (2016, Juni 9). *Digitale utfordringer i betalingsystemet*. Hentet Juni 17, 2018 fra Norges Bank: <https://www.norges-bank.no/Publisert/Foredrag-og-taler/2016/2016-06-09-Digitaliseringskonferanse/>
- Nicolaisen, J. (2017, April 25). *Hva skal våre penger være?* Hentet Juni 15, 2018 fra Norges Bank: <https://www.norges-bank.no/Publisert/Foredrag-og-taler/2017/2017-04-25-dnva/>
- Norges Bank. (2013, September 2). *Norges Banks Stående Fasiliteter*. Hentet Juni 16, 2018 fra <https://www.norges-bank.no/Bank-og-marked/Likviditetsstyringssystemet/Norges-Banks-staende-fasiliteter/>

- Norges Bank. (2014, November 11). *FAQ - Penger*. Hentet Juni 15, 2018 fra <https://www.norges-bank.no/FAQ/penger/>
- Norges Bank. (2014, November 12). *Kostnader i det norske betalingssystemet*. Hentet Juni 18, 2018 fra [https://static.norges-bank.no/contentassets/c6ed2ec861034f47afb5ea233363a5d3/norges\\_bank\\_memo\\_5\\_2014.pdf](https://static.norges-bank.no/contentassets/c6ed2ec861034f47afb5ea233363a5d3/norges_bank_memo_5_2014.pdf)
- Norges Bank. (2016, Mai). *Norges Banks oppgjørssystem -Rammevilkår, funksjoner og oppgaver med Norges Banks oppgjørssystem, bankenes sikkerhetsstillelse for lån, kontohold for staten*. Hentet Juni 15, 2018 fra [https://www.norges-bank.no/globalassets/upload/betalingsystemer/rammevilkar\\_nbo\\_mai\\_2016.pdf](https://www.norges-bank.no/globalassets/upload/betalingsystemer/rammevilkar_nbo_mai_2016.pdf)
- Norges Bank. (2017, Mai 18). *Finansiell infrastruktur*. Hentet Juni 16, 2018 fra [https://static.norges-bank.no/contentassets/0af5e6ca88d54c7ca6ab9cd8b44257c8/finansiell\\_infrastruktur\\_2017.pdf?v=05/18/2017145640&ft=.pdf](https://static.norges-bank.no/contentassets/0af5e6ca88d54c7ca6ab9cd8b44257c8/finansiell_infrastruktur_2017.pdf?v=05/18/2017145640&ft=.pdf)
- Norges Bank. (2017, Mai 8). *Kunderetta betalingsformidling 2016*. Hentet Juni 15, 2018 fra [https://static.norges-bank.no/contentassets/b633cbc4154540abab705d622eefe52f/nb\\_memo\\_2\\_2017.pdf?v=05/16/2017163134&ft=.pdf](https://static.norges-bank.no/contentassets/b633cbc4154540abab705d622eefe52f/nb_memo_2_2017.pdf?v=05/16/2017163134&ft=.pdf)
- Norges Bank. (2017, Februar 27). *Norges Bank - Sentralbankvirksomhet*. Hentet Juni 15, 2018 fra [https://static.norges-bank.no/contentassets/0909ca87effb4b1f8bdf164878a16b1/sentralbankens\\_virksomhet\\_2017.pdf?v=02/27/2018080908&ft=.pdf](https://static.norges-bank.no/contentassets/0909ca87effb4b1f8bdf164878a16b1/sentralbankens_virksomhet_2017.pdf?v=02/27/2018080908&ft=.pdf)
- Norges Bank. (2017, Mai 19). *Styring av bankenes reserver - systemet i Norge*. Hentet Juni 15, 2018 fra <https://www.norges-bank.no/Bank-og-marked/Likviditetsstyringssystemet/Styring-av-bankenes-reserver/>
- Norges Bank. (2018, Mai 18). *Digitale sentralbankpenger*. Hentet Juni 16, 2018 fra <https://static.norges-bank.no/contentassets/166efadb3d73419c8c50f9471be26402/nbmemo-1-2018-digitalesentralbankpenger.pdf?v=05/18/2018121951&ft=.pdf>
- Norges Bank. (2018). *Endringer i styringsrenten*. Hentet Juni 16, 2018 fra <https://www.norges-bank.no/pengepolitikk/Styringsrenten/Styringsrenten-Oversikt-over-rentemoter-og-endringer-i-styringsrenten/>
- Olsen, Ø. (2014, Juni 3). *Penger og frihet – Betydningen av tillit*. Hentet Juni 15, 2018 fra Norges Bank: <https://www.norges-bank.no/Publisert/Foredrag-og-taler/2014/3-juni-Oystein-Olsen-Kulturhistorisk-museum/>
- Oslo Economics. (2014, Mai). *Markedet for innovative, digitale betalingstjenester*. Hentet Juni 16, 2018 fra [https://www.regjeringen.no/globalassets/upload/kmd/aif/rapport-5-2014\\_innovative\\_digitale\\_betalingslosninger.pdf](https://www.regjeringen.no/globalassets/upload/kmd/aif/rapport-5-2014_innovative_digitale_betalingslosninger.pdf)
- PwC. (2017). *Cybercrime Survey 2017*. Hentet Juni 17, 2018 fra <https://www.pwc.no/no/publikasjoner/cybercrime-survey-2017.pdf>
