NORGES BANK

2018

FINANSIELL INFRASTRUKTUR

Norges Bank

Oslo 2018

Adresse: Bankplassen 2
Post: Postboks 1179 Sentrum, 0107 Oslo
Telefon: 22 31 60 00
Telefaks: 22 41 31 05
E-post: central.bank@norges-bank.no
Internett: http://www.norges-bank.no

Ansvarlig redaktør: Øystein Olsen
Omslag og grafisk utforming: Brandlab
Trykk: 07 Media AS
Teksten er satt med 9,5 pkt Azo Sans Light

ISSN 1894-8308 (trykk)
ISSN 1894-8316 (online)

Innhold

Hovedstyrets vurdering

Rapporten *Finansiell infrastruktur* er en del av Norges Banks arbeid for å fremme finansiell stabilitet og et effektivt betalingssystem. Hovedstyret drøftet innholdet i rapporten 2. mai 2018.

Samfunnet er avhengig av at betalingssystemet og annen finansiell infrastruktur fungerer. Det sikrer at privatpersoner og bedrifter kan betale for varer og tjenester, at banker kan formidle finansiering og at risiko kan omfordeles. En sikker og effektiv finansiell infrastruktur er en forutsetning for finansiell stabilitet. Norges Bank følger interbanksystemenes og verdipapiroppgjørssystemets virksomhet gjennom tilsyns- og overvåkingsarbeid. Hovedstyret vurderer den finansielle infrastrukturen som sikker og effektiv. Enkelte sårbarheter gjør seg likevel gjeldende.

Betalingssystemets sentraliserte struktur og avhengighet av IKT gjør det sårbart for cyberangrep. Et effektivt forsvar krever spesialisert kompetanse og samordning. Norges Bank følger opp at interbanksystemene som Norges Bank fører tilsyn med har tilfredsstillende forsvarsverk. Et viktig element i arbeidet er å følge opp systemeiernes kontroll og styring med cybersikkerhet hos sine IKT-leverandører. Regjeringen vil etablere en felles arena for myndigheter med tilsynsansvar for IKT-sikkerhet. Formålet er informasjonsutveksling og kompetanseoverføring for å øke kvaliteten på IKT-sikkerhetstilsyn, og dermed forbedre IKT-sikkerheten. Initiativet bidrar også til bedre utnyttelse av knappe IKT-ressurser.

Svikt hos sentrale IKT-leverandører kan sette viktige deler av betalingssystemet – og andre sentrale samfunnsfunksjoner – ut av spill. Slik konsentrasjonsrisiko kan vanskelig håndteres av den enkelte systemeier. Hovedstyret mener det bør utredes hvordan sentrale IKT-leverandører til betalingssystemet best kan underlegges tilsyn, herunder om et slikt tilsyn skal være samordnet mellom relevante myndigheter.

Effektive elektroniske beredskapsløsninger er avgjørende for at betalingssystemet kan gjenopprettes raskt ved avbrudd. Kontanter er en del av den samlede beredskapen ved en eventuell svikt i de elektroniske beredskapsløsningene. Basert på forslag fra Finanstilsynet og Norges Bank fastsatte Finansdepartementet 17. april 2018 en forskrift for å tydeliggjøre bankenes plikt til kontantberedskap.

Kontanter er fortsatt en betydelig betalingsmåte i en normalsituasjon. Tilbudet av kontanttjenester er i hovedsak tilfredsstillende, men sårbart. Etter Norges Banks syn er det behov for at bankenes lovbestemte plikt til å tilby kontanttjenester også i en normalsituasjon tydeliggjøres.

Etter initiativ fra Finans Norge og Norges Bank utvikles nå en løsning for oppgjør av realtidsbetalinger uten kredittrisiko for bankene. I februar i år offentliggjorde syv nordiske banker at de vil utrede muligheten for en felles nordisk infrastruktur, i første omgang for realtidsbetalinger. Formålet er blant annet å redusere betalingskostnadene og sørge for bedre grensekrysende betalinger i Norden. Initiativet reiser spørsmål knyttet til eventuell deltakelse i et utenlandsk interbanksystem og etablering av kritisk infrastruktur i utlandet som må avklares. Hovedstyret legger til grunn at en forbedret løsning for oppgjør av realtidsbetalinger i Norge ikke realiseres vesentlig senere enn det som har vært planlagt.

Felles løsninger, standarder og tidlig bruk av ny teknologi har gitt en effektiv finansiell infrastruktur i Norge. Nye aktører i bank- og betalingssystemet kan bedre effektiviteten ytterligere. Konkurransen bør imidlertid fortsatt foregå innenfor rammen av felles infrastruktur. En viktig infrastruktur for blant annet mobilbetalinger er registre som kobler kontonumre sammen med telefonnumre. Et felles register for alle aktører som yter betalingstjenester, vil legge til rette for høy kvalitet og like konkurransevilkår og fremme et effektivt betalingssystem.

Hva er finansiell infrastruktur?

Finansiell infrastruktur kan defineres som et nettverk av systemer som lar brukere gjennomføre finansielle transaksjoner med hverandre. Systemene omfatter betalingssystemet, verdipapiroppgjørsystemet, verdipapirregistre, sentrale motparter og transaksjonsregistre.

Infrastrukturen skal sørge for at pengebetalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp. Effektiv finansiell infrastruktur er en forutsetning for en moderne økonomi. Tilnærmet alle økonomiske transaksjoner som utføres forutsetter bruk av finansiell infrastruktur. Infrastrukturen spiller dermed en sentral rolle for stabiliteten til det finansielle systemet.

Samfunnets kostnader ved en svikt i den finansielle infrastrukturen kan bli vesentlig større enn de bedriftsøkonomiske kostnadene til systemeierne. Derfor er den finansielle infrastrukturen gjenstand for regulering.

Norges Banks ansvar

Det følger av sentralbankloven § 1 at Norges Bank skal fremme et effektivt betalingssystem innenlands og overfor utlandet. Betalingssystemet omfatter alle måter, ordninger og innretninger som kan benyttes til å utføre eller formidle betalinger. Effektivitet i betalingssystemet innebærer at betalinger kan gjennomføres raskt, sikkert, til lave kostnader og på måter som er tilpasset brukernes behov.

Norges Bank gir konsesjon og fører tilsyn med avregnings- og oppgjørssystemer for pengeoverføringer mellom banker (interbanksystemer). Tilsynsansvaret følger av betalingssystemloven kapittel 2. Norges Banks overvåking bygger på sentralbankloven § 1 og internasjonale prinsipper.

Norges Bank utøver myndighetsansvaret på dette området ved å:

- Følge med på utviklingstrekk i den finansielle infrastrukturen og være en pådriver for endringer som kan gjøre den mer effektiv.
- Overvåke og føre tilsyn med enkeltaktører.
- Sørge for sikkert, raskt og kostnadseffektivt oppgjør av betalinger mellom banker med konto i Norges Bank.
- Utstede sedler og mynt og sørge for at de kan fungere effektivt som betalingsmiddel.

I rapporten *Finansiell infrastruktur* gjør Norges Bank rede for bankens tilsyns- og overvåkingsarbeid siden forrige rapport, og gir uttrykk for hvor banken mener det er behov for endringer. Rapporten inneholder også omtale av sårbarheter og aktuelle utviklingstrekk i den finansielle infrastrukturen.

1 Sårbarheter

1.1 CYBERSIKKERHET

Betalingssystemets sentraliserte struktur og avhengighet av IKT gjør det sårbart for cyberangrep. Et vellykket angrep på den finansielle infrastrukturen kan medføre at kunder ikke får gjennomført sine betalinger og tap av store verdier. Et vellykket angrep kan også innebære at sensitiv informasjon kommer på avveie eller blir manipulert. Antall cyberangrep øker, og metodene er i stadig endring. Angrepene rammer på tvers av land, sektorer og virksomheter. Et effektivt forsvar krever samordning og målrettet innsats både av myndighetene og private systemeiere. Regjeringens arbeid med ny nasjonal strategi for IKT-sikkerhet er et viktig tiltak i denne sammenheng.

Endringer i bank- og betalingssystemet

Endringer i bank- og betalingssystemet øker angrepsflaten for cyberangrep. Det reviderte betalingstjenestedirektivet (PSD2)[1] pålegger banker å åpne opp systemene sine slik at tredjepartsaktører kan få tilby tjenester knyttet til betalinger og kontoinformasjon. Det innebærer at flere aktører får behandle personopplysninger, kontoinformasjon og transaksjonsdata. Finanstilsynet er konsesjonsgiver og tilsynsmyndighet for tredjepartsaktører i henhold til PSD2 og stiller krav til bankenes og tredjepartaktørenes IKT-sikkerhet. I tråd med ansvarsprinsippet er det virksomhetene selv som skal sørge for at informasjon og systemer er godt nok sikret, og som skal iverksette nødvendige tiltak.

Flere store teknologiaktører er også blitt tilbydere av betalingstjenester. Selskapene baserer tjenestene sine på store datamengder som kan ha høy økonomisk verdi, og nettverksfordeler kan føre til at én eller noen få aktører blir svært store innen betalingstjenester på internasjonalt nivå.[2] Konsentrasjonen av informasjon kan gjøre selskapene til attraktive mål for cyberangrep, fordi et vellykket angrep mot dem vil kunne få store konsekvenser.

Nye aktører i betalingsmarkedet fører til økt spredning av betalingsinformasjon. Store internasjonale aktører vil kunne oppbevare mye betalingsinformasjon og annen informasjon om kundene som kan komme på avveie og misbrukes. Sårbarheter knyttet til tilgang, behandling og oppbevaring av informasjon kan ha betydning for tilliten til betalingssystemet og finansiell stabilitet.

Ny teknologi

Kunstig intelligens og kvantedatamaskiner er eksempler på ny teknologi som også kan utnyttes til cyberangrep.

Ved hjelp av *kunstig intelligens* kan angripere analysere og benytte store mengder informasjon for mer målrettede angrep. Det er viktig at tiltakene for cybersikkerhet er tilsvarende avanserte for å beskytte betalingssystemet mot truslene som kunstig intelligens kan representere. Kryptografi er teknikker som skal sikre informasjonens integritet og konfidensialitet. Krypteringsteknikker har stor betydning for IKT-

1 Revised Payment Services Directive (PSD2) ble innført i EU i januar 2018. PSD2 er foreløpig ikke tatt inn i EØS-avtalen.

2 Se også ramme om digitale plattformer og nettverksfordeler i kapittel 2.1.

CYBERSIKKERHET

Cybersikkerhet innebærer at systemene i den finansielle infrastrukturen er tilgjengelige, beskyttet mot uønsket innsyn og at informasjonen er pålitelig. Det vil si at systemene oppfyller tre viktige mål for informasjonssikkerhet[1]:

- **Tilgjengelighet**: Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at tjenesten og aktuell informasjon er tilgjengelig ved behov.
- **Konfidensialitet**: Sikkerhet for at nærmere angitt informasjon beskyttes mot innsyn fra uvedkommende, og at kun autoriserte personer får tilgang til informasjonen.
- **Integritet:** Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig, gyldig (ikke korrumpert) og et resultat av autoriserte og kontrollerte aktiviteter.

1 Departementene (2012).

ULIKE FORMER FOR CYBERANGREP[1]

Angrep rettet mot finansiell infrastruktur kan ramme systemenes tilgjengelighet. Angrepene kan også ramme informasjonens konfidensialitet og integritet gjennom henholdsvis uautorisert uthenting av informasjon og uautoriserte betalingstransaksjoner. Angrep kan ramme langs flere dimensjoner.

DDoS (Distributed denial of service)
DDoS er Internett-angrep som overbelaster en server med så stor trafikk at normal tilgang for ordinære brukere hindres. Hensikten er å ramme systemenes tilgjengelighet.

Phishing og sosial manipulering
De ansatte utgjør ofte det svakeste leddet i cyberforsvaret. Ved phishing utgir kriminelle seg for å være noen andre for å hente ut sensitiv informasjon. Kriminelle benytter i økende grad phishing og sosial manipulering for å trenge inn i finansforetakenes systemer, både for uthenting av sensitiv informasjon og til manipulering av betalingsoppdrag.

Vannhull-angrep
Vannhull betegner en angrepsstrategi der virus plantes på nettsteder det er naturlig at ansatte i finanssektoren besøker (vannhull). Viruset følger med over til datasystemene på den ansattes arbeidsplass, hvor det åpner en inngang som kan benyttes av kriminelle. Hensikten kan være ren informasjonsinnhenting eller informasjonsinnhenting som grunnlag for å gjøre uautoriserte transaksjoner. I februar 2017 ble 20 banker i Polen infisert med skadevare som var blitt distribuert via webserveren til det polske finanstilsynet.

1 Boksen bygger på Finanstilsynet (2017a).

sikkerhet og er en forutsetning for sikker elektronisk kommunikasjon, herunder mellom aktørene i den finansielle infrastrukturen. *Kvantedatamaskiner* fungerer etter andre prinsipper enn tradisjonell digital teknologi. Slike maskiner er under utvikling og vil utfordre dagens krypteringsmekanismer. Krypterte data kan også lagres av kriminelle for dekryptering om kvantedatamaskiner blir tilgjengelige. Nasjonal sikkerhetsmyndighet (NSM) har satt i gang et arbeid for videreutvikling av krypteringsteknologi for nasjonale graderte systemer for å gjøre dem resistente mot kvantedatamaskiner.[3]

Felles forsvar

Cyberangrep rammer på tvers av land, sektorer og virksomheter. Samordning og informasjonsdeling er avgjørende for å få et effektivt forsvar og redusere risikoen for cyberangrep. Myndighetene og finansnæringen har sammenfallende interesser på dette feltet. Det er etablert samarbeidsorganer på nasjonalt nivå og på sektornivå, samt et felles cyberkoordineringssenter. Nordic Financial CERT er et privat samarbeidsorgan for finansiell sektor som koordinerer arbeidet med cybersikkerhet og hendelseshåndtering. Myndighetene har flere initiativ for videre samordning under arbeid, se ramme om cybersikkerhet og regulering på side 6.

Tilsyn

Tilsyn er et viktig virkemiddel for myndighetene for å påse at aktørene etterlever kravene til cybersikkerhet. Norges Banks tilsyns- og overvåkingsarbeid med cybersikkerhet er basert på globale standarder. Dette arbeidet omtales nærmere i kapittel 3. De nordiske sentralbankene har etablert en årlig konferanse om cybersikkerhet for å øke kompetansen på feltet. Konferansen ble avholdt første gang høsten 2017. I tillegg har sentralbankene i Norden kontaktflater på operativt nivå. Finanstilsynet følger opp finansforetakenes cybersikkerhet gjennom IKT-tilsyn.

Den teknologiske utviklingen krever økt IKT-sikkerhetskompetanse også hos tilsynsmyndighetene. Justis- og beredskapsdepartementet og Forsvarsdepartementet skal utrede og etablere en felles arena for myndigheter med tilsynsansvar for IKT-sikkerhet.[4]

3 NSM (2017).

4 Meld. St. 38 (2016–2017).

CYBERSIKKERHET OG REGULERING

Forsvarsdepartementet og Justis- og beredskapsdepartementet har ansvaret for henholdsvis den militære og den sivile IKT-sikkerheten på nasjonalt nivå. Nasjonal sikkerhetsmyndighet (NSM) skal ivareta et overordnet og sektorovergripende ansvar på vegne av de to departementene. NSM er Norges ekspertorgan for informasjons- og objektsikkerhet og utgjør det nasjonale fagmiljøet for IKT-sikkerhet.

CPMI-IOSCO
Det internasjonale sentralbankorganet CPMI (Committee on Payment and Market Infrastructures) har sammen med IOSCO (International Organisation of Securities Commissions), det internasjonale organet for verdipapirtilsyn, utarbeidet en utfyllende veiledning for å vurdere cybersikkerhet i finansiell infrastruktur (CPMI-IOSCO 2016). Norges Banks tilsyns- og overvåkningsarbeid med cybersikkerhet er basert på disse prinsippene, se kapittel 3.

Network and Information Security Directive (NIS-direktivet)
Europaparlamentets og Rådets direktiv av 6. juli 2016 definerer tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU. NIS-direktivet pålegger blant annet medlemsstater å sørge for at operatører av viktige tjenester, herunder banker og finansiell infrastruktur, iverksetter sikkerhetstiltak og rapporterer hendelser. Det stiller også krav til utveksling av informasjon. Justis- og beredskapsdepartementet arbeider med gjennomføringen av NIS-direktivet i Norge.

Stortingsmelding om IKT-sikkerhet og ny nasjonal strategi for IKT-sikkerhet
I juni 2017 ble stortingsmeldingen om IKT-sikkerhet lagt frem (Meld. St. 38 (2016–2017)). Dette er den første stortingsmeldingen om IKT-sikkerhet. Tittelen «Et felles ansvar» viser til at verken myndigheter eller private aktører kan kontrollere sin digitale sårbarhet alene.

For å følge opp meldingen arbeider regjeringen med en ny nasjonal strategi for IKT-sikkerhet som etter planen skal ferdigstilles høsten 2018. Justis- og beredskapsdepartementet og Forsvarsdepartementet leder strategiarbeidet og ønsker en bred involvering av både offentlige og private aktører. Norges Bank har gitt innspill til arbeidet med ny nasjonal strategi for IKT-sikkerhet. Sentrale momenter var at det bør vurderes om reguleringen av sentrale IKT-leverandører er tilstrekkelig og at det ved utkontraktering av IKT-drift til utlandet bør vurderes å stille krav om virksom beredskapsløsning i Norge.[1] Regjeringen har opprettet et privat-offentlig samarbeidsforum hvor strategiske spørsmål knyttet til digitale sårbarheter og IKT-sikkerhet blir diskutert mellom private aktører og myndighetene. Det første møtet ble holdt i januar 2018.[2]

IKT-sikkerhetsutvalg
I september 2017 nedsatte regjeringen et utvalg som skal utrede reguleringsbehov på IKT-sikkerhetsområdet og organisering av tverrsektorielt ansvar. Utvalget skal vurdere hvorvidt det eksisterende regelverket er godt nok og om det ivaretar de nye digitale samfunnsutfordringene. Utvalget skal også foreslå konkrete rettslige og organisatoriske endringer på IKT-sikkerhetsområdet. Utvalget skal levere sin utredning innen 1. desember 2018.

Ny lov om nasjonal sikkerhet
Stortinget vedtok i februar 2018 ny lov om nasjonal sikkerhet. Den nye loven tydeliggjør hvem som har ansvaret for forebyggende sikkerhetsarbeid. Det enkelte departement vil ha ansvar for sin sektor. Samtidig skal sikkerhetsmyndighetens helhetlige ansvar styrkes. Videre legger den nye loven til rette for økt samhandling mellom offentlige myndigheter og mer samarbeid mellom offentlig og privat virksomhet, slik at det forebyggende sikkerhetsarbeidet blir bedre og mer helhetlig.

