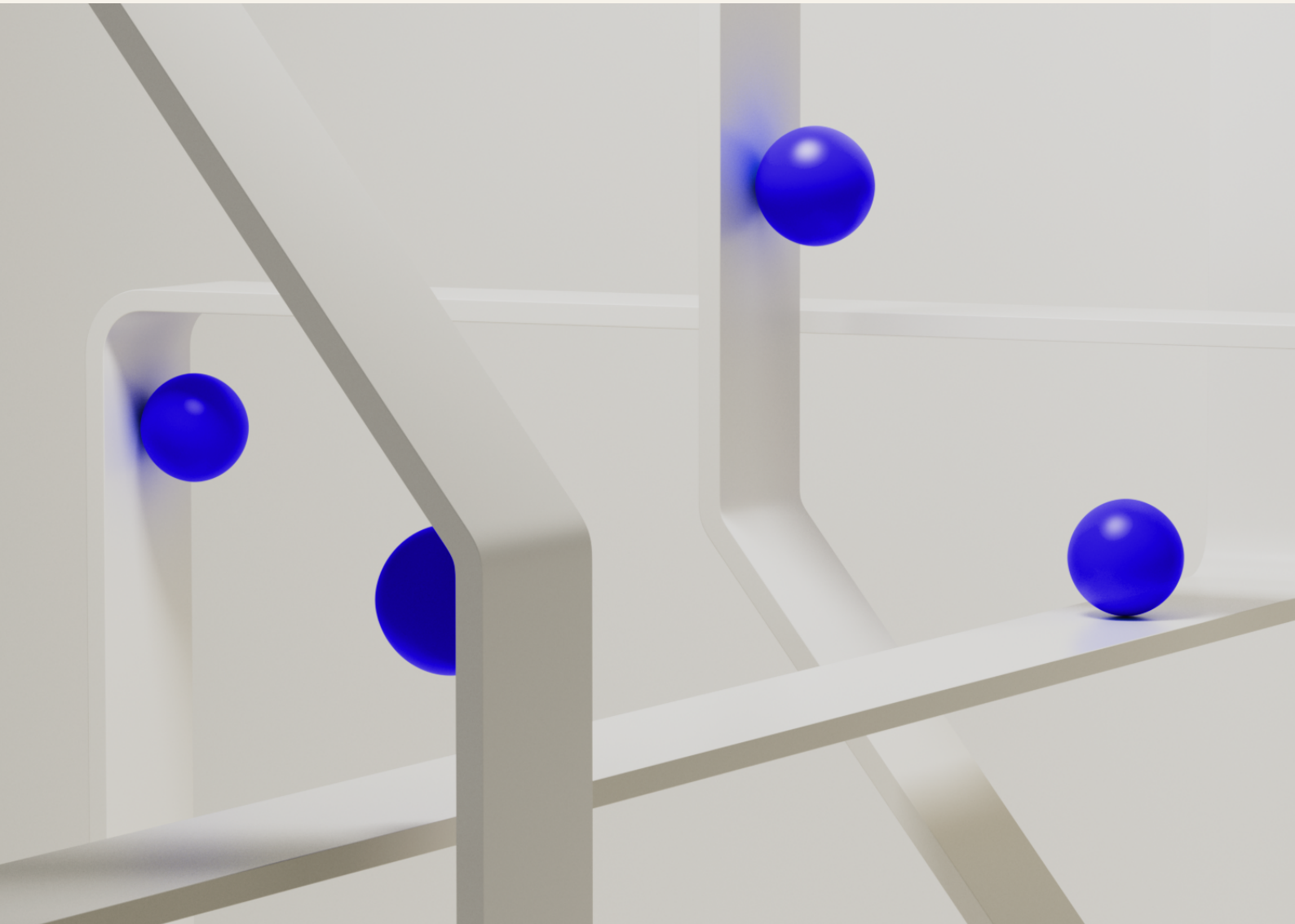
Norges Bank

Finansiell infrastruktur

2026



Utvalgte nøkkeltall

359 mrd. kr.