- Regjeringen. (2017). *Finansmarkedsmeldingen 2016–2017. (Meld. St.34)*. Hentet Juni 15, 2018 fra <https://www.regjeringen.no/no/dokumenter/meld.-st.-34-20162017/id2548252/sec3>
- Regjeringen. (2018, Mars 2). *Ny forskrift for pengepolitikken*. Hentet Juni 15, 2018 fra <https://www.regjeringen.no/no/aktuelt/ny-forskrift-for-pengepolitikken/id2592551/>
- Schneider, F. (2015, Januar 20). *Size and Development of the Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2015: Different Developments*. Hentet Juni 16, 2018 fra <http://www.econ.jku.at/members/Schneider/files/publications/2015/ShadEcEurope31.pdf>

- 
- Schneider, F., & Enste, D. H. (2000, Mars). *Shadow Economies: Size, Causes, and Consequences*. Hentet Juni 16, 2018 fra Journal of Economic Literature: <http://www.economics.uni-linz.ac.at/members/Schneider/files/publications/JEL.pdf>
- Segendorf, B. (2014, Juni 17). *Have virtual currencies affected the retail payments market?* Hentet Juni 16, 2018 fra Economic Commentaries: [https://www.riksbank.se/globalassets/media/rapporter/ekonomiska-kommentarer/fore-2017/engelska/2014/rap\\_ek\\_kom\\_nr02\\_140617\\_eng.pdf](https://www.riksbank.se/globalassets/media/rapporter/ekonomiska-kommentarer/fore-2017/engelska/2014/rap_ek_kom_nr02_140617_eng.pdf)
- Sentralbankloven. Lov av 9.september 1985 om Norges Bank og pengevesenet mv.
- Sparebanken Møre. (2018). *Straksbetaling*. Hentet Juni 17, 2018 fra <https://www.sbm.no/person/betaling/nettbank---tillegg/straksbetaling/256/4391/>
- Statistisk sentralbyrå. (2015, Oktober 1). *Familier og husholdninger, 1.januar 2014*. Hentet Juni 17, 2018 fra <https://www.ssb.no/befolkning/statistikker/familie/aar/2014-12-12?fane=om#content>
- Statistisk sentralbyrå. (2015, Januar 8). *Forbruk - Vi kjøper mer av det meste*. Hentet Juni 15, 2018 fra <https://www.ssb.no/inntekt-og-forbruk/artikler-og-publikasjoner/vi-kjoper-mer-av-det-meste>
- Statistisk sentralbyrå. (2017, Mai 19). *Bruk av IKT i husholdningene*. Hentet Juni 16, 2018 fra <https://www.ssb.no/ikthus>
- Sveriges Riksbank. (2009). Stockholms Banco. I G. Wetterberg, *Money and Power: From Stockholms Banco 1656 to Sveriges Riksbank Today* (ss. 25-45). Stockholm: Sveriges Riksbank.
- Sveriges Riksbank. (2017, September). *Riksbankens e-kronaprojekt*. Hentet Juni 16, 2018 fra [https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport\\_ekrona\\_uppdaterad\\_170920\\_sve.pdf](https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_sve.pdf)
- Symantec. (2012). *Banks likely to remain top cybercrime targets*. Hentet Juni 17, 2018 fra Symantec: [https://www.symantec.com/content/en/us/enterprise/other\\_resources/b\\_Financial\\_Attacks\\_Exec\\_Report.pdf](https://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf)
- Syrstad, O. (2011). *Systemer for likviditetsstyring: Oppbygging og egenskaper*. Hentet Juni 17, 2018 fra Norges Bank: [https://static.norges-bank.no/globalassets/upload/publikasjoner/staff-memo/2011/staffmemo\\_0511.pdf?v=03/09/2017122442&ft=.pdf](https://static.norges-bank.no/globalassets/upload/publikasjoner/staff-memo/2011/staffmemo_0511.pdf?v=03/09/2017122442&ft=.pdf)
- Vavrinec, C. (2017, November 6). *Can Bitcoin Become a Viable Alternative to Fiat Currencies? An empirical analysis of Bitcoin's volatility based on a GARCH model*. Hentet Juni 17, 2018 fra [https://www.researchgate.net/publication/316851272\\_Can\\_Bitcoin\\_Become\\_a\\_Viable\\_Alternative\\_to\\_Fiat\\_Currencies\\_An\\_Empirical\\_Analysis\\_of\\_Bitcoin's\\_Volatility\\_Based\\_on\\_a\\_GARCH\\_Model](https://www.researchgate.net/publication/316851272_Can_Bitcoin_Become_a_Viable_Alternative_to_Fiat_Currencies_An_Empirical_Analysis_of_Bitcoin's_Volatility_Based_on_a_GARCH_Model)
- Vipps. (u.d.). *Ta betalt med Vipps*. Hentet Juni 18, 2018 fra <https://www.vipps.no/>
- Zamyatin, A., Stifter, N., Judmayer, A., Schindler, P., E., W., & Knottenbelt, W. (2018). *(Short Paper) A Wild Velvet Fork Appears!* Hentet Juni 18, 2018 fra <https://eprint.iacr.org/2018/087.pdf>