1 Norges Bank (2018a).
2 Solberg (2018).

Videre skal NSM vurdere etablering av en sentral kapasitet med IKT-sikkerhetskompetanse som skal benyttes som en ressurs for tilsynsmyndighetene.[5] Formålet er informasjonsutveksling og kompetanseoverføring for å øke kvaliteten på IKT-sikkerhetstilsyn, og dermed forbedre IKT-sikkerheten. Initiativene vil også bidra til bedre utnyttelse av knappe IKT-ressurser.

1.2 UTKONTRAKTERING OG SENTRALE IKT-LEVERANDØRER

IKT-leverandører har bidratt til utviklingen av effektive løsninger i betalingssystemet. Betalingssystemets avhengighet av IKT-leverandører har imidlertid ført til sårbarheter. Det innebærer en konsentrasjonsrisiko at flere av aktørene har utkontraktert IKT-driften til samme leverandør. Svikt hos sentrale IKT-leverandører kan ramme viktige deler av betalingssystemet. Det bør utredes hvordan sentrale IKT-leverandører til betalingssystemet best kan underlegges tilsyn, herunder om et slikt tilsyn skal være samordnet mellom relevante myndigheter.

Styring og kontroll

Utkontraktering innebærer å overlate en oppgave til en oppdragstaker istedenfor å utføre den selv. I betalingssystemet er drift og utvikling av IKT i stor grad utkontraktert. Systemeiere har ansvaret for utkontrakterte oppgaver. Det krever at de har tilstrekkelig med ressurser og kompetanse til å føre effektiv styring og kontroll med sine leverandører og eventuelle underleverandører.[6]

Omfattende utkontraktering av IKT-oppgaver kan redusere systemeiernes kompetanse til å føre en effektiv styring og kontroll med utkontraktert virksomhet, som igjen kan svekke sikkerheten i betalingssystemet. I tillegg kan bruk av leverandører gjøre det mer utfordrende å kontrollere om uautorisert personell får tilgang til systemene og sensitiv informasjon. Utstrakt utkontraktering av IKT-drift til utlandet kan føre til at den nasjonale evnen til drift, utvikling og oppfølging av sentral IKT-virksomhet i betalingssystemet svekkes. Det kan også være mer utfordrende for norske myndigheter å håndtere en beredskapssituasjon dersom viktige deler av IKT-driften skjer fra et annet land. Behovet for nasjonal kontroll med betalingssystemet i en krisesituasjon kan tale for at deler av IKT-driften skjer fra Norge. Ved drift fra utlandet bør det vurderes om det er behov for en operativ beredskapsløsning i Norge som på kort varsel kan overta driften.

KARTLEGGING AV UTKONTRAKTERING I BETALINGSSYSTEMET

Den samlede risikoen ved utkontraktering i betalingssystemet kan bli betydelig selv om risikoen til den enkelte aktør og hver enkelt utkontraktering er forsvarlig. En arbeidsgruppe med representanter fra Finanstilsynet og Norges Bank kartlegger våren 2018 omfanget av utkontraktering i bank- og betalingssystemet. Kartleggingen skal gi grunnlag for å vurdere om utkontraktering svekker foretakenes styring og kontroll med driften. Kartleggingen skal også gi grunnlag for å vurdere om utkontraktering generelt, og til utlandet spesielt, vil vanskeliggjøre myndighetenes mulighet for styring og kontroll med virksomhetene i en beredskapssituasjon. Kartleggingen vil også gi en bedre oversikt over sentrale IKT-leverandører og konsentrasjonsrisiko.

Konsentrasjonsrisiko

Profesjonelle IKT-leverandører kan ha mer ressurser og kompetanse til å utvikle robuste løsninger enn de enkelte systemeierne. Det er store faste kostnader knyttet til IKT, og for å oppnå stordriftsfordeler bruker flere aktører samme leverandør.

Det innebærer en konsentrasjonsrisiko at flere av aktørene i betalingssystemet har utkontraktert driften av IKT-systemene til noen få leverandører.[7] Dersom sentrale IKT-leverandører til betalingssystemet feiler, enten som følge av operasjonell svikt eller angrep, kan viktige deler av betalingssystemet stoppe opp. Problemer hos IKT-leverandøren Evry 6. oktober 2017 rammet om lag 40 banker i Norge, i tillegg til at Posten og Telenor ble berørt. Hendelsen illustrerer hvor bredt det kan ramme når en sentral IKT-leverandør feiler.

En trend er også at flere IKT-leverandører benytter samme datasenter for fysisk plassering av maskinene for å utnytte stordriftsfordeler. Det utgjør en geografisk konsentrasjonsrisiko at mange av systemene

5 Meld. St. 38 (2016–2017).
6 Norges Bank (2016) og Norges Bank (2017a).
7 Norges Bank (2017a).

i den finansielle infrastrukturen kan rammes av en svikt på ett sted.

Regulering

IKT-leverandører er ikke underlagt tilsvarende regulering og tilsyn som de konsesjonspliktige aktørene i bank- og betalingssystemet. Det innebærer at Finanstilsynet og Norges Bank ikke kan stille krav direkte til IKT-leverandørene som systemeierne i betalingssystemet benytter. Kravene må rettes mot konsesjonshaver som får ansvaret for at IKT-leverandørene følger opp.

Financial Stability Board (FSB) viser i en rapport fra juni 2017 til at håndtering av operasjonell risiko fra tjenesteleverandører er en utfordring som bør prioriteres internasjonalt.[8] I rapporten heter det at myndighetene bør ta stilling til om nåværende tilsynsrammer for viktige tredjepartsleverandører til finansinstitusjoner er hensiktsmessige, og at dette gjelder spesielt hvis flere finansinstitusjoner er avhengig av samme tredjepartsleverandør. FSB viser til at slik konsentrasjon kan medføre behov for økt koordinering mellom myndigheter med ansvar for IKT-sikkerhet. I Storbritannia ble det i 2017 innført en lovendring som innebærer at tjenesteleverandører til systemviktige betalingssystem kan underlegges tilsyn av Bank of England, se ramme om Bank of Englands tilsyn med leverandører til systemviktige betalingssystem.

Konsentrasjonsrisiko kan vanskelig håndteres av den enkelte systemeier. Det bør utredes hvordan IKT-leverandører og datasentre som er kritiske for betalingssystemet og andre sentrale samfunnsfunksjoner best kan underlegges tilsyn. En slik utredning må avgrenses mot sikkerhetslovutvalgets pågående arbeid, se boks om IKT-sikkerhetsutvalgets mandat.[9] For å få en helhetlig regulering bør det vurderes om et slikt tilsyn skal være samordnet med tilsynsmyndigheter for annen kritisk infrastruktur som er avhengig av de samme IKT-leverandørene. Regjeringens initiativ til å etablere en felles arena for myndigheter med tilsynsansvar for IKT-sikkerhet er i tråd med dette.[10]

8 FSB (2017a).

9 Se også ramme om cybersikkerhet og reguleringsarbeid i kapittel 1.1.

10 Se avsnitt om tilsyn i kapittel 1.1 om cybersikkerhet.

MANDAT IKT-SIKKERHETSUTVALG

OPPFØLGING AV MELD. ST. 38 (2016–2017) OM IKT-SIKKERHET

Problemstilling 1: Er dagens regulering hensiktsmessig for å oppnå forsvarlig nasjonal IKT-sikkerhet?

Problemstilling 2: Har vi en hensiktsmessig fordeling og organisering av tverrsektorielt ansvar på etatsnivå innen nasjonal IKT-sikkerhet?

Problemstilling 3: Hvilke regulatoriske og organisatoriske grep bør gjøres for å styrke nasjonal IKT-sikkerhet?

Utvalget skal levere sin utredning i desember 2018.

BANK OF ENGLANDS TILSYN MED LEVERANDØRER TIL SYSTEMVIKTIGE BETALINGSSYSTEM

I 2017 ble det gjennomført en endring i den britiske banklovgivningen (Banking Act 2009) som innebærer at tjenesteleverandører til systemviktige betalingssystem kan underlegges tilsyn av Bank of England.[1] HM Treasury utpeker hvilke tjenesteleverandører til betalingssystemet som skal underlegges tilsyn. Systemeiers ansvar for styring og kontroll endres ikke av at leverandøren underlegges tilsyn av Bank of England.

Formålet med lovendringen er å styrke Bank of Englands mulighet til å fremme finansiell stabilitet. Som følge av endringen kan Bank of England stille krav til tjenesteleverandører for systemviktige betalingssystem og håndheve kravene. Bank of England vil blant annet kunne kreve informasjon direkte fra leverandørene, kreve at leverandørene får utført risikovurderinger av eksterne eksperter og stille krav til styresammensetningen hos leverandørene. I tillegg kan Bank of England stille krav til planlagte endringer som kan påvirke risikoen til disse tjenesteleverandørene, slik som lansering av nye produkter og tjenester, endrede eierforhold og utkontraktering.

1 Se Bank of England (2018).

1.3 TILBUDET AV KONTANTTJENESTER

Elektroniske betalingsmåter brukes stadig oftere, men kontanter er fortsatt en viktig betalingsmåte både i en normal- og beredskapssituasjon. Kontanter er tvungne betalingsmidler i forbrukerforhold og utgjør en del av beredskapen til betalingssystemet. Tilbudet av kontanttjenester er i hovedsak tilfredsstillende, men sårbart. Det er en klar trend i retning av færre innskudds- og uttaksmuligheter, og i tillegg drives en viktig del av tilbudet av aktører som ikke er forpliktet til å opprettholde tilbudet. Det er behov for at bankenes lovbestemte plikt til å tilby kontanttjenester i en normalsituasjon tydeliggjøres.

Publikums tilgang til å gjøre kontantuttak er i hovedsak tilfredsstillende i dag. Tilgangen er i stor grad basert på minibanker og uttak i butikker i forbindelse med varekjøp, såkalt cashback. Kontantuttak fra minibanker og cashback ved varekjøp er banknøytrale løsninger. Det innebærer at kundene kan ta ut kontanter i en minibank eller i en butikk uavhengig av bankforbindelse. Antallet bankfilialer og minibanker reduseres. Det fører til at cashback ved varekjøp utgjør en økende andel av det samlede tilbudet av uttakstjenester.

Publikums tilgang til å gjøre kontantinnskudd er ikke fullt ut tilfredsstillende i dag. Tilgangen er i hovedsak basert på innskudd i post i butikk/postkontor og innskudds- og resirkuleringsmaskiner. Innskudds- og resirkuleringsmaskinene er bankspesifikke og kan bare benyttes av bankenes egne kunder. Gjennom DNBs avtale med Posten, kan kundene i DNB gjøre kontantinnskudd og andre enklere banktjenester ved vel 1300 butikker og omtrent 30 postkontorer. Kunder i andre banker kan også gjøre innskudd gjennom denne ordningen, men da som en giroinnbetaling mot et gebyr på 100 kroner og 3–7 dagers ventetid før pengene er på konto. Innskuddsmulighetene gjennom Posten framstår dermed som lite effektive for kunder av andre banker enn DNB.

De private selskapene Nokas og Loomis drifter og eier en stor andel av minibankene og natt- og døgnsafene. Sammen med butikker som tilbyr cashback ved varekjøp, er Nokas og Loomis således sentrale for tilbudet av kontanttjenester. Butikkene, Nokas og Loomis er ikke forpliktet til å tilby kontanttjenestene som de driver i egen regi. De kan derfor avvikle tilbudet om de ikke finner det lønnsomt eller hensiktsmessig. Det gjør tilbudet sårbart.

Regulering

Finansforetaksloven § 16-4 fastslår bankenes plikt til å motta kontanter fra kundene og gjøre innskudd tilgjengelig for kundene i form av kontanter. Det følger av forarbeidene til loven at bankene plikter å tilby allmennheten effektive og rasjonelle ordninger for innskudd og bruk av innskuddskonto i samsvar med kundenes vanlige behov.

En viktig del av kontanttjenestetilbudet er avhengig av aktører som ikke er forpliktet til å opprettholde tilbudet. Det er uansett klart at det er bankene som har plikt etter finansforetaksloven § 16-4 første ledd til å sørge for at tilbudet av kontanttjenester er tilfredsstillende. Om betydelige deler av tilbudet dekkes av aktører som ikke er forpliktet etter loven eller avtale med bankene, må bankene være forberedt på å tre inn på kort varsel for å opprettholde et tilstrekkelig tilbud.

Effektive elektroniske beredskapsløsninger er avgjørende for at betalingssystemet kan gjenopprettes raskt ved avbrudd. Kontanter er en del av den samlede beredskapen ved en eventuell svikt i de elektroniske beredskapsløsningene.[11] Basert på forslag fra Finanstilsynet og Norges Bank fastsatte Finansdepartementet 17. april 2018 en forskrift for å tydeliggjøre bankenes ansvar for å distribuere kontanter til publikum i en beredskapssituasjon.[12]

På tilsvarende måte mener Norges Bank at det er behov for at bankenes lovbestemte plikt til å tilby kontanttjenester også i en normalsituasjon tydeliggjøres.[13] Distribusjon av kontanter i en beredskapssituasjon og normalsituasjon vil basere seg på den samme infrastrukturen og henger dermed sammen. Norges Bank skriver i brev 20. februar 2018:

> *Norges Banks vurdering er at bankenes plikt etter loven til å tilby kontanttjenester bør tydeliggjøres. En slik tydeliggjøring bør være tilstrekkelig konkret, og bør etter Norges Banks syn blant annet spesifisere krav til gografisk tilgjengelighet av tjenestene, f.eks. nærhet til handelssteder. Videre er det Norges Banks vurdering at økt bruk av banknøytrale fellesløsninger trolig vil bidra til at plikten etter loven kan oppfylles på en samfunnsøkonomisk effektiv måte. Et eksempel på slike fellesløsninger er banknøytrale innskudds- og resirkulerings-*

11 Norges Bank (2017a).
12 Finansdepartementet (2018b).
13 Norges Bank (2018b).

automater, som kundene kan benytte uavhengig av bankforbindelse, slik tilfellet er med minibanker.

I Finansmarkedsmeldingen 2018 skriver Finansdepartementet blant annet at bankene har et ansvar for å opprettholde tilfredsstillende kontanttilbud i hele landet også fremover, se ramme om tilgang på kontanter i en normalsituasjon.

TILGANG PÅ KONTANTER I EN NORMALSITUASJON

Finansdepartementet har bedt Finanstilsynet, i samråd med Norges Bank, om å undersøke hvordan bankene etterlever plikten i finansforetaksloven § 16-4 om å gjøre kontanter tilgjengelig i en normalsituasjon og vurdere om det er behov for å innskjerpe plikten.[1] Norges Bank sendte brev med sine vurdereringer av kontanttjenestetilbudet til Finanstilsynet 20. februar 2018. Finanstilsynet sendte svar til Finansdepartementet 1. mars 2018.

I Finansmarkedsmeldingen 2018, som ble publisert 27. april, skriver Finansdepartementet:[2]

Regjeringen mener det er av stor betydning at publikum har tilgang til bankinnskudd og betalingstjenester på en hensiktsmessig måte. Det er betryggende at Finanstilsynet har funnet at kontanttjenester er tilgjengelig i hele landet, men utviklingen kan gi grunnlag for bekymring. Bankene har et ansvar for å opprettholde tilfredsstillende kontanttilbud i hele landet også fremover. Dette ansvaret kan trolig ofte håndteres mest effektivt gjennom fellesløsninger, slik Finanstilsynet og Norges Bank har pekt på. Dersom bankene ikke opprettholder et godt nok tilbud, har Finansdepartementet mulighet for å fastsette konkrete plikter for enkeltbanker i forskrift. Det vil imidlertid kunne innebære unødvendig høye kostnader sammenlignet med et velorganisert samarbeid bankene imellom. Regjeringen vil følge opp disse spørsmålene i samarbeid med Finanstilsynet og Norges Bank, og i dialog med finansnæringen, og gi Stortinget en oppdatert orientering i neste års finansmarkedsmelding.

1 Finansdepartementet (2017a).
2 Finansdepartementet (2018a).

BRUKEN AV KONTANTER I NORGE OG ANDRE LAND

Norges Bank har gjennomført spørreundersøkelser om hvordan norske husholdninger betaler. Undersøkelser i 2017 og 2018 indikerer at kontantbetalinger utgjør 11 prosent av betalingene på utsalgssteder.[1] I lignende undersøkelser fra 2007 og 2013 utgjorde kontantbetalingene henholdsvis 24 og 15 prosent av antall betalinger på utsalgssteder.

Selv om den samlede bruken av kontanter i Norge faller, er bruken i enkelte bransjer fortsatt betydelig. Tall fra dagligvarebransjen i Norge viser at kontantene står for 20–25 prosent av antall betalinger.[2]

I de skandinaviske landene er kontantbruken svært lav sammenlignet med andre land. Tabell 1 viser resultater fra spørreundersøkelser rettet mot husholdningene i ulike land. I enkelte av eurolandene utgjør betalinger med kontanter opp mot 90 prosent av de samlede betalinger på utsalgssteder. Det er en del ulikheter i metodevalg, hvilke typer betalinger som er inkludert i de ulike undersøkelsene og tidspunktene undersøkelsene ble gjennomført, slik at tallene ikke er fullstendig sammenlignbare.[3]

Tabell 1. Kontantbruk i utvalgte land

Land	Periode	Kontantandel i prosent (antall)
Euroområdet totalt	2014–2016	79
- Hellas	2015–2016	88
- Italia	2015–2016	86
- Tyskland	2014	80
- Frankrike	2015–2016	68
- Finland	2015–2016	54
- Nederland	2016	45
Storbritannia	2016	44
USA	2016	31
Danmark	2017	23
Sverige	2018	13
Norge	2017–2018	11

Kilder: Danmarks Nationalbank, ESB, Federal Reserve Bank of San Francisco, Sveriges Riksbank, UK Finance og Norges Bank

1 Se Norges Bank (2018c) for mer informasjon om undersøkelsene.
2 Aera (2018).
3 Norges Bank (2018c).

2 Utviklingstrekk

2.1 ENDRET BETALINGSLANDSKAP

Betalingssystemet er i endring langs flere dimensjoner. Bruken av kontanter er på vei ned, mens kontopenger blir tilgjengelige i stadig flere former. Løsninger for oppgjør av realtidsbetalinger uten kredittrisiko for bankene er under utvikling. Nye aktører kommer til og utfordrer bankenes dominerende rolle i betalingssystemet.