Daglig omsetning i Norges Banks oppgjørssystem

95

Antall banker med konto i Norges Bank

37,7 mrd. kr.

Verdien av kontanter i sirkulasjon

9,6 mill.

Daglig antall transaksjoner inn til bankenes felles avregningssystem

575 228

Daglig antall realtidstransaksjoner

37 %

Andel av betalinger på fysiske utsalgssteder som gjøres med mobiltelefon

---

Daglig omsetning i Norges Banks oppgjørssystem: Gjennomsnitt for 2025. Kilde: Norges Bank
Antall banker: Antall banker med konto i Norges Bank ved utgangen av 2025. Kilde: Norges Bank
Verdien av kontanter i sirkulasjon: Gjennomsnittlig verdi av kontanter i omløp i 2025. Kilde: Norges Bank
Daglig antall transaksjoner inn til bankenes felles avregningssystem NICS: Gjennomsnitt for 2025. Kilde: Bits
Daglig antall realtidstransaksjoner gjennom NICS Real: Gjennomsnitt for 2025. Kilde: Bits
Andel av betalinger på fysiske utalgssteder som gjøres med mobiltelefon: Spørreundersøkelse gjennomført våren 2026. Kilde: Norges Bank

Norges Banks rapport om finansiell infrastruktur

I den årlige rapporten Finansiell infrastruktur drøfter Norges Bank utviklingstrekk, sårbarhet og risiko i den finansielle infrastrukturen. Rapporten er en del av Norges Banks arbeid med å fremme finansiell stabilitet og et sikkert og effektivt betalingssystem.

Norges Banks øvrige rapporter om finansiell stabilitet

I den halvårlige rapporten Finansiell stabilitet vurderer Norges Bank utsiktene for finansiell stabilitet. Rapporten drøfter sykliske og strukturelle utviklingstrekk i banker og andre finansforetak, finans-markedene og norsk økonomi som har betydning for sårbarhet og risiko i det finansielle systemet.

Rapporten Det norske finansielle systemet som utgis årlig, gir en samlet oversikt over det finansielle systemet i Norge, dets oppgaver og hvordan disse oppgavene blir utført.

Innhold

Ansvarlig redaktør: Ida Wolden Bache

Rapporten ble publisert 10. juni og er tilgjengelig på www.norges-bank.no

Hovedstyrets vurdering

Norge har et effektivt og sikkert betalingssystem. Driften er stabil og betalinger kan gjennomføres raskt, til lave samfunnsøkonomiske kostnader og på måter som er tilpasset brukernes behov.

Samtidig viser trusselvurderinger at vi står overfor den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. Geopolitiske spenninger øker risikoen for at fiendtlige aktører forsøker å utnytte sårbarheter. Teknologisk utvikling, spesielt innen kunstig intelligens og kvanteteknologi, bidrar også til et mer krevende trusselbilde. For å redusere sårbarheter og sikre tilstrekkelig motstandskraft også i fremtiden kreves systematisk og langsiktig arbeid.

Motstandskraften må styrkes
Virksomheter i finansiell sektor gjør en betydelig innsats i å øke motstandskraften i egne systemer. Det er viktig at dette arbeidet videreføres.

Trusselbasert penetrasjonstesting bidrar til å identifisere sårbarheter slik at de kan lukkes før angripere utnytter sårbarhetene. Ved innføring av Lov om digital motstandsdyktighet i finanssektoren (DORA-loven) ble det krav om at foretak med særskilt betydning for det finansielle systemet gjennomfører slike tester av sine systemer og prosesser. Deling av testerfaringer i hele finanssektoren bidrar til å øke motstandskraften i den finansielle infrastrukturen samlet sett.

Fremveksten av stadig kraftigere kunstig intelligens-modeller endrer risikobildet for cybersikkerhet, særlig ved at identifisering av sårbarheter i programvare skjer raskere og i større omfang. Kunstig intelligens-verktøy gir angripere økte muligheter til å utnytte sikkerhetshull før de blir tettet, men kan på sikt styrke forsvar gjennom å bidra til mer effektiv utbedring av sårbarheter. Utviklingen innebærer at systemeiere må oppdatere systemene oftere og raskere. Det forsterker også behovet for god oversikt over IT-systemene. Veletablerte tiltak som overvåking av egne systemer og hyppigere sikkerhetstesting reduserer risiko.