Viktige drivkrefter bak utviklingen i betalingsmarkedet er ny teknologi, endret forbrukeratferd, internasjonalisering og ny regulering. Drivkreftene påvirker og forsterker hverandre.

- Bruken av kontanter er på vei ned, mens kontopenger blir tilgjengelige i stadig nye former. Brukerne forventer at betalingsløsningene skal følge teknologiutviklingen ellers i samfunnet. Smarttelefonen (mobiltelefonen) har fått en stor rolle i brukernes hverdag både for kommunikasjon, kjøp av varer og tjenester og etter hvert også for å gjennomføre betalinger. Det innebærer at brukerne har en forventning om at pengene skal kunne bli tilgjengelige på konto raskt og døgnet rundt.

- Aktørene i betalingssystemet tilpasser seg teknologiutviklingen. Det har ført til endringer i både aktørbildet, konkurransesituasjonen og verdikjeden. Globale teknologiselskaper utvikler betalingsløsninger med utgangspunkt i sine store kundenettverk og eierskap til teknologiske plattformer.[14]

- Nytt regelverk for betalingstjenester legger til rette for innovasjon og konkurranse gjennom regulert tilgang til betalingskontoer. Det åpner betalingsmarkedet opp for andre enn banker.

Mobile betalingsløsninger og umiddelbart oppgjør

Bruk av betalingsapplikasjoner på mobiltelefonen er i vekst. Mobiltelefonen kan benyttes til å gjøre opp i en rekke betalingssituasjoner, slik som ved betalinger mellom privatpersoner, netthandel, regningsbetaling og betaling på utsalgssted. Vi forventer å se utvikling av nye mobilbetalingstjenester og endret betalingsmønster i årene fremover, blant annet som følge av ny regulering.[15]

Finansnæringen har lenge jobbet med å finne løsninger som gjør at betalinger kan skje i samsvar med brukernes behov for umiddelbare oppgjør. Straksbetalinger, en løsning som sørger for at pengene kommer umiddelbart inn på mottakers konto, ble etablert i 2012. Mobilbetalingsløsningen Vipps legger nå til rette for at systemets brukere skal kunne benytte Straksbetalinger.

Løsningen for Straksbetalinger kan imidlertid ikke benyttes for alle typer betalinger og den innebærer kredittrisiko for bankene i oppgjøret. Bits AS (finansnæringens infrastrukturselskap) og Norges Bank samarbeider derfor om å utvikle en løsning for oppgjør av realtidsbetalinger uten kredittrisiko for bankene, såkalt BRO (Betalinger med Raskere Oppgjør). BRO-løsningen skal etter planen være på plass innen utgangen av 2019.[16]

I februar i år offentliggjorde syv nordiske banker at de vil utrede muligheten for en felles nordisk infrastruktur, i første omgang for realtidsbetalinger. Formålet er blant annet å redusere betalingskostnadene og sørge for bedre grensekryssende betalinger i Norden. Det pågår nå arbeid for å vurdere hvordan BRO-prosjektet vil påvirkes av dette initiativet. Saken reiser spørsmål som må utredes nærmere, både når det gjelder eventuell deltakelse i et utenlandsk interbanksystem og etablering av kritisk infrastruktur i utlandet. Norges Bank legger til grunn at en forbedret løsning for oppgjør av realtidsbetalinger i Norge ikke realiseres vesentlig senere enn det som har vært planlagt.

Endret markedsstruktur

Ny regulering (PSD2) pålegger bankene å åpne systemene sine slik at tredjepartsaktører kan tilby tjenester knyttet til betalinger og kontoinformasjon. PSD2 er både en respons på utviklingen i betalingsmarkedet og en katalysator for den videre utviklingen.[17] Flere store internasjonale teknologiselskaper, som Apple, Samsung og Google, er også på vei inn i betalingsmarkedet og kan vurdere å tilby mobilbetalingstjenester til norske kunder. Foreløpig har teknologiselskapenes betalingsløsninger kun blitt lansert i enkelte av de andre nordiske landene.

Fra en situasjon med flere mobile betalingsløsninger i markedet er Vipps nå den eneste norske mobile betalingsløsningen. Mot slutten av 2017 ble det kjent

14 Se ramme om digitale plattformer og nettverksfordeler.
15 Det reviderte betalingstjeneste direktivet PSD2.
16 Se Norges Bank (2017a) for mer informasjon om Straksbetalinger og BRO.
17 Norges Bank har avgitt høringsuttalelse til Finansdepartementet og Justis- og beredskapsdepartementet om forslag til regler som gjennomfører PSD2 i norsk rett, se Norges Bank (2017b) og Norges Bank (2017c).

at Vipps, BankAxept og BankID ønsker å fusjonere. Et av formålene er å stå sterkere i konkurransen mot globale selskaper. BankID benyttes til signering og identifisering for en lang rekke private og offentlige tjenester. BankAxept, bankenes nasjonale debetkortsystem, er det mest benyttede kortsystemet i Norge. Samtidig som fusjonen kan gi stordriftsfordeler, kan den også skape hindringer for andre aktører som vil etablere seg innenfor den samme verdikjeden. Fusjonen forutsetter godkjenning av Konkurransetilsynet og Finansdepartementet. Konkurransetilsynet godkjente fusjonen 27. april 2018. Fusjonen er til behandling i Finanstilsynet, som forbereder saken for Finansdepartementet.

Selv om flere utviklingstrekk legger til rette for økt konkurranse, er det også mekanismer som på sikt kan svekke konkurransen. Et eksempel er at én eller noen få globale aktører blir dominerende tilbydere av betalingstjenester på internasjonalt nivå, se også ramme om digitale plattformer og nettverksfordeler. Videre kan aktører som kontrollerer deler av betalingsinfrastrukturen, stenge konkurrerende aktører ute. Et eksempel er at kun Apple Pay får benytte nærfeltskommunikasjon (NFC) for kontaktløse betalinger på Apples mobiltelefoner.

En viktig infrastruktur for mobilbetalinger er såkalte aliasregistre som kobler sammen kontonumre og telefonnumre. Et felles register for alle aktører som yter betalingstjenester vil legge til rette for høy registerkvalitet, like konkurransevilkår og interoperabilitet på tvers av aktører og systemer.

Felles løsninger, standarder og tidlig bruk av ny teknologi har gitt en effektiv finansiell infrastruktur i Norge. Nye aktører i bank- og betalingssystemet kan bedre effektiviteten ytterligere. Konkurransen bør imidlertid fortsatt foregå innenfor rammen av felles infrastruktur.

DIGITALE PLATTFORMER OG NETTVERKSFORDELER[1]

I en tradisjonell forretningsmodell skapes verdi sekvensielt i hvert ledd i en kjede. Et selskap kjøper inn råvarer fra sine leverandører, bearbeider disse og selger varene videre til kunder. I et selskap med en plattform som forretningsmodell skapes verdi i interaksjonen mellom tilbydere og konsumenter.

Plattformer er ikke noe nytt i seg selv. Eksempel på en tradisjonell plattform er en børs eller et kjøpesenter hvor kjøpere og selgere møtes. Men digitale plattformer kan skaleres i mye større grad. Kjente eksempler på digitale plattformer er Google, Facebook og Finn.no.

Digitale plattformer har sterke nettverkseffekter. Et stort antall brukere gjør det også lønnsomt for andre tjenestetilbydere (tredjeparter) å utvikle komplementære tjenester. Nettverksfordelene kan bidra til at dominerende plattformer får en nær-monopolsituasjon. Det kan svekke konkurransen om plattformselskapene utnytter sin markedsmakt.

De siste årenes teknologiske utvikling, med blant annet smarttelefoner og sosiale medier, har vært viktig for utbredelsen av digitale plattformer. Plattformene søker å oppnå konkurransemessige fortrinn ved å redusere eller fjerne tidkrevende oppgaver og komplekse steg. Et eksempel er Vipps, som har forenklet betalinger mellom privatpersoner. Samtidig trekker ledende plattformer til seg kunder basert på at de allerede har mange kunder, og ikke nødvendigvis fordi de er best. Slike innlåsingseffekter kan hemme konkurranse og motvirke at bedre teknologiske løsninger vinner fram.

1 Se Ameln og Songe-Møller (2018).

2.2 KRYPTOAKTIVA OG DESENTRALISERT TEKNOLOGI

Det finnes et stort antall kryptoaktiva, også kjent som kryptovaluta, og nye kommer stadig til. Det er finansiell, juridisk og operasjonell risiko forbundet med kryptoaktiva, og finanstilsynsmyndigheter nasjonalt og internasjonalt har advart mot investeringer i slike aktiva. Norges Bank vurderer fortløpende om utviklingen innen kryptoaktiva kan utgjøre en risiko for finansiell stabilitet og om det er behov for regulering. Den underliggende, desentraliserte teknologien har potensielle bruksområder innenfor finansiell infrastruktur.

Penge- og betalingsfunksjoner

Kryptoaktiva og desentralisert teknologi har fått stor oppmerksomhet de siste årene. En stor andel kryptoaktiva assosieres med penge- og betalingsfunksjoner ved at de utgjør egne betalingsmidler og betalingssystemer. For noen kryptoaktiva er betalingsmiddelet kun et virkemiddel for å sikre driften av andre tjenester som nyttiggjør den desentraliserte teknologien. For eksempel kan kryptoaktiva fungere som betaling for prosessering av automatiserte kontrakter (såkalte smartkontrakter).

Kryptoaktiva som er utviklet for å fylle penge- og betalingsfunksjonen mangler imidlertid sentrale egenskaper penger og et betalingssystem må ha for å dekke behovet til et bredt publikum. Penger skal fungere som byttemiddel, verdioppbevaring og måleenhet. Særlig de store verdisvingningene fra dag til dag gjør kryptoaktiva lite egnet som penger. Prisvekst og verdisvingninger har snarere gjort kryptoaktiva attraktivt som spekulasjonsobjekt. At kryptoaktiva

NÆRMERE OM KRYPTOAKTIVA OG DESENTRALISERT TEKNOLOGI

Kryptoaktiva er kjennetegnet ved kryptografi og desentraliserte registre. Krypteringsnøkler benyttes for å godkjenne transaksjoner, og fører til at deltakerne i utgangspunktet kan opptre anonymt[1]. Informasjonen i systemet distribueres til alle deltakerne og lagres som et delt register (regnskapssystem) som oppdateres av brukerne selv. Systemet er organisert slik at integriteten til registeret blir ivaretatt uten behov for en sentral aktør. Dette omtales ofte som desentralisert teknologi.

Mange kryptoaktiva benytter såkalt blokkjedeteknologi for å ivareta integriteten til det desentraliserte registeret. Deltakere som ønsker det, kan konkurrere om å samle nye transaksjoner i nettverket i blokker og validere at disse er gyldige og konsistente med foregående blokker av transaksjoner (blokkjeden). Nye enheter av en kryptoaktiva utvinnes ved at deltakere som validerer blokker løser energikrevende kryptografiske «puslespill». Gyldige blokker blir belønnet i form av nyutstedte enheter av en kryptoaktiva (derav begrepet utvinning) og/eller inntekter fra transaksjonsgebyrer knyttet til den aktuelle blokken. Validering av blokker krever mye ressurser samtidig som gevinsten går tapt om en blokk ikke blir akseptert og bygget videre på i etterfølgende valideringer. Slik skaper systemet insentiver til at blokkjeden oppdateres med gyldige transaksjoner.[2] En nærmere beskrivelse av blokkjedeteknologi er gitt i Norges Bank (2014) og Norges Bank (2016).

De fleste kryptoaktivaene er åpne for at alle kan delta. Det skjer i tillegg en utvikling av kryptoaktiva med tilgangsregulert deltakelse, se også ramme om bruk av desentralisert teknologi i finansiell infrastruktur.

1 Transaksjonsanalyse kan imidlertid brukes til avdekke informasjon om deltakernes identitet.
2 Det er utviklet mekanismer for validering av blokkjeder som krever mindre ressurser. Det finnes også alternativ desentralisert teknologi som ikke er basert på blokkjeder.

som regel ikke er en fordring på noen, skaper grunnleggende utfordringer knyttet til å skape tillit og verdifasthet. I et effektivt betalingssystem skjer betalingene raskt, sikkert, kostnadseffektivt og i tråd med brukernes behov. Prosesseringskapasiteten til kryptoaktivaene som benyttes i dag er begrenset. Prosesseringen tar lang tid og systemene krever mye av deltakerne for at sikkerheten skal ivaretas. Teknologien må derfor utvikles videre før den er konkurransedyktig mot moderne, sentraliserte betalingssystemer for et bredt publikum.

Manglende egenskaper for å fungere som penger og betalingssystem for et bredt publikum gjør at flere sentralbanker bruker betegnelsen kryptoaktiva i stedet for kryptovaluta.[18]

18 Carney (2018).

Finansiell risiko

Store prissvingninger kombinert med usikker økonomisk verdsetting gjør at det er stor finansiell risiko forbundet med investeringer i kryptoaktiva. Det står verken en sentralbank eller andre institusjoner bak som garanterer for eller fremmer stabilitet i verdien. Investorer som har kjøpt mens prisen var lav har tjent store summer, men verdien kan falle raskt, også til null. Noen har også tapt investeringene som følge av cyberkriminalitet og usikre kryptoaktivabørser. Finanstilsynsmyndigheter i mange land, inkludert i Norge, har advart mot investeringer i kryptoaktiva.[19]

Mange av de nye kryptoaktivaene har blitt satt i sirkulasjon gjennom en såkalt «Initial Coin Offering» (ICO), der investorer kan kjøpe enheter av en kryptoaktiva

19 Finanstilsynet (2013) og Finanstilsynet (2018).

BRUK AV DESENTRALISERT TEKNOLOGI I FINANSIELL INFRASTRUKTUR

Desentralisert teknologi har mange potensielle bruksområder innenfor finansiell infrastruktur. Et felles desentralisert register over finansielle beholdninger kan gi økt effektivitet fordi aktørene slipper å avstemme egne registre mot hverandre og det kan redusere motpartsrisiko. Operasjonell risiko kan også reduseres ved at slik teknologi ikke er avhengig av at en sentral part er i drift. I Norges Bank (2016) ble ulike potensielle bruksområder omtalt. Siden har bruksområdene blitt utviklet videre:

- Den australske børsen ASX annonserte i pressemelding 7. desember 2017 at den vil erstatte det eksisterende systemet for avregning og oppgjør med et nytt system basert på desentralisert teknologi.[1] ESMA og ECB har redegjort for potensielle anvendelsesområder for desentralisert teknologi i verdipapirmarkedene mer generelt.[2]

- «Project Stella» er et samarbeid mellom den europeiske sentralbanken og den japanske sentralbanken om hvordan man kan organisere et sikkert system for levering mot betaling (DvP) der aktivaene ligger henholdsvis på et felles desentralisert register og på hver sine desentraliserte registre.[3]

- Japanske banker har vurdert å bruke desentralisert teknologi i oppgjøret mellom banker.[4] Enkelte sentralbanker, som den kanadiske, har vurdert og testet teknologien til bruk for oppgjør i sentralbanken.[5]

Det er imidlertid utfordringer knyttet til bruk av desentralisert teknologi i oppgjøret mellom banker, blant annet at teknologien er umoden og at konfidensiell informasjon ikke skal gjøres tilgjengelig for uvedkommende.

Norges Bank følger utviklingen innen desentralisert teknologi, og vurderer om teknologien kan bidra til økt effektivitet for betalingssystemer og annen finansiell infrastruktur under Norges Banks ansvarsområde.

1 ASX (2017).
2 ESMA (2017a) og ECB (2018).
3 ECB (2018).
4 Ripple (2017).
5 Chapman et. al. (2017) og Bech og Garratt (2017).

på et tidlig stadium. Midlene kan brukes til å videreutvikle en kryptoaktiva, samtidig som investorene gis insentiver til å promotere denne. Slike investeringer har stor finansiell risiko. ESMA, den europeiske verdipapir- og markedstilsynsmyndigheten, og Finanstilsynet har advart om risikoen ved ICO-investeringer.[20] De har blant annet pekt på manglende investorbeskyttelse, muligheten for svindel og hvitvasking. Flere land har tatt initiativ til å regulere ICO-er, samt skape klarhet i hvilken grad de rammes av verdipapirregelverket.

Juridisk og operasjonell risiko

Det juridiske rammeverket rundt kryptoaktiva er ikke fullt utviklet. Det er usikkert i hvilken grad investorer er rettslig beskyttet. Det er også risiko knyttet til det rettslige ansvaret ved å være en deltaker i systemet. Ved å være en bidragsyter til at transaksjoner distribueres i nettverket, kan en deltaker bli del av en hvitvaskingsoperasjon. Videre er det operasjonell risiko. Mange kryptoaktiva er ikke tilstrekkelig testet for funksjonene de skal fylle. Utvikling av ny teknologi, som blant annet kvantedatamaskiner og kunstig intelligens, kan utnyttes på en måte som kan true integriteten i systemene.[21]

Systemrisiko

FSB konkluderer med at kryptoaktiva ikke utgjør noen global finansiell risiko i dag.[22] Dette er i samsvar med flere sentralbankers vurderinger.[23] På sikt kan denne konklusjonen endre seg, og i litteraturen[24] pekes det på flere måter kryptoaktiva kan true finansiell stabilitet:

- Kjøp av kryptoaktiva finansieres med gjeld.
- Finansinstitusjoner holder store usikrede beholdninger i kryptoaktiva.
- Kryptoaktiva benyttes som sikkerhet for oppgjør i store finansielle transaksjoner.
- Kryptoaktiva får en vesentlig rolle i betalingssystemet eller verdipapiroppgjøret.

Betydningen for den finansielle stabiliteten kan øke ved framvekst av finansielle derivater basert på kryptoaktiva. Slike derivater ser i økende grad ut til å bli utviklet internasjonalt.

Norges Bank vurderer fortløpende om utviklingen innen kryptoaktiva kan utgjøre en risiko for finansiell stabilitet i Norge og behovet for regulering, se avsnitt om regulering nedenfor. FSB vil utvikle metoder for å vurdere systemisk risiko knyttet til kryptoaktiva.[25] Et slikt metodeverk vil være nyttig for det videre arbeidet i Norges Bank.

Regulering av kryptoaktiva

Mange land har innført særskilte reguleringer for handel med kryptoaktiva eller vurderer slike reguleringer. Både formålet med regulering og valg av virkemiddel kan variere fra land til land, se ramme om reguleringsstrategier for kryptoaktiva på side 27.

En utfordring med regulering av kryptoaktiva er håndheving. Kryptoaktiva med åpen deltakelse har fravær av en sentral aktør, og deltakerne er mer eller mindre anonyme og spredt over landegrensene. Det fører til at andre aktører i verdikjeden, som for eksempel kryptoaktivabørser, må reguleres i stedet. Det samme gjelder tradisjonelle finansinstitusjoner dersom disse involverer seg i kryptoaktiva. For kryptoaktiva med tilgangsregulert deltakelse er imidlertid mulighetsrommet for regulering større, ettersom deltakerne er kjente og det finnes en sentralisert styringsstruktur som kontrollerer tilgang og utvikling av systemet.

Kryptoaktiva er fortsatt et relativt nytt fenomen. Kunnskapsnivået om hvordan markedene fungerer og hvordan reguleringer bør utformes er lavt sammenliknet med mange andre deler av økonomien. Det øker risikoen for at reguleringer kan virke feil og dessuten hemme innovasjon og utvikling. Regulering bør prioriteres der samfunnets behov er klart. Kriminalitetsbekjempelse og forbrukervern er eksempler på slike behov i dag.

Norges Bank vil vurdere behov for regulering for å motvirke risikoer som kan true finansiell stabilitet (systemrisiko) og effektiviteten i betalingssystemet. Det er for tidlig å si hvilke reguleringer som kan bli aktuelle. Som omtalt over, vil kryptoaktiva først og fremst få betydning for finansiell stabilitet om de inngår i balansen til tradisjonelle finansinstitusjoner og om de tas i bruk av operatører for finansiell infrastruktur. Norges Bank vil derfor følge særlig med på

20 ESMA (2017a) og Finanstilsynet (2017b).
21 Se kapittel 1.1 om cybersikkerhet.
22 FSB (2018).
23 Se for eksempel Carney (2018).
24 Se for eksempel Ali et al. (2014), He et al. (2017) og FSB (2018).
25 FSB (2018).

hvordan disse institusjonene involverer seg i kryptoaktiva, og vil vurdere om slik involvering bør reguleres.

Kryptoaktiva og tjenester basert på desentralisert teknologi er ofte grenseoverskridende. Samarbeid på tvers av reguleringsmyndigheter er viktig for å sikre et konsistent regelverk. Flere internasjonale sentralbankorganer diskuterer regulering av kryptoaktiva og desentralisert teknologi.[26] Andre myndigheter har også samarbeidsfora hvor regulering diskuteres. Blant annet deltar Finanstilsynet i samarbeidsgrupper i regi av ESMA.

26 Se blant annet CPMI (2015), CPMI (2017) og FSB (2017a).

REGULERINGSSTRATEGIER FOR KRYPTOAKTIVA[1]

Kryptoaktiva kan reguleres på flere måter:

Informasjonstiltak
Informasjonstiltak er en mild form for regulering. Finansmyndighetene i mange land, inkludert i Norge, har valgt å advare brukerne om risikoen ved å investere i kryptoaktiva. Slike advarsler vil kunne avhjelpe problemer med asymmetrisk informasjon, men kan være mindre effektive for å løse andre problemer, slik som bruk av kryptoaktiva til hvitvasking.

Tolkning og tilpasning av gjeldende regelverk
Ofte finnes det allerede et gjeldende regelverk som kommer til anvendelse. For eksempel kan ICO-er rammes av ulike deler av verdipapirregelverket og skatteregler kommer til anvendelse for investorer. I EU ble det i desember 2017 oppnådd politisk enighet om å gjøre endringer i det fjerde hvitvaskingsdirektivet, slik at handel med kryptoaktiva ble omfattet. Det kan ofte være usikkerhet om i hvilken grad et gjeldende regelverk omfatter tjenester knyttet til kryptoaktiva, og myndighetene har i slike tilfeller en rolle for å klargjøre hvordan regelverket skal praktiseres.

Særregulering
Mange land har valgt å innføre særskilte reguleringer for visse typer virksomhet som er involvert i kryptoaktiva. Blant annet er handelsplasser, slik som kryptoaktivabørser, blitt underlagt regulering. Ved innføring av særreguleringer er det viktig å beholde konsistensen til annet regelverk.

Forbud
Forbud, for eksempel mot alle transaksjoner i kryptoaktiva, kan sees på som en ekstrem form for særregulering. Slike forbud må eventuelt innføres med varsomhet. Forbud kan utløse uheldige omgåelser av regelverket, samtidig som at det er så inngripende at det kan hindre ønsket innovasjon og utvikling, også innen annen desentralisert teknologi.

Helhetlig regelverk
Et helhetlig regelverk vil kunne bidra til en konsistent regulering av kryptoaktiva på tvers av reguleringsområder. Samtidig må et helhetlig regelverk for kryptoaktiva også være konsistent med regelverk for andre finansielle tjenester for å unngå uheldige konkurransevridninger. Kunnskapsnivået bør økes før et slikt regelverk vurderes. Norges Bank kjenner ikke til land som har valgt en slik tilnærming til regulering av kryptoaktiva.

1 Basert på kategorisering i CPMI (2015).

Digitale sentralbankpenger[1]

Digitale sentralbankpenger (DSP) er elektroniske penger utstedt av sentralbanken som er tilgjengelige for publikum. Ingen sentralbanker i industriland har innført DSP. Men flere sentralbanker, også Norges Bank, analyserer om det er fornuftig å innføre DSP og i tilfelle i hvilken form.

Motivasjonen for å vurdere DSP varierer mellom sentralbanker og avhenger av forhold i det enkelte land. Et særlig trekk ved Norge er lav og fallende kontantbruk.

Kontantbruken er likevel betydelig, og kontantene vil være med oss i overskuelig fremtid. Men det kan ikke utelukkes at kontantbruken på et tidspunkt blir såpass lav at kontantene er marginalisert som allment tilgjengelig betalingsmiddel. Vi må derfor vurdere om det er noen viktige egenskaper ved kontanter som bankinnskudd ikke vil kunne videreføre, og om det er behov for andre sentralbankpenger i tillegg til kontanter.

Kontantene har flere egenskaper:

- De er et kredittrisikofritt alternativ til kontopenger. Det gir publikum en mulighet til å trekke sine innskudd ut av bankene, noe som i seg selv kan opprettholde tilliten til bankinnskudd. De bidrar også til konkurranse blant betalingsmidlene. Kredittrisikofritt betyr ikke at kontanter er uten risiko for tyveri og annet tap eller kostnader ved å få tak i dem.
- De er en uavhengig beredskapsløsning om de elektroniske systemene er nede. Kontantene er ikke avhengig av teknologi eller en tredje part i betalingsøyeblikket.
- De er tvungent betalingsmiddel som kan brukes av alle. At et betalingsmiddel er tvungent, betyr at en part i en handel kan kreve at en handel gjøres opp med dette betalingsmiddelet, dersom partene ikke har avtalt noe annet. Når kontopenger kan byttes til kontanter (tvungent betalingsmiddel), bidrar det til publikums tillit til kontopenger.
- Kontantbruken er ikke sporbar og bidrar slik sett til personvern. På den andre siden kan manglende sporbarhet gjøre det mer krevende å avdekke visse typer kriminalitet.

For Norges Bank er det et spørsmål om DSP er nødvendig og ønskelig for å sikre at vi også i fremtiden har et sikkert og effektivt betalingssystem og tillit til pengevesenet. Vi må derfor stille oss spørsmålene:

- Hvilke egenskaper ønsker vi at betalingssystemet skal ha i fremtiden?
- Er det en risiko for at viktige egenskaper vil mangle, og tilliten til pengevesenet svekkes, om ikke Norges Bank eller andre myndigheter foretar seg noe?

1 Se Norges Bank (2018d) for en bredere drøfting av DSP.

- Hvis ja, er DSP det beste virkemiddelet for å oppnå ønskede egenskaper?

- Er det noen andre egenskaper som DSP har, som vi ikke ønsker?

Norges Bank må også vurdere om det kan oppstå situasjoner der DSP er nødvendig for å redusere faren for at norske kroner substitueres med andre valutaer.

Det er primært to hovedmodeller for å organisere et DSP-system:

- En **verdibasert modell** er kjennetegnet av at pengene er lagret lokalt i et betalingsinstrument, typisk betalingskort eller betalingsapplikasjon på en smarttelefon. Betalingene skjer direkte mellom partene, uten å gå veien om en sentral tredje part. Slik sett ligner en verdibasert modell på kontanter.

- En **kontobasert modell** er kjennetegnet ved at både lagringen av verdier og håndteringen av betalinger er sentralisert. Pengene ligger på kontoer og flytter seg fra én konto til en annen i systemet, slik som for betalinger med bankinnskudd.

Det kan også være mellomløsninger med elementer fra begge hovedmodellene. Bruk av desentralisert teknologi har potensial, blant annet for beredskapsformål. Teknologien er imidlertid umoden, se nærmere omtale i kapittel 2.2.

DSP kan ha konsekvenser for de private bankenes balanse og finansiering, strukturen i banksektoren, finansiell stabilitet, pengepolitikken og sentralbankens balanse og risiko. Konsekvensene av DSP vil avhenge av den konkrete utformingen og formålet med DSP.

Mange forhold må tas hensyn til ved utformingen av en eventuell DSP. Norges Bank vil i tiden fremover nærmere vurdere:

- Formål med DSP,

- hvilken type løsning for DSP som best oppnår formålene,

- konsekvensene av DSP-løsninger og

- den samfunnsøkonomiske nytte-kostnadsvurderingen av DSP.

Norges Bank vil i arbeidet ha kontakt med sentralbanker, akademia og andre nasjonale og internasjonale aktører. Dette er langsiktig arbeid og det er for tidlig å trekke noen konklusjoner om innføring av DSP.

3 Tilsyn og overvåking

3.1 NORGES BANKS ARBEID MED TILSYN OG OVERVÅKING[27]

Tilsyn

Norges Bank fører tilsyn med avregnings- og oppgjørssystem for pengeoverføringer mellom banker (interbanksystem). Norges Bank gir konsesjon og fører tilsyn med at interbanksystemene etterlever betalingssystemloven og konsesjonsvilkår. Dersom Norges Bank oppdager forhold som er i strid med betalingssystemloven eller konsesjonsvilkårene, vil Norges Bank pålegge interbanksystemene å rette opp forholdene. I ytterste konsekvens kan Norges Bank trekke tilbake konsesjonen.

Norges Bank fører tilsyn med:
- Norwegian Interbank Clearing System (NICS).
- Oppgjørsbanksystemet til DNB Bank ASA (DNB).

Norges Bank kan gi unntak fra kravet om konsesjon til interbanksystemer som vurderes å ha begrenset betydning for finansiell stabilitet. Oppgjørsbanksystemet til SpareBank 1 SMN har et slikt unntak.

Overvåking

Norges Bank overvåker systemene i den finansielle infrastrukturen. Overvåkingen bygger på sentralbankloven § 1 og internasjonale prinsipper for systemer i den finansielle infrastrukturen.[28] Dersom Norges Bank avdekker forhold som hemmer effektiviteten, vil Norges Bank oppfordre systemeier om å rette opp svakhetene, og eventuelt ta opp dette med relevant tilsynsmyndighet.

Norges Bank overvåker:
- Norges Banks oppgjørssystem (NBO).
- Oppgjørsbanksystemet til SpareBank 1 SMN.
- Registerfunksjonen til Verdipapirsentralen (VPS), i samarbeid med Finanstilsynet.
- Verdipapiroppgjøret (VPO), i samarbeid med Finanstilsynet.
- De tre sentrale motpartene LCH Ltd (LCH), EuroCCP N.V. (EuroCCP) og SIX x-clear Ltd (SIX x-clear). Dette skjer i samarbeid med Finanstilsynet og andre lands myndigheter.
- CLS Bank International (CLS). Norges Bank deltar i en komité med representanter fra relevante sentralbanker som overvåker CLS. Overvåkingsarbeidet er ledet av den amerikanske sentralbanken.

27 Se omtale av Norges Banks ansvar på side 3.
28 CPMI-IOSCO (2012).

Nærmere om NBO

Betalingssystemlovens bestemmelser om tilsyn med interbanksystemer gjelder ikke for Norges Banks oppgjørssystem (NBO). Norges Bank overvåker NBO. Overvåkingen og driften av NBO er plassert i ulike organisatoriske enheter i Norges Bank. Etter beslutning i 2017 er det klargjort at forsvarslinjen i NBO sin risikostyring ikke er en del av overvåkingen som gjengis i denne rapporten. En konsekvens av dette er at prinsipp 2 (styringsstruktur), prinsipp 3 (rammeverk for risikostyring) og enkelte av hovedhensynene i prinsipp 17 (operasjonell risiko) ikke lenger vurderes av enheten som overvåker NBO.

Vurdering etter internasjonale prinsipper

Norges Bank evaluerer systemene som er underlagt tilsyn og overvåking etter internasjonale prinsipper utarbeidet av CPMI-IOSCO.[29]

Samarbeid med Finanstilsynet

Finanstilsynets tilsynsvirksomhet og Norges Banks tilsyns- og overvåkingsarbeid er delvis overlappende. Norges Bank samarbeider derfor med Finanstilsynet. Mens Norges Bank har ansvar for å følge opp interbanksystemer, følger Finanstilsynet opp kunderettede systemer for betalingstjenester.

Tabell 3.1 gir en oversikt over de ulike systemene i den finansielle infrastrukturen med tilhørende tilsyns- og overvåkingsorgan.

29 Se ramme om internasjonale myndigheter og sentrale motparter på side 35.

BETALINGSSYSTEMLOVENS DEFINISJONER

Betalingssystemer er interbanksystemer og systemer for betalingstjenester.

Interbanksystemer er systemer for overføring av penger mellom banker med felles regler for avregning og oppgjør.

Systemer for betalingstjenester er systemer for overføring av penger mellom kundekontoer i banker eller hos andre som kan yte betalingstjenester.

Verdipapiroppgjørssystemer er systemer basert på felles regler for avregning, oppgjør eller overføring av finansielle instrumenter.

TABELL 3.1 Finansiell infrastruktur som er underlagt tilsyn eller overvåking

System	Instrument	Operatør	Tilsyn/overvåking	Forvaltningsorgan
Oppgjørssystemet til Norges Bank (NBO)	Penger	Norges Bank	Overvåking	Norges Bank
Norwegian Interbank Clearing System (NICS)	Penger	Bits AS	Tilsyn og overvåking	Norges Bank
Oppgjørssystemet til DNB Bank ASA	Penger	DNB Bank ASA	Tilsyn og overvåking	Norges Bank
Oppgjørssystemet til SpareBank 1 SMN	Penger	SpareBank 1 SMN	Overvåking	Norges Bank
Verdipapiroppgjørs-systemet (VPO)	Verdipapir Penger	Verdipapirsentralen ASA (VPS)	Tilsyn og overvåking	Tilsyn med VPS og VPO: Finanstilsynet Overvåking av VPO: Norges Bank
VPS' registerfunksjon	Verdipapir	VPS	Tilsyn og overvåking	Tilsyn med registerfunksjonen: Finanstilsynet Overvåking av registerfunksjonen: Norges Bank
Det sentrale motparts-systemet til SIX x-clear	Finansielle instrument	SIX x-clear Ltd. (SIX x-clear)	Tilsyn og overvåking	Tilsyn med SIX x-clear : Det sveitsiske finanstilsynet Overvåking: Den sveitsiske sentralbanken, Norges Bank og Finanstilsynet
Det sentrale motparts-systemet til LCH	Finansielle instrument	LCH Ltd. (LCH)	Tilsyn og overvåking	Tilsyn med LCH: Bank of England Overvåking av LCH: EMIR College og Global College, blant annet Norges Bank
Det sentrale motparts-systemet til EuroCCP	Finansielle instrument	EuroCCP N.V. (EuroCCP)	Tilsyn og overvåking	Tilsyn med EuroCCP: Den nederlandske sentralbanken Overvåking av EuroCCP: EMIR College, blant annet Norges Bank
CLS	Penger	CLS Bank International (CLS)	Tilsyn og overvåking	Tilsyn med CLS: Federal Reserve Overvåking av CLS: Sentralbanker med valuta i CLS, blant annet Norges Bank

Tilsyn og overvåking 2017/2018

Norges Bank har i tilsyns- og overvåkingsarbeidet det siste året lagt vekt på systemeiernes arbeid med cybersikkerhet og kontroll med utkontraktert virksomhet. Norges Bank vil fortsatt ha spesiell oppmerksomhet på disse områdene i 2018.

Cybersikkerhet

Overvåkingen av og tilsynet med cybersikkerhet tar utgangspunkt i den utfyllende veiledningen som CPMI-IOSCO publiserte på dette området i 2016. Systemeiernes organisering av arbeidet med cybersikkerhet, beskyttelse mot cyberrisiko og beredskap for cyberrisiko blir spesielt vektlagt i overvåkings- og tilsynsmøtene. Finanstilsynet er normalt til stede på disse møtene. Norges Bank har også deltatt på enkelte IKT-tilsyn med Finanstilsynet.

Utkontraktering

En arbeidsgruppe med representanter fra Finanstilsynet og Norges Bank kartlegger våren 2018 omfanget av utkontraktering i bank- og betalingssystemet. Kartleggingen skal blant annet gi grunnlag for å vurdere om utkontraktering svekker systemeiernes styring og kontroll med driften, se også omtale i ramme om kartleggging av utkontraktering i betalingssystemet på side 7.

Evaluering av norske systemer etter internasjonale prinsipper

Systemeierne gjennomførte i 2014 en selvevaluering opp mot prinsippene fra CPMI-IOSCO. På grunnlag av selvevalueringen og annen informasjon evaluerte Norges Bank systemene samme år. Etter 2014 har Norges Bank gjennomført årlige evalueringer av prinsippene som ikke har vært oppfylt. I tillegg har det blitt utført evalueringer ved endringer av systemene som kan påvirke vurderingen. Hovedkonklusjonen fra evalueringene til Norges Bank og Finanstilsynet er at norske systemer i stor grad oppfyller prinsippene.

Systemene blir evaluert etter de prinsippene som er relevante for systemet. Graden av oppfyllelse er basert på følgende kriterier:

- **Oppfylt:** Eventuelle mangler er ikke vesentlige.
- **I hovedsak oppfylt:** Systemet har én eller flere mangler som gir grunn til uro. Påpekte mangler bør være fulgt opp innen et fastsatt tidspunkt.
- **Delvis oppfylt:** Systemet har én eller flere mangler som kan bli alvorlige om det ikke rettes opp raskt. Arbeidet med å utbedre dette må gis høy prioritet.
- **Ikke oppfylt:** Systemet har én eller flere mangler som er så alvorlige at det er nødvendig med umiddelbar handling.
- **Ikke relevant:** Prinsippet er ikke relevant for systemet.