Fremvekst av kvantedatamaskiner kan på sikt utgjøre en trussel mot sikkerhetsmekanismene som benyttes i den finansielle infrastrukturen. Det er derfor nødvendig å innføre kvantesikker kryptografi. Dette er et

omfattende arbeid. Den enkelte virksomhet har ansvar for å sikre egne systemer, men koordinering er viktig for at den finansielle infrastrukturen samlet sett skal være tilstrekkelig sikret. Finans Norges råd til finanssektoren om hvordan utviklingen i kunstig intelligens og kvanteteknologi bør håndteres bidrar til samordnet tilnærming i sektoren.

Samarbeid må styrkes

Den finansielle infrastrukturen består av mange aktører og systemer som må virke sammen for å fungere. Harmonisering av systemer, operasjonelle rammeverk og rutiner på tvers av landegrenser kan gi store effektiviseringsgevinster, men forutsetter tett koordinering og felles innsats. Arbeidet med innføring av kortere oppgjørssyklus i verdipapirhandel (T+1) over hele Europa innen 11. oktober 2027 understreker dette.

Norges Bank mener samarbeid med nordiske og andre europeiske sentralbanker er det beste valget for sikker og stabil drift av oppgjørssystemet i et langsiktig perspektiv. Arbeidet med å koble norske kroner til det europeiske straksbetalingssystemet TARGET Instant Payment Settlement (TIPS) pågår. Parallelt med dette jobbes det også med nødvendige avklaringer for norsk deltakelse i oppgjørssystemet T2.

Det er viktig å kunne opprettholde kritiske funksjoner i den finansielle infrastrukturen, også i en krise-, krigs- eller konfliktsituasjon. Identifisering av grunnleggende nasjonale funksjoner etter sikkerhetsloven gir viktig innsikt i kritiske funksjoner og foretak som understøtter disse. Norges Bank mener likevel at det er behov for en bredere gjennomgang for å vurdere om det er tilstrekkelig styringsevne og handlefrihet for kritiske funksjoner i finansiell sektor i fred, krise og krig. En slik gjennomgang bør også belyse avhengigheter og konsentrasjonsrisiko. Det kan gi et bedre grunnlag for å vurdere behov for tiltak, som for eksempel uavhengige beredskapsløsninger. Slik gjennomgang kan også gi myndighetene et bedre grunnlag for å vurdere konsekvensene av potensielle endringer, slik som oppkjøp og fusjoner.

Den finansielle infrastrukturen blir sikrere med flere betalingsløp

I Norge samarbeider myndighetene og finansnæringen om hvordan beredskapen i betalingssystemet bør styrkes for å kunne stå imot mer alvorlige hendelser. Samarbeidet har resultert i flere anbefalte tiltak som omfatter hele betalingskjeden: hos bankene, i systemene for avregning og oppgjør, og hos utsalgsstedene og husholdningene. Det jobbes nå med å gjennomføre tiltakene, og det er viktig at arbeidet fortsatt prioriteres høyt.

Den finansielle infrastrukturen blir samlet sett både sikrere og mer effektiv når det er flere betalingsløp tilgjengelig, og det er gode beredskapsløsninger ved svikt i ett eller flere ledd. Myndigheter, finansnæring og brukere bidrar til styrket beredskap og redusert risiko gjennom å tilgjengeliggjøre alternative betalingsløp, etablere uavhengige beredskapsløsninger og ha god egenberedskap.

Et av tiltakene som ble fullført våren 2026, er oppdaterte anbefalinger om egenberedskap for betalinger. Disse inkluderer nå også anbefalinger om egenberedskap for utsalgssteder. Sentralt i anbefalingene er at både betaler og betalingsmottaker setter seg i stand til å benytte flere ulike betalingsformer. Mobilbetalingers økende betydning tilsier at også mobilbaserte betalingsløsninger bør støtte flere underliggende betalingsløp.