Norges Bank oppfordrer alle systemeiere til å rette opp avdekkede mangler. Norges Bank kan kreve at systemer underlagt tilsyn oppfyller prinsippene. Oppfølging av VPS/VPO skjer i samarbeid med Finanstilsynet.

Nærmere om vurderingene gjort i 2017/2018
Norges Bank har i 2017/2018 lagt vekt på systemeiernes organisering av arbeidet med cybersikkert. Systemeierne har gjort en evaluering opp mot veiledningen om cybersikkerhet (CPMI-IOSCO 2016). Det berører prinsipp 2 (styringsstruktur), prinsipp 3 (rammeverk for risikostyring), prinsipp 8 (finalitet), prinsipp 17 (operasjonell risiko) og prinsipp 20 (lenker mellom systemer). Norges Bank vil basert på evalueringene gjennomføre en vurdering i 2018/2019.

NICS, VPO og VPS er i tillegg blitt vurdert på følgende prinsipper:

NICS
Prinsipp 17 (operasjonell risiko) ble vurdert som i hovedsak oppfylt i 2017, som følge av mangler ved beredskapsløsningen. Norges Bank vil gjøre en ny vurdering av NICS opp mot prinsipp 17 i 2018.

VPO
Prinsipp 1 (juridisk grunnlag) og prinsipp 13 (prosedyrer ved mislighold) er i hovedsak oppfylt fordi VPS sine regler for å håndtere insolvens hos en deltaker er uklare. VPS har samarbeidet med oppgjørsenheten i Norges Bank om å endre reglene i tråd med Finansdepartementets forskrift av 22. september 2016 om gjennomføring av verdipapiroppgjøret. VPS og Norges Bank annonserte 15. mai 2018 at nytt regelverk vil tre i kraft 18. juni 2018.[1]

Prinsipp 3 (rammeverk for risikostyring) og 15 (forretningsrisiko) stiller krav om beredskapsplan for finansielle problemer. VPS vil ferdigstille en slik plan før foretaket søker om CSDR-autorisasjon. Inntil planen er sluttført, vurderer Norges Bank og Finanstilsynet de to prinsippene som i hovedsak oppfylt.

Prinsipp 19 (indirekte deltakelse) vurderes fortsatt som i hovedsak oppfylt fordi det er mangler ved kvantitative analyser og systematisk risikovurdering av indirekte deltakere.

Registerfunksjonen til VPS
Prinsipp 3 (rammeverk for risikostyring) og 15 (forretningsrisiko) gjelder både for VPO og VPS. De to prinsippene er i hovedsak oppfylt av samme grunn som nevnt under VPO.

Prinsipp 20 (lenker mellom systemer) er i hovedsak oppfylt fordi VPS ikke selv evaluerer lenker som innebærer at verdipapirer i et utenlandsk verdipapirregister blir delregistrerte i VPS. VPS vil oppfylle dette kravet før foretaket søker om CSDR-autorisasjon.

1 VPS (2018) og Norges Bank (2018e).

TABELL 1 Oppsummering av systemene mot prinsippene. Årstall markerer tidspunkt for siste evaluering

Prinsipp / type FMI	NBO	NICS	VPO	VPS register-funksjon	DNB (privat opp-gjørsbank)	SMN (privat opp-gjørsbank)
1. Juridisk grunnlag	2014	2014	2018	2014	2014	2014
2. Styringsstruktur		2017	2014	2014	2014	2014
3. Rammeverk for risikostyring		2015	2018	2018	2014	2014
4. Kredittrisiko	2014		2014		2014	2014
5. Sikkerhetsstillelse	2014					
6. Marginer						
7. Likviditetsrisiko	2014	2014	2014		2014	2014
8. Finalitet	2014	2014	2014		2014	2014
9. Pengeoppgjør	2014	2014	2014		2014	2014
10. Fysisk levering						
11. Verdipapirregistre				2014		
12. EoV-oppgjørssystem	2014		2014			
13. Deltakermislighold	2014	2014	2018	2014	2014	2014
14. Segregering og portabilitet						
15. Forretningsrisiko	2014	2014	2018	2018	2014	2014
16. Investeringsrisiko			2014	2014	2014	2014
17. Operasjonell risiko	2017[1]	2017	2014	2014	2014	2014
18. Tilgang og deltakerkrav	2014	2014	2014	2014	2014	2014
19. Indirekte deltakelse	2014		2018	2014		
20 Lenker mellom systemer			2014	2018		
21. Effektivitet	2014	2014	2014	2014	2014	2014
22. Kommunikasjon	2014	2014	2014	2014		
23. Publisering av informasjon	2014	2014	2014	2014	2014	2014
24. Transaksjonsregistre						

Forklaring til tabellen:
Oppfylt | I hovedsak oppfylt | Delvis oppfylt | Ikke oppfylt | Ikke relevant | Ikke del av overvåkingen av NBO[2]

1 Enkelte hovedhensyn i prinsippet er ikke vurdert, se nærmere omtale av overvåkingen av NBO på side 20.
2 Se nærmere omtale av overvåkingen av NBO på side 20.

3.2 INTERBANKSYSTEMER

Interbanksystemer er systemer for overføring av penger mellom banker, med felles regler for avregning og oppgjør.

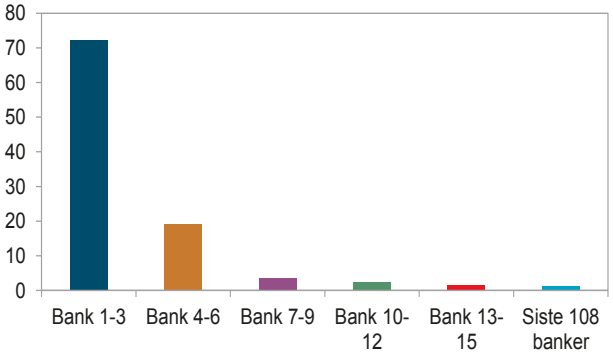
NBO – NORGES BANKS OPPGJØRSSYSTEM

Kort om systemet

Norges Bank er øverste oppgjørsbank i det norske betalingssystemet. I Norges Banks oppgjørssystem (NBO) foretas oppgjør mellom banker og andre institusjoner som har konto i Norges Bank. Alle betalinger i norske kroner blir i siste instans gjort opp i NBO, se figur 3.1.

I NBO gjøres betalinger opp både enkeltvis (brutto) og etter en avregning (netto). Mens nettooppgjørene skjer på fastlagte tidspunkter gjennom dagen, kan betalinger til bruttooppgjør gjøres opp på et hvilket som helst tidspunkt i åpningstiden til NBO.

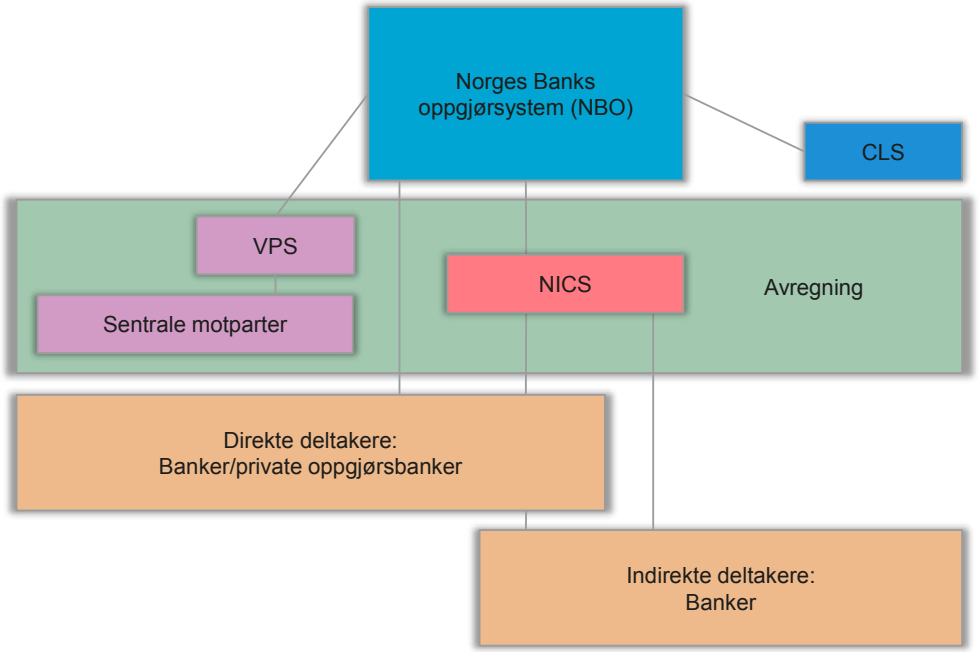
FIGUR 3.2 Andel bruttobetalinger foretatt av bankene. Prosent. 2017



Kilde: Norges Bank

Alle banker med konto i NBO kan sende betalinger til bruttooppgjøret, men de 15 største bankene står for 99 prosent av omsetningen, se figur 3.2. Analyser Norges Bank har gjennomført viser også at største-

FIGUR 3.1 Det norske betalingssystemet



Figuren gir ikke et fullstendig bilde

Kilde: Norges Bank

delen av omsetningen i bruttooppgjøret er knyttet til penge- og valutamarkedet, se ramme om kartlegging av omsetningen i Norges Banks oppgjørssystem på side 26.

Norges Bank gjør opp avregninger som kommer fra NICS, VPS og CLS, se figur 3.3. I avregningen fra NICS inngår i hovedsak betalinger fra privatpersoner, staten og bedrifter. Avregningen fra VPS er pengedelen av verdipapiroppgjøret. Avregningen fra CLS er finansieringen av norske kroner til valutaoppgjøret i CLS.

Banker kan delta direkte eller indirekte i oppgjørene i NBO. Indirekte deltakere gjør opp gjennom en korrespondentbank. Se nærmere omtale av direkte og indirekte deltakelse i ramme om kartlegging av omsetningen i Norges Banks oppgjørssystem på side 26.

Utkontraktering

Norges Bank har inngått avtale om rettighet til å benytte og få vedlikehold av systemet for NBO med det italienske selskapet SIA S.p.A. (SIA). Programvaren for NBO er utviklet av det sør-afrikanske selskapet Perago, som er eid 100 prosent av SIA. IKT-driften av oppgjørssystemet har siden 2003 vært utkontraktert til EVRY Norge AS.

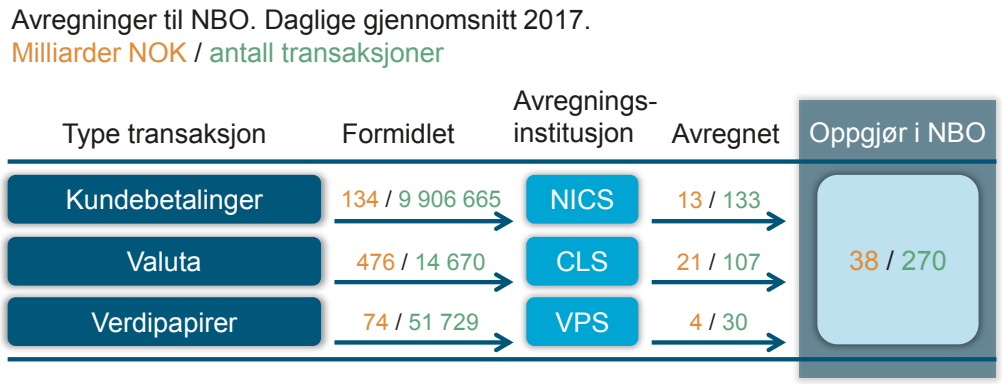
Stabiliteten i systemet

Driften av NBO har vært stabil det siste året, med unntak av teknisk svikt i september og oktober. Samme type tekniske feil førte til at NBO stoppet opp 29. september og 18. oktober 2017. Begge dagene førte feilen til at det ikke ble prosessert betalinger i om lag en halv time. 29. september ble 64 betalingsoppdrag på til sammen 12,4 milliarder kroner forsinket med inntil en halv time, mens tilsvarende tall for 18. oktober var 34 transaksjoner og 6,4 milliarder kroner. Feilen er rettet. Dette er den mest alvorlige feilen i NBO siden dagens oppgjørssystem ble tatt i bruk i 2009.

Overvåking

NBO har det siste året lagt vekt på cyberrisiko. I den forbindelse har oppgjørsenheten i Norges Bank gjennomført en egenevaluering mot veiledningen for cybersikkerhet fra CPMI-IOSCO (2016). Overvåkingsenheten i Norges Bank vil følge opp denne egenevalueringen i 2018.

FIGUR 3.3 Oppgjør av avregninger i NBO



Kilder: Bits, VPS, CLS og Norges Bank

Kartlegging av omsetningen i Norges Banks oppgjørssystem

Sentralbanker kjenner størrelsen på omsetningen i oppgjørssystemene, men har mindre kunnskap om formålet med transaksjonene og om transaksjonene er direkte eller indirekte (korrespondentbankbetalinger). Norges Bank har samlet inn data fra bankene, NBO, NICS og CLS og utviklet algoritmer for å analysere omsetningen i NBO. Basert på dette arbeidet kjenner Norges Bank nå andelen av direkte og indirekte betalinger og formålet for nær 80 prosent av omsetningen i NBO.[1]

Direkte deltakelse i oppgjørene bidrar til finansiell stabilitet.[2] En bank som deltar direkte, er ikke avhengig av andre banker i oppgjøret, mens den ved indirekte deltakelse trenger en korrespondentbank. Svikt i en korrespondentbank kan dermed ramme flere banker. Formålet med betalingene må tas med i vurderingen av konsekvensene av en svikt. Et bortfall av et oppgjør på ti milliarder kroner kan innebære at flere hundre tusen husholdninger rammes, eller det kan være én enkelt pengemarkedstransaksjon.

Norges Bank vurderer om hensynet til finansiell stabilitet tilsier at det bør settes grenser for indirekte deltakelse i NBO.[3] Norske banker har i samarbeid med Norges Bank etablert en løsning som sikrer oppgjør av vanlige norske kundebetalinger dersom en korrespondentbank (privat oppgjørsbank) svikter. En grense for indirekte deltakelse vil derfor eventuelt gjelde for store utenlandske banker som er aktive i det norske penge- og kredittmarkedet. Analysene som Norges Bank har gjennomført, vil være en del av beslutningsgrunnlaget i dette spørsmålet.

Penge- og kredittmarkedstransaksjoner dominerer omsetningen

Hoveddelen av omsetningen i NBO er knyttet til penge- og kredittmarkedet, samt handel med valuta, se figur 1. Om lag 9 prosent er kundebetalinger, som ofte er knyttet til kjøp av varer og tjenester.[4] Målt i beløp utgjør likevel innenlandske betalinger i gjennomsnitt 13 milliarder kroner av omsetningen i NBO hver dag. Bakenforliggende bruttoomsetning er i gjennomsnitt hele 134 milliarder kroner hver dag.[5]

Stor andel indirekte deltakelse i NBO

Informasjonen som Norges Bank har hentet inn, viser at indirekte deltakere står for en stor andel av omsetningen i NBO, se figur 2. Totalt gjøres det opp transaksjoner for i gjennomsnitt 212 milliarder kroner daglig og av dette er 81 milliarder kroner, eller 38 prosent, fra indirekte deltakere. Store internasjonale banker uten konto i Norges Bank står bak hovedtyngden av den indirekte omsetningen. I hovedsak er dette transaksjoner knyttet til valuta- og interbankmarkedet (lån til/fra andre banker). Innenlandsk betalingsformidling vil i liten grad bli rammet om store indirekte deltakere mister tilgangen til oppgjøret i NBO.

Korrespondentbankers egne transaksjoner utgjør størstedelen av omsetningen i NBO

Figur 3 viser de indirekte deltakernes andel av korrespondentbankenes egne transaksjoner i NBO:

- Grønne (kategori 1): Transaksjoner fra banker med konto i Norges Bank. Det er 7 utenlandske og ingen norske banker i denne kategorien.
- Oransje (kategori 2): Transaksjoner fra banker uten konto i Norges Bank. Det er 51 utenlandske banker og 1 norsk bank i denne kategorien.
- Blå (kategori 3): Transaksjoner fra banker med lav andel (maksimum 0,5 prosent) av omsetningen i korrespondentbankene. Det er 204 utenlandske og 126 norske banker i denne kategorien.

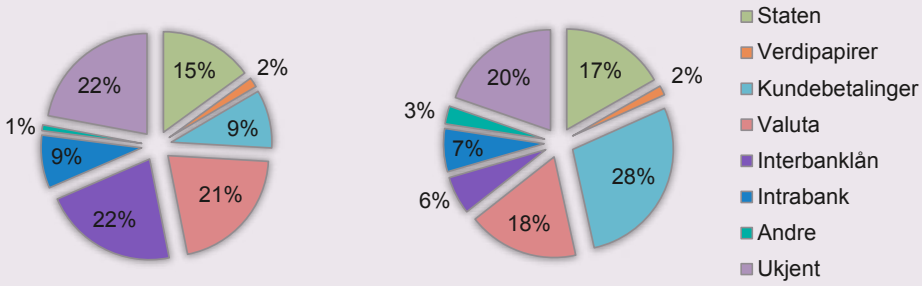
I kategori 1 og 2 er det vist med streker hvor stor hver enkelt indirekte deltaker er. En bank kan ha flere

1 Se Fevolden og Smith (2018) for mer informasjon om datasett, metode og resultater.
2 Prinsipp 19 i CPMI-IOSCO (2012) anbefaler at banker med stor omsetning deltar direkte.
3 Bank of England har satt grensen til to prosent av den totale omsetningen i oppgjøret eller 40 prosent av korrespondentbankens egne transaksjoner.
4 For 22 prosent av omsetningen kan vi ikke fastslå formålet helt presist, men det synes trygt å anta at omsetningen er knyttet til penge- og kredittmarkedet.
5 Se figur 3.3 i kapittel 3 av rapporten.

korrespondentbanker, slik at antallet streker i figuren ikke er i overensstemmelse med antall banker nevnt i punktene over.

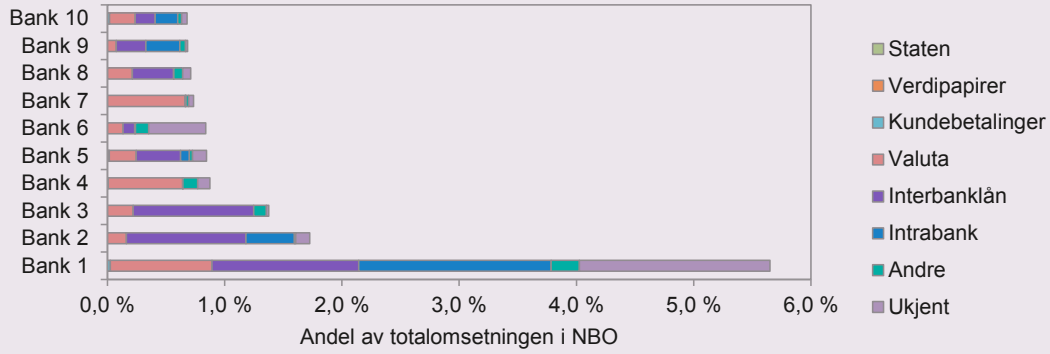
Den største indirekte deltakeren står for 34 prosent av korrespondentbankens egne transaksjoner. Dette er en utenlandsk bank uten konto i Norges Bank og den vises med en tykkere kantlinje i figuren.

FIGUR 1: Formålet med transaksjoner til oppgjør i NBO. Venstre: verdi, høyre: antall



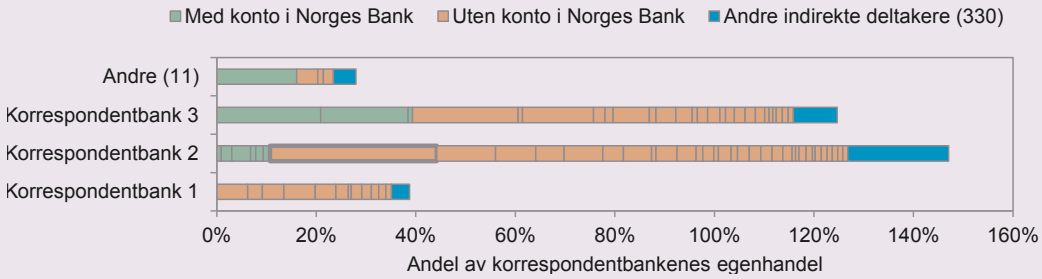
Kilde: Norges Bank

FIGUR 2: Formålet med transaksjonene til de 10 største indirekte deltakerne i NBO



Kilde: Norges Bank

FIGUR 3: Indirekte deltakeres andel av korrespondentbankenes egenhandel i NBO



Kilde: Norges Bank

NICS – NORWEGIAN INTERBANK CLEARING SYSTEM

Kort om systemet

NICS er bankenes felles system for avregning og mottak av betalingstransaksjoner. Nesten alle betalingstransaksjoner i Norge, herunder korttransaksjoner, blir sendt til NICS. De fleste transaksjonene som NICS mottar, inngår i en avregning. Det innebærer at det blir regnet ut en nettoposisjon for hver enkelt bank mot alle andre banker. Avregningsresultatet blir sendt til Norges Banks oppgjørssystem (NBO), hvor nettoposisjonene gjøres opp. Oppgjør av avregninger skjer fem ganger daglig på hverdager, henholdsvis kl. 05.30, 09.30, 11.30, 13.30 og 15.30.

Bankene sender også transaksjoner via NICS som ikke inngår i en avregning. Disse transaksjonene blir gjort opp enkeltvis (brutto) i NBO. Betalinger kan gjøres opp enkeltvis i hele åpningstiden i NBO, det vil si mellom kl. 05.30 og 16.35. Slike transaksjoner er typisk på over 25 millioner kroner.

Utkontraktering

Operatøren Bits AS har utkontraktert den tekniske driften av NICS til Nets Norge Infrastruktur (NNI). NNI benytter også andre selskaper i Nets-konsernet til å utføre driftsoppgaver.

Stabiliteten i systemet

Den tekniske driften av NICS har vært stabil de siste årene. Det siste året har det vært få avvik. NICS ble imidlertid berørt av en hendelse i Evry 6. oktober 2017 som førte til at mange banker verken fikk levert transaksjoner til NICS eller mottatt transaksjoner fra NICS. Hendelsen førte til at det oppstod tregheter i utsendelse av transaksjoner til banker som i utgangspunktet ikke var berørt av hendelse i Evry. Bits AS har opplyst til Norges Bank at svakheten som førte til tregheten er rettet opp. 24. april 2018 førte et avvik i NICS-systemet til at morgenoppgjøret ble utsatt mer enn to timer. Norges Bank følger opp hendelsen overfor Bits AS.

Tilsyn

Norges Bank mottok i 2016 søknad om overføring av operatøransvaret for NICS fra NICS Operatørkontor til Bits AS, blant annet fordi sistnevnte har større kapasitet og kompetanse. Bits AS er et infrastrukturselskap opprettet av Finans Norge i 2016. I juni 2017 fattet Norges Bank vedtak som ga Bits AS operatøransvaret for NICS. Konsesjonsvilkårene ble oppdatert i forbindelse med overføringen.

I november 2016 mottok Norges Bank en endringsmelding om overføring av enkelte driftsoppgaver fra Nets i Norge til Nets i Danmark. Oppgavene som ble flyttet omfattet blant annet systemovervåking. Bits AS fikk i september 2017 en midlertidig tillatelse til å gjennomføre endringen på visse vilkår. Ett av vilkårene er at det må opprettholdes en operativ beredskapsløsning i Norge med kompetanse og ressurser til straks å kunne overta driften.

I oktober 2017 mottok Norges Bank en endringsmelding fra Bits AS om flytting av ett av de to driftsstedene til NICS, slik at den geografiske avstanden mellom dem økte. Videre omfattet endringsmeldingen også etablering av nytt driftsoppsett for NICS med blant annet duplisering av driftsmiljøet på begge driftssteder. Økt avstand er positivt, da det reduserer risikoen for at samme hendelse skal ramme begge driftsstedene samtidig. Det nye driftsstedet er imidlertid samlokalisert med flere andre aktører i den finansielle infrastrukturen, noe som øker konsentrasjonsrisikoen i betalingssystemet. Endringsmeldingen ble tatt til etterretning.

Flyttingen av det ene driftsstedet er en del av en ny datasenterstrategi for NICS. Bits AS har tidligere vurdert behovet for et tredje driftssted for å forsterke kriseløsningene for NICS.[30] I følge Bits AS vil etablering av ny datasenterstrategi eliminere flere av de forhold som aktualiserte behovet for et tredje driftssted for NICS. Bits AS har derfor stilt vurderingen av et tredje driftssted i bero. Ved behandlingen av endringsmeldingen om flytting av det ene driftsstedet og endringer i driftsoppsettet har Norges Bank ikke vurdert om dette endrer behovet for et tredje driftssted. Norges Bank har bedt Bits AS om å snarlig redegjøre for prosessen for vurdering av behovet for et tredje driftssted.

I tilsynet med NICS har Norges Bank det siste året lagt særlig vekt på cybersikkerhet. I den forbindelse har Bits AS gjennomført en egenevaluering mot retningslinjene i CPMI-IOSCO (2016). Norges Bank har i etterkant av denne egenevalueringen etterspurt oppfølgingstiltak fra Bits AS.

Norges Bank vil gjøre en ny vurdering av NICS opp mot prinsipp 17 om operasjonell risiko i CPMI-IOSCO i 2018. Bits AS' redegjørelse for behovet for nytt driftssted og oppfølgingstiltak knyttet til cyberrisiko vil være viktige elementer i denne vurderingen.

30 Norges Bank (2017a).

PRIVATE OPPGJØRSBANKER

Kort om systemene

Det er tre private oppgjørsbanker i Norge som gjør opp for andre banker i NBO. DNB Bank ASA er oppgjørsbank for 91 banker, Sparebank 1 SMN for 10 banker og Danske Bank for én bank.

Banker som kalles private oppgjørsbanker, er banker som utfører korrespondentbanktjenester for andre banker i den innenlandske betalingsformidlingen. Det innebærer at de overtar posisjonene til andre banker etter avregninger i NICS og gjør opp på deres vegne i NBO. Etter oppgjøret i Norges Bank blir oppgjørskontoene til deltakerbankene belastet eller godskrevet i den private oppgjørsbanken.

Oppgjørssystemet til Danske Bank har et så begrenset omfang at Norges Bank ikke overvåker systemet.

Utkontraktering

Både DNB og Sparebanken 1 SMN har utkontraktert driften av sine oppgjørssystemer. Driftstjenestene leveres i hovedsak av Evry for begge oppgjørssystemene.

Stabiliteten i systemene

DNB hadde to avvik i oppgjørssystemet i 2017. Avvikene inntraff 16. mars og 15. juni. SpareBank 1 SMN hadde ett avvik 6. oktober. Verken avvikene i DNB eller i SpareBank 1 SMN fikk vesentlige konsekvenser. Feilene er rettet opp. Driftssituasjonen for oppgjørsbanksystemet til DNB og SpareBank 1 SMN har vært stabil det siste året utover de nevnte avvikene.

Tilsyn og overvåking

DNB har konsesjon fra Norges Bank for sitt oppgjørssystem. Norges Bank gjennomfører halvårlige tilsynsmøter med DNB om oppgjørsbanksystemet. Tema på møtene det siste året har blant annet vært utkontraktering og cyberrisiko. Vurderingen av cyberrisiko blir i hovedsak gjort etter veiledningen om cybersikkerhet fra CPMI-IOSCO. Norges Bank har også deltatt i IKT-tilsyn sammen med Finanstilsynet for å kunne vurdere om oppgjørssystemet til DNB er i tråd med veiledningen. Enkelte av temaene i veiledningen ble ikke behandlet i IKT-tilsynet til Finanstilsynet. Norges Bank har i samråd med Finanstilsynet sendt et brev til DNB hvor DNB blir bedt om å gjøre rede for disse temaene.

I mars 2017 mottok Norges Bank en endringsmelding om at DNB ville flytte deler av driften av oppgjørssystemet til utlandet. DNB fikk 15. september 2017 en midlertidig tillatelse til flytting på visse vilkår. Ett av vilkårene er at det må være en operativ beredskapsløsning i Norge med kompetanse og ressurser til straks å overta driften. DNB har ikke benyttet seg av tillatelsen så langt.

Sparebanken 1 SMN har fritak for konsesjon, og Norges Bank fører derfor ikke tilsyn med oppgjørsbanksystemet til denne banken. Norges Bank overvåker likevel virksomheten og gjennomfører regelmessige møter. På møtene gjennomgås blant annet driftssituasjonen, gjennomførte øvelser og eventuelle systemendringer. Et viktig tema på tilsynsmøtet i 2018 vil være cybersikkerhet.

CLS

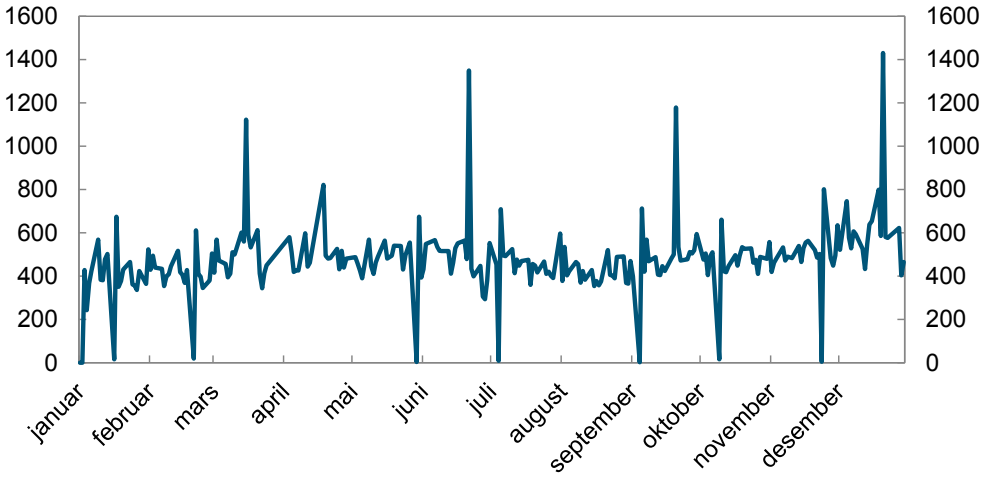
Kort om systemet

CLS Bank International (CLS) er en internasjonal oppgjørsbank for valutahandler. 18 valutaer blir gjort opp i CLS, blant annet norske kroner. På kontoene bankene har i CLS, blir hver enkelt valutahandel gjort opp enkeltvis (brutto). CLS regner ut en nettoposisjon for hver direkte deltaker i hver valuta. Inn- og utbetalinger av valuta mellom bankene og CLS skjer mellom deres kontoer i de ulike sentralbankene. En oppgjørsdeltaker uten konto i sentralbanken kan benytte en annen bank (korrespondentbank) for betalinger til og fra CLS. I januar 2017 introduserte CLS to nye medlemskapskategorier: oppgjørsmedlemskap for institusjoner som ikke eier aksjer i CLS og oppgjørsmedlemskap for flere enheter innen samme konsern.

Tradisjonelt er valutahandler blitt gjort opp i oppgjørssystem i ulike land og i ulike tidssoner. Partene har derfor hatt en risiko for at motparten ikke betaler inn sin del en handel (såkalt «Herstatt-risiko»). I CLS er oppgjør av den ene betalingen i en valutahandel betinget av at den andre betalingen gjøres opp. Det fjerner Herstatt-risikoen i valutaoppgjøret. Norske banker handler valuta for store beløp hver dag, og CLS har derfor bidratt til en vesentlig reduksjon i Herstatt-risikoen for norske banker, se figur 3.4.

Ved utgangen av 2017 deltok 67 banker direkte i CLS. DNB var eneste norske deltaker. Institusjoner som ikke deltar direkte i CLS, kan få gjort opp valutahandler

FIGUR 3.4: Oppgjør i norske kroner i CLS. Daglig total. Milliarder NOK. 2017



Kilde: Norges Bank

BREXIT OG FINALITETSDIREKTIVET

En stor andel av oppgjørene til norske finansinstitusjoner skjer i utenlandske interbanksystemer. Avtalene om avregning og oppgjør har tradisjonelt sett ikke vært bindende for aktører som er satt under insolvensbehandling. Det har medført usikkerhet i slike situasjoner.

I EØS-området er usikkerheten fjernet ved at finalitetsdirektivet (98/26/EF) har gitt interbanksystemer adgang til å inngå avtaler med sine deltakere om avregning og oppgjør som også er bindende under insolvensbehandling. Direktivets bestemmelser er tatt inn i nasjonal lovgivning i alle EØS-land. Avtalene gir dermed økt forutsigbarhet i situasjoner med insolvens hos en deltaker i EØS.

Storbritannia meldte seg ut av EU 29. mars 2017 og trer ut av EU 29. mars 2019. Storbritannia vil imidlertid beholde bestemmelsene fra finalitetsdirektivet i sin lovgivning, og avtalene britiske interbanksystem har med britiske deltakere vil dermed fortsatt ha rettsvern. For at avtalene også skal gjelde deltakerne i andre EØS-land, må det presiseres i de nasjonale lovgivningene at rettsvernsreglene i direktivet også gjelder for interbanksystem utenfor EØS.

Finansdepartementet sendte 2. mars 2018 på høring et forslag om å endre betalingssystemloven, slik at loven også vil gjelde for finansinstitusjoner som deltar i systemer utenfor EØS. Dersom dette forslaget tas inn i norsk lov, vil avtalene mellom britiske interbanksystemer og norske deltakere være beskyttet av finalitetsdirektivet også etter at Storbritannia har gått ut av EU. Dette vil fjerne usikkerheten for norske deltakere. Eksempler på land som allerede har valgt en slik løsning er Danmark, Tyskland, Belgia og Spania.

i CLS gjennom en direkte deltaker. I 2017 deltok 259 norske institusjoner på denne måten.

Regelverket for CLS er underlagt britisk lovgivning. CLS Bank International, som driver oppgjørssystemet, er hjemmehørende i USA og har en amerikansk banklisens for begrenset bankvirksomhet.

Finansdepartementet har sendt på høring et forslag om endring av betalingssystemloven, slik at britiske interbanksystemer fremdeles vil være beskyttet av oppgjørsdirektivet etter at Storbritannia trer ut av EU i 2019, se egen ramme om Brexit og finalitetsdirektivet. Uttredelsen av Storbritannia vil dermed ikke føre til at CLS vil ha juridisk usikkerhet overfor norske deltakere i valutaoppgjøret.

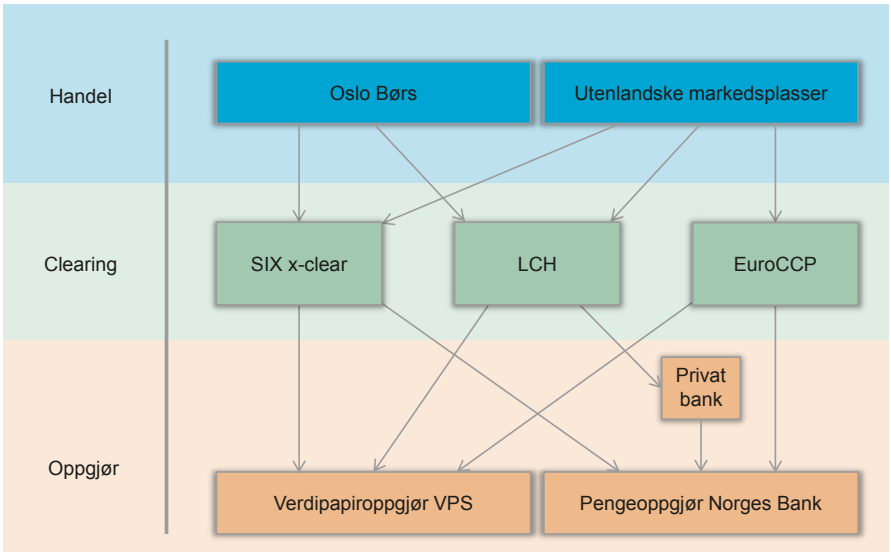
Utkontraktering
IBM leverer operative tjenester og støttefunksjoner til CLS.

Stabiliteten i systemet
Det siste året har det ikke vært hendelser som har påvirket oppgjøret av norske kroner i CLS.

Tilsyn og overvåking
CLS er underlagt både tilsyn og overvåking. Den amerikanske sentralbanken fører tilsyn med CLS. 23 sentralbanker, blant annet Norges Bank, samarbeider om å overvåke CLS. Den amerikanske sentralbanken leder overvåkingsgruppen. Gruppen har internasjonale prinsipper fra CPMI-IOSCO som utgangspunkt for sitt samarbeid og sine vurderinger.

CLS Bank har offentliggjort en oppdatert vurdering av hvordan CLS følger internasjonale prinsipper fra CPMI-IOSCO. Sentralbankene som deltar i overvåkingen av CLS, har hatt anledning til å gi kommentarer. CLS Bank oppdaterer vurderingen annethvert år.

FIGUR 3.5 Handel, clearing og oppgjør av aksjer i norske kroner



Kilde: Norges Bank

3.3 VERDIPAPIROPPGJØRET

Verdipapirsentralen ASA (VPS) har konsesjon som norsk verdipapirregister. VPS er også operatør av det norske verdipapiroppgjøret (VPO). I VPO blir rettigheter til verdipapirer bokført på VPS-konti. Tilhørende pengeoppgjør skjer i NBO.