Fortsatt behov for kontanter
Kontanter har fortsatt en viktig funksjon i betalingssystemet, særlig av beredskapshensyn og for finansiell inkludering, selv om systemet først og fremst sikres gjennom effektive og sikre digitale løsninger. Kontanter brukes i en liten andel av antall betalinger. Samtidig viser en undersøkelse utført for Norges Bank at en fjerdedel av befolkningen bruker kontanter månedlig eller oftere. I samme undersøkelse mener et klart flertall at muligheten til å kunne ta ut og sette inn kontanter er viktig.

Norges Bank har foretatt en ny vurdering av valørsammensetningen. Det er besluttet å holde dagens valørsammensetning uendret, men Norges Bank stanser tilførselen av 1000-kroneseddelen. Den utgjør i dag en begrenset andel av antall sedler i omløp, og har i normalsituasjoner ikke vesentlig betydning for effektivitet ved kontantbetalinger. I alvorlige beredskapssituasjoner vil imidlertid 1000-kroneseddelen kunne ha en viktig rolle. Ved behov kan Norges Bank åpne for tilførsel igjen.

For at kontanter skal kunne fylle sine funksjoner, må publikum ha tilstrekkelig mulighet til å få tak i og bruke kontanter, og næringsdrivende må kunne få tak i veksel og sette inn kontantomsetning. Bankene har en lovpålagt plikt til å tilby sine kunder et tilstrekkelig kontanttjenestetilbud. Det meste av kontanthåndteringen gjennomføres av andre leverandører av kontanttjenester enn bankene. Norges Bank understreker at bankenes ansvar ikke er betinget av et velfungerende leverandørmarked.

Dagens kontanttjenestetilbud er sårbart og har noen svakheter. Hvis bankene ikke sikrer tilfredsstillende løsninger for kontanttjenestetilbudet, mener Norges Bank at det bør utformes mer detaljert regulering av bankenes kontanttjenestetilbud.

Utredningen av tokenisering og digitale sentralbankpenger fortsetter
Norges Bank har vurdert om innføring av digitale sentralbankpenger er hensiktsmessig for at det også i fremtiden skal være sikkert, effektivt og attraktivt å betale med norske kroner. Banken har konkludert med at det nå ikke er grunnlag for å innføre slike penger. Innføring av digitale sentralbankpenger er ikke det best egnede tiltaket nå, hverken for å fremme innovasjon i betalingssystemet, styrke beredskapen eller på annen måte bidra til et mer effektivt og sikkert betalingssystem. Samtidig skjer den teknologiske utviklingen i finanssystemet raskt, og nye tjenester og aktører kommer til. Tokenisering gir muligheter for innovasjon, effektivisering og reduksjon i oppgjørsrisiko. Dersom tokeniserte transaksjoner brer om seg, kan det bli behov for å innføre

løsninger for oppgjør av dem i sentralbankpenger. Samtidig er det flere forhold ved tokenisering som må avklares. Norges Bank fortsetter utredningen av tokenisering og digitale sentralbankpenger for å være klar til å kunne innføre digitale sentralbankpenger dersom det blir nødvendig. Norges Bank vil utvide samarbeidet med aktører i finansnæringen om teknisk testing.

Den europeiske sentralbanken (ECB) har kommet langt i arbeidet med kunderettede digitale sentralbankpenger – en digital euro. ECB oppgir at dersom nødvendig regulering vedtas i EU i år, kan digital euro bli innført i 2029. ECB og eurosystemet utreder og tester også oppgjørsløsninger i sentralbankpenger for transaksjoner og handel i tokeniserte verdier. Disse kan være aktuell infrastruktur for nye former for betalinger og oppgjør i norske kroner, dersom det blir behov og Norges Bank inngår avtale om å benytte det europeiske oppgjørssystemet T2.