Transaksjoner som blir sendt til oppgjør i VPO, kommer fra flere markedsplasser og går gjennom flere sentrale motparter, se figur 3.5. Sentrale motparter deltar i VPO fordi de trer inn i aksjehandler på regulerte markedsplasser og blir motpart til både selger og kjøper av aksjene. Dette kalles clearing.

OPPGJØRSSYSTEMET TIL VERDIPAPIRSENTRALEN

Kort om systemet

Verdipapiroppgjøret (VPO) omfatter oppgjør av aksjer, egenkapitalbevis og rentepapirer i norske kroner. I VPO deltar 36 aktører (verdipapirforetak, banker og sentrale motparter) direkte i VPS. Av disse er det 19 som deltar direkte i pengeoppgjøret i NBO. Deltakerne i NBO er banker og sentrale motparter. I tillegg er det flere aktører som deltar indirekte.

For aksjehandler som cleares via sentral motpart beregner de sentrale motpartene en netto posisjon per aksje og en netto pengeposisjon for hver deltaker. Avregningen medfører at færre aksjetransaksjoner sendes til oppgjør i VPO. Transaksjoner med obligasjoner i norske kroner blir ikke avregnet av sentrale motparter.

VPO gjennomføres to ganger per dag, kl. 06 og 12. VPO er basert på multilateralt nettooppgjør. I 2017 var daglig netto oppgjørsverdi 4,3 milliarder norske kroner. 73 prosent av verdien ble gjort opp i morgenoppgjøret.

Før hvert oppgjør beregner VPS deltakernes posisjoner både på penge- og papirsiden. Pengeposisjonene blir gjort opp på særskilte VPO-oppgjørskontoer i NBO. Etter at pengeoppgjøret er gjennomført, blir rettigheter til verdipapirene bokført på VPS-konti (levering mot betaling). Disse rettighetene bokføres

NYE REGLER FOR VERDIPAPIROPPGJØR OG VERDIPAPIRREGISTRE

EU vedtok i 2014 en forordning for verdipapiroppgjør og verdipapirregistre, CSDR (Central Securities Depository Regulation). Verdipapirregistre har en sentral rolle ved utstedelse, oppgjør, oppbevaring og sikkerhetsstillelse av finansielle instrumenter. De er derfor systemviktige institusjoner for verdipapirmarkedet. Hensikten med reguleringen er å bidra til trygge og effektive verdipapirregistre og verdipapiroppgjørssystemer i EU.

I henhold til CSDR startet europeiske verdipapirregistre høsten 2017 prosessen med å søke sine hjemlandsmyndigheter om nye tillatelser etter CSDR. CSDR-autorisasjon gir verdipapirregistrene tillatelse til å tilby tjenester i hele EU, slik at de kan konkurrere med hverandre.

Som beskrevet i Norges Bank (2017a) forbereder Finansdepartementet innføringen av CSDR og ny verdipapirregisterlov i Norge. CSDR vil medføre endringer i det norske verdipapiroppgjøret VPO og mer omfattende regulering av VPS. Det er usikkert når CSDR kan bli innført i Norge. Når reguleringen blir innført, vil VPS søke om CSDR-autorisasjon.

Norges Bank overvåker i dag ingen andre verdipapirregistre enn VPS, men dette kan bli endret med CSDR. Dersom utenlandske verdipapirregistre med CSDR-autorisasjon vil gjøre opp i norske kroner over visse terskelverdier, skal Norges Bank samarbeide med de aktuelle utenlandske myndighetene om overvåkingen.

én og én (brutto). I 2017 var det i gjennomsnitt 52 000 slike transaksjoner i VPS daglig. Det er nå omtrent 1,35 millioner VPS-konti og markedsverdien av verdipapirer registrert i VPS er omtrent 5 600 milliarder kroner.

Verdipapirhandel på regulerte markedsplasser skal etter standard prosedyre gjøres opp etter to dager. Ikke alle handler blir gjort opp til avtalt dag. Det skyldes i hovedsak at selger eller kjøper mangler dekning. I 2017 ble 96,6 prosent av transaksjonene og 93,6 prosent av oppgjørsverdien i VPO gjort opp til avtalt dag. De fleste transaksjonene som ikke ble gjort opp til avtalt dag, ble gjort opp en eller to dager senere. 0,2 prosent ble kansellert.

VPS gjennomfører i perioden 2016–2018 et fornyelsesprogram som omfatter IKT-systemer, organisasjon, kompetanse og markedspraksis. Programmet dreier seg blant annet om tilpasning til ny EU-regulering (CSDR). For å oppfylle CSDR må VPS søke norske myndigheter om ny autorisasjon for virksomheten og gjennomføre endringer i tjenestetilbud og drift. VPS vil blant annet øke antall oppgjør fra to til tre per dag. Planen er å innføre et tredje daglig oppgjør kl. 14.45 i fjerde kvartal 2018.

Utkontraktering
VPS har ikke utkontraktert driften av sine systemer.

Stabiliteten i systemet
Det har det siste året vært få avvik i VPO, men 5. mars 2018 ble morgenoppgjøret omtrent fire og en halv time forsinket som følge av en systemendring. Av hensyn til deltakerne ble det påfølgende formiddagsoppgjøret utsatt med om lag halvannen time. VPS har opplyst at det er gjennomført tiltak for å sikre at en tilsvarende feil ikke skal skje igjen.

Overvåking
Norges Bank overvåker VPO og VPS, mens Finanstilsynet fører tilsyn med VPS, herunder VPS sin oppgjørsvirksomhet. Norges Bank gjennomfører halvårlige overvåkingsmøter med VPS, der Finanstilsynet inviteres som observatør. I tillegg blir det avholdt møter om spesielle tema etter behov. Norges Bank har i overvåkingen det siste året blant annet vært opptatt av cybersikkerhet og VPS' arbeid med å forberede seg på ny EU-regulering, se rammen om nye regler for verdipapirppgjør og verdipapirregistre.

SENTRALE MOTPARTER

Kort om systemene
Sentrale motparter trer inn i handler mellom kjøper og selger av finansielle instrumenter og garanterer for at kontraktene blir oppfylt (clearing), se figur 3.6. Banker og andre aktører i finansmarkedet reduserer dermed eksponeringene mot hverandre, men til gjengjeld må sentrale motparter håndtere store eksponeringer. I perioder med markedsuro kan robuste sentrale motparter gi et viktig bidrag til finansiell stabilitet.

EU-reguleringen EMIR[31] trådte i kraft i Norge 1. juli 2017[32] og innfører blant annet clearingplikt for visse typer OTC-derivater[33] og rapporteringsplikt for alle derivater.

EMIR stiller også krav til hvordan sentrale motparter og transaksjonsregistre skal drives og hvordan myndighetene skal utføre sitt tilsynsarbeid.

Ingen sentrale motparter har hovedkontor i Norge, slik at norske aktørers handler med finansielle instrumenter gjøres opp gjennom ulike utenlandske sentrale motparter. Handel med aksjer i norske kroner på ulike markedsplasser gjøres opp gjennom sveitsiske SIX x-clear, nederlandske EuroCCP og britiske LCH. SIX x-clear og LCH clearer aksjer på Oslo Børs, se figur 3.5. LCH gjør også opp OTC-rentederivater.

Overvåking
Norges Banks overvåking med sentrale motparter som er viktige for finansiell sektor i Norge foregår gjennom deltakelse i internasjonale samarbeidsløsninger:

- Den nederlandske sentralbanken har opprettet et College i tråd med EMIR for å overvåke EuroCCP. Norges Bank deltar som observatør uten stemmerett.

- Bank of England har opprettet et College i tråd med EMIR for å overvåke LCH. Bank of England har også etablert et Global College med bredere sammensetning enn EMIR College. Norges Bank deltar i Global College uten stemmerett.

31 EU (2012). EMIR (European Market Infrastructure Regulation) er EUs regulering av OTC-derivater, sentrale motparter og transaksjonsregistre, og forordningen er senere supplert med utfyllende bestemmelser.
32 Finanstilsynet (2017c).
33 OTC (over the counter)-derivater er derivater som inngås direkte mellom to parter utenom børs.

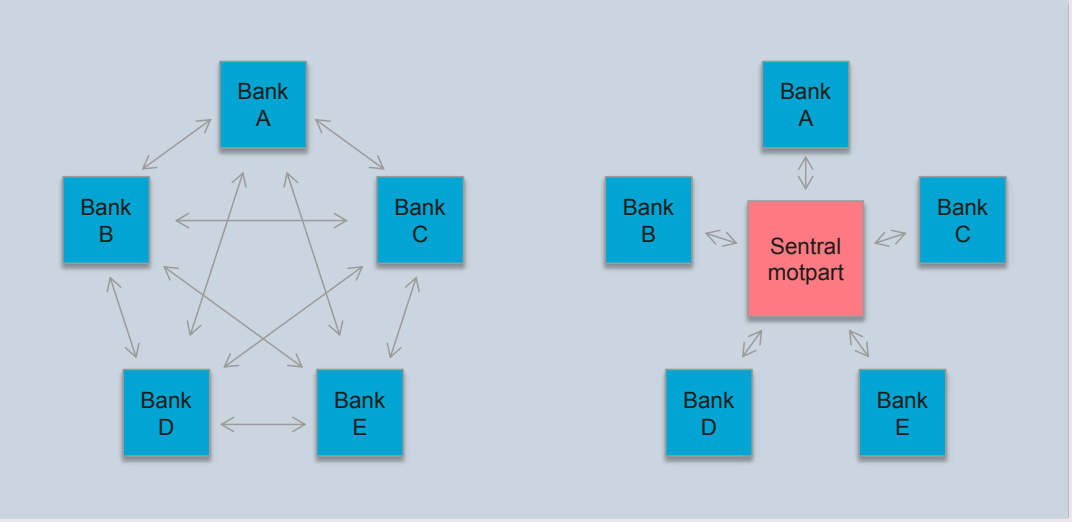
HOVEDTREKK I SENTRALE MOTPARTERS HÅNDTERING AV RISIKO

Forsvarlig styring av risikoen i sentrale motparter er avgjørende for en robust finansiell sektor. Sentrale motparter må være i stand til å utføre sin rolle på en god måte også under ekstreme markedsforhold. Det forutsetter at den sentrale motparten har tilgang til tilstrekkelige finansielle ressurser og en god forståelse av risikoen den påtar seg.

De finansielle ressursene består først og fremst av marginer fra deltakerne og misligholdsfond. *Marginer* er kontanter og verdipapirer som en deltaker må stille for å dekke eksponeringene som den utsetter den sentrale motparten for. Marginene fra en deltaker skal dekke eksponeringene på minst 99 prosent av dagene. *Misligholdsfond* er kontanter og verdipapirer som deltakerne må betale inn for å dekke tap som andre deltakere kan påføre den sentrale motparten. Det trekkes på misligholdsfondet dersom marginene fra en feilende deltaker ikke er tilstrekkelige til å dekke et tap. Mens marginer vil dekke inn små tap, vil misligholdsfond sørge for fordeling av store tap.

Sentrale motparter gjennomfører en rekke kvantitative tester av risikoen de påtar seg. For eksempel utføres såkalt «backtesting» for å kontrollere at de innbetalte marginene vil dekke tapene på minst 99 prosent av dagene. Gjennom stresstester kontrollerer sentrale motparter at de har tilstrekkelig med finansielle ressurser til å fungere selv om de to største deltakerne skulle feile i en periode med stor markedsuro. En mer detaljert omtale av finansielle ressurser og tester for sentrale motparter er gitt i Norges Bank (2015).

Figur 3.6 Sentrale motparter



- Norges Bank og Finanstilsynet har inngått en samarbeidsavtale med sveitsiske myndigheter om overvåking av SIX x-clear.

Norges Bank mottar regelmessig kvalitative og kvantitative rapporter fra de tre sentrale motpartene, og deltar på minimum ett møte i året for hver av dem.

Internasjonalt arbeid

Fordi sentrale motparter og transaksjonsregistre ofte driver grensekryssende virksomhet, må både nasjonale og internasjonale myndigheter arbeide sammen for å få etablert en effektiv regulering. Internasjonalt arbeid som er relevant for Norges Banks overvåkingsarbeid, kan deles inn i to hovedkategorier: 1) Anbefalinger og analyser på globalt nivå og 2) Regulering og analyser på EU-nivå.

1) Anbefalinger og analyser på globalt nivå

På oppdrag fra G20s finansministre og sentralbanksjefer ble det i 2015 laget en arbeidsplan[34] for å videreutvikle regulering og overvåking av derivatmarkeder og sentrale motparter. I 2017 ble fire rapporter publisert for å følge opp planen:

- «Analysis *of Central Clearing Interdependencies*» (FSB, CPMI, IOSCO og Baselkomiteen)[35] analyserer data som avdekker avhengigheter mellom sentrale motparter og deres deltakere. Rapporten viser at det er en høy grad av konsentrasjon, der få sentrale motparter og banker står for det meste av omsetningen. Videre avdekkes relativ høy grad av

34 FSB, BCBS, CPMI og IOSCO (2015).
35 FSB, CPMI, IOSCO og BCBS (2017).

INTERNASJONALE MYNDIGHETERS SOM DELTAR I ARBEIDET MED Å GJØRE SENTRALE MOTPARTER MER ROBUSTE

Globalt nivå

«Financial Stability Board (FSB)» er et internasjonalt forum for sentralbanker og regjerninger som skal overvåke og gi råd om det globale finansielle systemet.

«Committee on Payment and Market Infrastructures (CPMI)» er en sentralbankkomite som skal fremme robuste og effektive løsninger knyttet til betalings-, clearing- og oppgjørssystemer.

«International Organisation of Securities Commissions (IOSCO)» er en forsamling av myndighetsorganer som regulerer verdipapir- og futuresmarkeder. Finanstilsynet er medlem i IOSCO.

«Basel Committee on Banking supervision (Baselkomiteen)» skal fremme samarbeid om regulering av banker.

FSB, CPMI og Baselkomiteen er opprettet av G10 eller G20 og har i hovedsak disse landene som deltakere.

EU-nivå

«European Securities and Markets Authority (ESMA)» er tilsynsorgan for verdipapirer og finansmarkeder. ESMA er forvaltningsorganet for EMIR, som regulerer sentrale motparter og transaksjonsregistre.

«European Systemic Risk Board (ESRB)» er en selvstendig enhet som skal fremme tilsynet av det finansielle systemet i EU. ESRB utfører analyser og gir råd til ESMA. Norges Bank er observatør i ESRB og deltar i flere av arbeidsgruppene til ESRB.

gjensidige avhengigheter mellom globale banker og store internasjonale sentrale motparter. Sistnevnte bruker de globale bankene som viktige leverandører for likviditets-, betalings- og depottjenester. En sentral motpart kan derfor rammes på flere måter av at en stor bank feiler.

- «*Guidance on Central Counterparty Resolution and Resolution Planning*» (FSB)[36] gir veiledning for avvikling av sentrale motparter, og planlegging av slik avvikling. God planlegging og beredskap er avgjørende for at alvorlige vansker i en sentral motpart ikke skal true den finansielle stabiliteten og bidra til en mest mulig hensiktsmessig fordeling av tapene.

- «*Resilience on Central Counterparties: Further guidance*» (CPMI-IOSCO)[37] utfyller og belyser prinsippene som ble laget for finansiell infrastruktur i 2012. Denne veiledningen presiserer hvordan sentrale motparter skal oppfylle prinsippene. For eksempel er det detaljert beskrevet hvilke tester som skal utføres og hvordan testene skal gjennomføres.

- «*Framework for supervisory stress testing of central counterparties*» (CPMI-IOSCO)[38] er et utkast til rammeverk for myndighetenes stresstesting av sentrale motparter. Stresstestene skal brukes til å vurdere konsekvensene av at flere sentrale motparter utsettes for samme hendelse, se stresstesten til ESMA omtalt under EU-nivå.

36 FSB (2017b).
37 CPMI-IOSCO (2017a).
38 CPMI-IOSCO (2017b).

2) Regulering og analyser på EU-nivå

I regi av EU ble det i 2017 gjennomført lovgivningsarbeid og nye analyser av sentrale motparter og transaksjonsregistre. Milepæler i dette arbeidet var:

- EU-kommisjonen publiserte i mai 2017 et forslag for EMIR 2, med kun enkelte mindre endringer.[39]

- EU-kommisjonen innførte i november 2017 nye krav for rapportering til transaksjonsregistre.[40] Dette har forbedret kvaliteten på rapportene. Data fra transaksjonsregistre gir blant annet myndighetene en bedre oversikt over eksponeringene i finansiell sektor og er dermed viktige i arbeidet for finansiell stabilitet.

- ESMA gjennomførte i 2017 stresstest av alle sentrale motparter i EU-området.[41] Testen belyste de sentrale motpartenes evne til å bære tap og til gjøre opp for seg til rett tid. Stresstesten viste at europeiske sentrale motparter er robuste, og at de kan dekke tap selv om flere deltakere feiler samtidig.

Videre sendte ESMA i januar 2018 på høring et forslag som presiserer retningslinjene fra 2013 for å motvirke prosykliske marginkrav, se egen ramme om retningslinjer for å motvirke at marginkrav virker prosyklisk.

39 EU (2017a).
40 EU (2017b).
41 ESMA (2017b).

RETNINGSLINJER FOR Å MOTVIRKE AT MARGINKRAV VIRKER PROSYKLISK

I perioder med markedsuro blir eksponeringene som den sentrale motparten har mot sine deltakere større, og for å dekke eksponeringene øker den sentrale motparten marginkravene. I slike perioder har markedsaktørene ofte knapp likviditet. EU-kommisjonen innførte i 2013 retningslinjer som skal motvirke at marginer økes i perioder hvor bankene har knapp likviditet (prosyklikalitet).[1]

Prosyklikalitet kan motvirkes ved at sentrale motparter krever mer marginer i normale perioder. Det kan gjøres ved at marginmodellene inkluderer observasjoner fra stressperioder, ved at parameterne i marginmodellene baseres på observasjoner gjennom minst 10 år eller ved at marginmodellene inkluderer en buffer.

Norges Bank deltar i en arbeidsgruppe i ESRB som har bred fokus på prosyklikalitet på tvers av ulike markeder. Gruppen skal levere sin rapport innen utgangen av 2019.

1 EU (2013).

Referanser

Aera (2018). Skapt av handelen – for handelen. Presentasjon, Betalingsformidling 2018, Trondheim.
https://static1.squarespace.com/static/562a32b0-e4b0e6f4ec3104ae/t/5aaa5f5c53450a6f4dea99b7/1521114995286/Aera+Betalingskonferansen+Mars+2018+Light.pdf

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014a). The economics of digital currencies. Bank of England Quarterly Bulletin, 54(3), 276-286.
https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/the-economics-of-digital-currencies.pdf?la=en&hash=E9E56A61A6D71A97DC8535FEF211CC08C0F59B30

Ameln, M. og P. Songe-Møller (2018). Hvorfor er digitale plattformer så kraftfulle? Sprint Consulting.
https://sprint.no/hvorfor-er-digitale-plattformer-sa-kraftfulle/

ASX (2017), ASX selects distributed ledger technology to replace CHESS, Press Release.
https://www.asx.com.au/documents/asx-news/ASX-Selects-DLT-to-Replace-CHESS-Media-Release-7December2017.pdf

Bank of England (2018). The Bank of England's supervision of financial market infrastructures – Annual Report 2018.
https://www.bankofengland.co.uk/news/2018/february/supervision-of-financial-market-infrastructures-annual-report-2018

Bech, M. L. og R. Garratt (2017). Central Bank Cryptocurrencies, BIS Quarterly Review, 17. september.
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Carney, M. (2018). The future of money. Tale 2. mars, Edinburgh.
https://www.bankofengland.co.uk/speech/2018/mark-carney-speech-to-the-inaugural-scottish-economics-conference

Chapman, J., R. Garratt, S. Hendry, A. McCormack og W. McMahon (2017). Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet? Bank of Canada Financial System Review, June 2017.
https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf

CPMI (2015). Digital Currencies.
https://www.bis.org/cpmi/publ/d137.pdf

CPMI (2017). Distributed ledger technology in payment, clearing and settlement – An analytical framework.
https://www.bis.org/cpmi/publ/d157.pdf

CPMI-IOSCO (2012). Principles for financial market infrastructures.
https://www.bis.org/cpmi/publ/d101a.pdf

CPMI-IOSCO (2016). Guidance on cyber resilience for financial market infrastructures.
https://www.bis.org/cpmi/publ/d146.pdf

CPMI-IOSCO (2017a). Resilience of central counterparties (CCPs): Further guidance on the PFMI, July 2017.
https://www.bis.org/cpmi/publ/d163.pdf

CPMI-IOSCO (2017b). Consultative report: Framework for supervisory stress testing of central counterparties (CCPs), June 2017.
https://www.bis.org/cpmi/publ/d161.pdf

Departementene (2012). Nasjonal strategi for informasjonssikkerhet.
https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

ECB (2018). Securities settlement systems: delivery-versus-payment in a distributed ledger environment, STELLA – a joint research project of the European Central Bank and the Bank of Japan.
https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf

ESMA (2017a). The Distributed Ledger Technology Applied to Securities Markets.
https://www.esma.europa.eu/press-news/esma-news/esma-assesses-dlt%E2%80%99s-potential-and-interactions-eu-rules

ESMA (2017b). Report: EU-wide CCP stress test 2017.
http://firds.esma.europa.eu/webst/ESMA70-151-1154%20EU-wide%20CCP%20Stress%20Test%202017%20Report.pdf

EU (2012). Regulation (EU) No 648/2012 of the European parliament and of the council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN

EU (2013). Commission delegated regulation (EU) No 153/2013.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0153&from=EN

EU (2017a). Proposal for amending Regulation (EU) No 648/2012.
https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-208_en

EU (2017b). Forordning til EMIR. Commission implementing regulation (EU) 2017/105 of 19 October 2016 amending Implementing Regulation (EU) No 1247/2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories.
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0105&from=EN

Fevolden, M. B. og L. Smith (2018). What Kind of Payments Settle in a Real Time Gross Settlement System? Kommende Norges Bank Staff Memo.

Finansdepartementet (2017a). Brev av 20. desember 2017 til Finanstilsynet.

Finansdepartementet (2017b). NOU 2017:13 Ny sentralbanklov. Organisering av Norges Bank og Statens pensjonsfond utland.
https://www.regjeringen.no/no/aktuelt/utredning-fra-sentralbanklovutvalget/id2558679/

Finansdepartementet (2018a). Finansmarkedsmeldingen 2018.
https://www.regjeringen.no/no/dokumenter/meld.-st.-14-20172018/id2599000/sec1

Finansdepartementet (2018b). Nye krav til bankenes kontantberedskap. Pressemelding 17. april.
https://www.regjeringen.no/no/aktuelt/nye-krav-til-bankenes-kontantberedskap/id2598131/

Finanstilsynet (2013). Advarsel til forbrukere – informasjon om virtuelle valutaer, 13. desember.
https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2013/advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/

Finanstilsynet (2017a). Risiko- og sårbarhetsanalyse (ROS) 2016.
https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/

Finanstilsynet (2017b). Initial Coin offerings (ICO-er) – advarsel til investorer og foretak, 20. november.
https://www.finanstilsynet.no/markedsadvarsler/2017/initial-coin-offerings-icoer---advarsel-til-investorer-og-foretak/

Finanstilsynet (2017c). Gjennomføring av EMIR. Rundskriv 6/2017, 4. juli.
https://www.finanstilsynet.no/tema/emir/

Finanstilsynet (2018). Finanstilsynet advarer forbrukere om kryptovaluta, 12. februar.
https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2018/finanstilsynet-advarer-forbrukere-om-kryptovaluta/

FSB (2017a). Financial Stability Implications from FinTech.
http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/

FSB (2017b). Guidance on Central Counterparty Resolution and Resolution Planning, July.
http://www.fsb.org/wp-content/uploads/P050717-1.pdf

FSB (2018). Letter to G20 Finance Ministers and Central Bank Governors, 13. mars.
http://www.fsb.org/wp-content/uploads/P180318.pdf

FSB, BCBS, CPMI og IOSCO (2015). 2015 CCP Workplan.
https://www.bis.org/cpmi/publ/d134b.pdf

FSB, CPMI, IOSCO og BCBS (2017). Analysis of Central Clearing Interdependencies, July 2017.
https://www.bis.org/cpmi/publ/d164.pdf

He, D., R. Leckow, V. Haksar, T. Mancini-Griffoli, N. Jenkinson, M. Kashima og H.Tourpe, H. (2017). Fintech and Financial Services: Initial Considerations. IMF Staff Discussion Notes.
https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

Meld. St. 38 (2016-2017). IKT-sikkerhet – Et felles ansvar. https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

Norges Bank (2014). Finansiell Infrastruktur 2014. https://www.norges-bank.no/Publisert/Publikasjoner/Finansiell-infrastruktur---rapport/Finansiell-infrastruktur-2014/

Norges Bank (2015). Finansiell stabilitet 2015. https://www.norges-bank.no/Publisert/Publikasjoner/Finansiell-stabilitet---rapport/2015-Finansiell-stabilitet/

Norges Bank (2016). Finansiell infrastruktur 2016. https://www.norges-bank.no/Publisert/Publikasjoner/Finansiell-infrastruktur---rapport/Finansiell-infrastruktur-2016/

Norges Bank (2017a). Finansiell infrastruktur 2017. https://www.norges-bank.no/Publisert/Publikasjoner/Finansiell-infrastruktur---rapport/finansiell-infrastruktur-2017/

Norges Bank (2017b). Brev av 17. august 2017 til Finansdepartementet. https://www.norges-bank.no/Publisert/Brev-og-uttalelser/2017/2017-08-17-brev/

Norges Bank (2017c). Brev av 12. desember 2017 til Justis- og beredskapsdepartementet. https://www.norges-bank.no/Publisert/Brev-og-uttalelser/2017/2017-12-12-brev/

Norges Bank (2018a). Brev av 7. februar 2018 til Finansdepartementet.

Norges Bank (2018b). Brev av 20. februar 2018 til Finanstilsynet.

Norges Bank (2018c). Kunderetta betalingsformidling 2017. Noregs Bank Memo 2/2018.

Norges Bank (2018d). Digitale sentralbankpenger. Norges Bank Memo 1/2018.

Norges Bank (2018e). Reviderte vilkår for kontohold i Norges Bank (NBO). Rundskriv 2/2018. https://www.norges-bank.no/Publisert/Rundskriv/2018/2-kontohold/

NSM (2017). Helhetlig IKT-risikobilde 2017. Nasjonal sikkerhetsmyndighet rapport. 27. september 2017. https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

Ripple (2017). Japan Bank Consortium Moves to Become Production-ready, 5. desember. https://ripple.com/insights/japan-bank-consortium-moves-become-production-ready/

Solberg, E. (2018). Nasjonal strategi for IKT-sikkerhet. Tale, 6. mars, Oslo. https://www.regjeringen.no/no/aktuelt/nasjonal-strategi-for-ikt-sikkerhet/id2592996/

VPS (2018). Endringer i VPO NOK Regelverket med virkning fra 18. juni 2018. https://www.vps.no/pub/endringer-i-vpo-nok-regelverket-med-virkning-fra-18-juni-2018/

LOVER OG FORSKRIFTER

Betalingssystemloven. Lov om betalingssystemer mv. LOV-1999-12-17-95. https://lovdata.no/dokument/NL/lov/1999-12-17-95

Forskrift om gjennomføring av verdipapiroppgjøret. FOR-2016-09-22-1095. https://lovdata.no/dokument/SF/forskrift/2016-09-22-1095

Sentralbankloven. Lov om Norges Bank og pengevesenet mv. LOV-1985-05-24-28. https://lovdata.no/dokument/NL/lov/1985-05-24-28

Verdipapirregisterloven. Lov om registering av finansielle instrumenter. LOV-2002-07-05-64. https://lovdata.no/dokument/NL/lov/2002-07-05-64

DIREKTIVER OG FORORDNINGER FRA EU

Forordning for verdipapiroppgjør og verdipapirregistre. Central Securities Depository Regulation (CSDR). Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0909

Forordning om OTC-derivater, sentrale motparter og transaksjonsregister. European Market Infrastructure Regulation (EMIR). Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R0648

Forordning til EMIR. Regulation (EU) 2016/1178 of 10 June 2016 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on the clearing obligation.
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R1178

Revidert betalingstjenestedirektiv (PSD2). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). OJ L 337, 23.12.2015, s. 35–127.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

Definisjoner og forkortelser

Avregning: Flere transaksjoner blir utlignet og for hver bank blir det regnet ut en nettoposisjon.

BankAxept-kort: Debetkort som er utstedt av en norsk bank og knyttet opp mot en bankkonto for bruk i Norge.

Clearing: Se sentral motpart.

CLS (Continuous Linked Settlement): System for oppgjør av handel med valuta. CLS sikrer betaling mot betaling og fjerner dermed kredittrisikoen i oppgjøret.

CPMI (Committee on Payments and Market Infrastructures): Et forum for sentralbanker som skal fremme effektive og robuste betalingssystem.

CSDR (Central Securities Depositories Regulation): EU-regulering (909/2014) om forbedret verdipapiroppgjør i EU og om verdipapirregistre.

Desentralisert register: Se desentralisert teknologi.

Desentralisert teknologi: Prosess og relatert teknologi som gjør det mulig for deltakere i et nettverk på en sikker måte å foreslå, validere og bokføre endringer i et register. Registeret er distribuert synkront mellom alle nodene i nettverket. Blokkjeder (Blockchain) er en form for desentralisert teknologi.

Digitale sentralbankpenger (DSP): En allment tilgjengelig elektronisk fordring på sentralbanken.

EMIR: European Market Infrastructure Regulation. EU-regulering (648/2012) om OTC-derivater, sentrale motparter og transaksjonsregistre.

ESMA: European Securities and Markets Authority.

ICO (Initial Coin Offering): Forhåndssalg av enheter av kryptoaktiva til investorer, ofte mens den fortsatt er under utvikling. Formålet kan være å finansiere videre utvikling.

IOSCO (International Organization of Securities Commissions): Internasjonal organisasjon for tilsyn med verdipapirmarkedene.

Krypteringsnøkler: Informasjon som brukes til å kryptere annen informasjon. Formålet kan være å skjule informasjon for uvedkommende eller å «signere» informasjon. For signering benyttes ofte en privat nøkkel for å signere informasjon, mens en korresponderende offentlig nøkkel benyttes til å verifisere at informasjonen er signert av den som besitter den private nøkkelen.

Kryptovaluta: Systemer for disponering av enheter i et register basert på krypteringsnøkler. Som hovedregel basert på desentralisert teknologi.

Lenke: Et sett med kontraktsmessige og operasjonelle ordninger som knytter sammen to eller flere systemer direkte eller gjennom et mellomledd.

Marginer: Midler som sentrale motparter krever inn fra medlemmene sine som sikkerhet.

NBO: Norges Banks oppgjørssystem.

NICS (Norwegian Interbank Clearing System): Et felles system norske banker har for avregning av betalingstransaksjoner.

NSM: Nasjonal sikkerhetsmyndighet.

OTC (Over the Counter): Handel utenfor regulert markedsplass.

PSD2: Revidert EU-direktiv (2015/2366) om betalingstjenester.

Sentral motpart: En institusjon som trer inn i handelen når handelen blir avtalt, og blir kjøper for selger og selger for kjøper. Den sentrale motparten garanterer for oppfylling av slike handler (clearing).

VPO: Verdipapiroppgjøret.

VPS: Verdipapirsentralen ASA.

Tabellvedlegg[1]

Tabell 1: Transaksjoner i avregnings- og oppgjørssystem. Antall daglige observasjoner. Gjennomsnitt

	2001	2002	2003	2004	2005	2006	2007	2008	2009[3]	2010	2011	2012	2013	2014	2015	2016	2017
NICS																	
NICS Brutto	303	300	596	611	532	547	593	605	524	568	548	594	659	624	772	980	1 021
NICS SWIFT Netto[1]	4 719	4 925	5 155	4 480	4 744	5 301	5 908	6 390	6 269	-	-	-	-	-	-	-	
NICS Netto (millioner)[2]	3,4	3,7	4,0	4,3	4,7	5,1	5,5	5,9	6,5	6,8	7,2	7,8	8,2	8,7	9,1	9,5	9,9
NBO																	
Totalt antall transaksjoner									1 165	1 146	1 138	1 274	1 406	1 367	1 565	1 835	1 958
RTGS brutto-transaksjoner utenom NICS									463	477	479	549	595	592	658	700	793

1 Avviklet i juni 2010.
2 Tidligere NICS Masse og NICS SWIFT Netto betalinger under 25 mill. inngår fra og med juni 2010 i NICS Netto.
3 For NBO er tallene for 2009 beregnet for perioden 17. april til 31. desember.

Kilder: Tallene under NICS er hentet fra NICS Operatørkontor. Tallene under NBO er hentet fra Norges Bank

1 Tabeller som viser utviklingen i kunderettet betalingsformidling er publisert i Norges Bank Memo 2/2018.

Tabell 2: Transaksjoner i avregnings- og oppgjørssystem. Daglig omsetning (milliarder kroner). Gjennomsnitt

	2001	2002	2003	2004	2005	2006	2007	2008	2009[3]	2010	2011	2012	2013	2014	2015	2016	2017
NICS	**211,4**	**212,5**	**248,7**	**195,7**	**200,8**	**224,8**	**254,5**	**246,6**	**213,1**	**196,5**	**221,4**	**247,8**	**253,5**	**262,8**	**285,9**	**284,1**	
NICS Brutto	151,2	149,5	187,8	129,4	135,5	155,3	176,8	165,9	124,1	107,2	119,1	138,6	136,0	140,9	160,1	158,7	163,3
NICS SWIFT Netto[1]	16,1	16,2	12,6	5,2	5,7	6,7	7,6	7,3	6,1	-	-	-	-	-	-	-	
NICS Netto[2]	44,1	46,8	48,3	61,1	59,6	62,8	70,1	73,4	82,9	89,3	102,3	109,2	117,5	121,9	125,8	125,4	133,7
NBO	**172,1**	**169,2**	**206,8**	**152,3**	**160,8**	**185,2**	**226,1**	**224,9**	**168,4**	**162,2**	**172,1**	**201,9**	**188,3**	**198,0**	**219,3**	**221,2**	**235,8**
NICS Brutto	150,7	149,5	187,7	128,9	135,5	155,3	180,2	163,9	113,2	106,3	119,0	137,7	135,2	140,8	157,5	156,1	159,0
RTGS brutto-transaksjoner utenom NICS	6,9	4,8	7,2	11,1	12,1	16,1	31,1	45,6	40,2	42,5	42,4	51,1	38,5	42,5	46,0	49,0	42,1
NICS SWIFT Netto[1]	5,3	5,5	2,1	1,0	0,9	1,0	1,2	1,1	0,9	1,1	-	-	-	-	-	-	
NICS Netto[2]	6,8	6,9	6,7	7,6	8,5	8,1	8,1	9,2	9,6	7,1	6,3	8,7	10,3	10,8	11,9	12,4	13,1
VPO og Oslo Clearing[4]	2,3	2,5	3,1	3,7	3,8	4,7	5,5	5,1	4,5	5,3	4,5	4,4	4,2	3,9	3,8	3,7	4,2
VPO						4,4	5,1	4,9	4,4	5,2	4,5	4,4	4,2	3,9	3,8	3,6	4,2
Oslo Clearing[5]						0,3	0,4	0,3	0,1	0,1	0,1	0,0	0,0	0,1	-	0,0	0,0

1 Avviklet i juni 2010.
2 Tidligere NICS Masse og NICS SWIFT Netto betalinger under 25 mill. inngår fra og med juni 2010 i NICS Netto.
3 For NBO er tallene for 2009 beregnet for perioden 17. april til 31. desember. I dette året er det et brudd i serien.
4 Avviklet i mai 2015 (legalt integrert i SIX x-clear).
5 Se note 4.

Kilder: Tallene under NICS er hentet fra NICS Operatørkontor. Tallene under NBO er hentet fra Norges Bank

Tabell 3: Antall deltakere i avregnings- og oppgjørssystem (ved årsslutt)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Norges Banks oppgjørssystem (NBO): Banker med konto i Norges Bank	**145**	**142**	**143**	**140**	**134**	**129**	**130**	**128**	**131**	**129**	**130**	**135**
Norges Banks oppgjørssystem (NBO): Banker med masseoppgjør i Norges Bank	23	23	22	21	21	21	22	22	21	22	22	21
DNB	104	103	103	106	105	103	98	98	97	94	94	93
SpareBank 1 SMN	17	18	16	16	13	12	11	11	11	11	11	11
Norwegian Interbank Clearing System (NICS)	146	146	143	145	142	138	132	131	130	128	128	125

Kilde: Norges Bank

NORGES BANK
Bankplassen 2, Postboks 1179 Sentrum, 0107 Oslo
www.norges-bank.no