Stablecoins har mangler som et allment pengealternativ

Stablecoins er et tokenisert pengealternativ som benytter åpne blokkjeder som transaksjonsinfrastruktur. Bruken av stablecoins er i dag i all hovedsak knyttet til investeringer i kryptoeiendeler, men er i vekst innenfor enkelte nisjer blant annet knyttet til internasjonale betalinger og betalinger som krever programmerbarhet. Stablecoins kan gi gevinster innenfor slike nisjer, men mangler samtidig noen egenskaper som kjennetegner allmenne betalingsmidler. Stablecoins har blant annet vært utsatt for verdisvingninger. Nye reguleringer gjør stablecoins mer robuste mot verdifall som følge av tillitssvikt. Men friksjoner vil fortsatt kunne føre til verdisvingninger som ikke er akseptable for allmenne betalingsmidler og systemviktige oppgjør. Bruken av åpne blokkjeder gir i dag heller ikke den tryggheten for brukerne som følger av eksisterende regelverk for tradisjonelle betalinger.

Hovedstyret

19. mai 2026

Et effektivt betalingssystem

Den norske finansielle infrastrukturen er effektiv, med stabil drift og få avbrudd. Betalinger kan gjennomføres raskt, til lave samfunnsøkonomiske kostnader og på måter som er tilpasset brukernes behov.

Internasjonal harmonisering, tilpasning til endrede standarder og teknologisk utvikling er viktige drivere for videre utvikling. I det følgende gjennomgås noen hovedtrekk i drift og videreutvikling av sentrale komponenter i den finansielle infrastrukturen den siste tiden.

Norges Banks oppgjørssystem (NBO)

NBO er kjernen i det norske betalingssystemet, og de fleste elektroniske betalinger i norske kroner gjøres i siste instans opp mellom bankene i dette oppgjørssystemet. Norges Bank er operatør av NBO.

Dagens oppgjørssystem er effektivt, og driften i 2025 var uten vesentlige avvik. Ved utgangen av 2025 hadde i alt 103 banker og andre finansielle foretak konto i NBO, en reduksjon fra 112 i 2024. Gjennomsnittlig daglig omsetning i NBO økte med 9 milliarder kroner til 359 milliarder kroner i 2025. Ved utgangen av året hadde bankene folio- og reserveinnskudd på 37 milliarder kroner.

Arbeidet med å videreutvikle NBO fortsatte i 2025. En sentral milepæl var overgangen til ISO 20022-standarden for betalingsmeldinger, som legger til rette for mer effektiv samhandling og utvikling av oppgjørssystemene i tråd med internasjonale krav. Det nye formatet ble først tatt i bruk for bruttobetalinger i mars, deretter i verdipapiroppgjøret, og i november for nettobetalinger. Migrering ble gjennomført i samarbeid med deltakerne i NBO og omfattet også tilpasninger i deltakernes egne systemer og prosesser for å imøtekomme kravene i den nye standarden. Driften av oppgjørssystemet med ny meldingsstandard har vært stabil etter produksjonssetting. Overgangen til ISO 20022 innebærer at oppgjørs-systemet fremover vil måtte oppdateres jevnlig i takt med nye versjoner av meldingsstandarden. Bits AS har besluttet at Norwegian Interbank Clearing System (se også omtale under) ikke skal utvikles for å motta og behandle ISO 20022-baserte transaksjoner. Dette har ført til en økning i

antall transaksjoner som sendes til NBO fra 4 595 per dag i 2024 til 13 577 i gjennomsnitt per dag i 2025. Mer detaljert rapportering om NBO er tilgjengelig i årsrapport for NBO.

Norges Bank har videreført arbeidet med neste generasjon oppgjørssystem. Nødvendige avklaringer for deltakelse i eurosystemets oppgjørstjeneste T2 som plattform for NBO RTGS pågår. Arbeidet omfatter blant annet vurderinger av sikkerhet, nasjonal kontroll og krav til beredskapsløsninger. En endelig beslutning vil bli tatt etter at nødvendige avklaringer er gjort.

Norges Bank har også arbeidet videre med etableringen av en ny tjeneste for straksbetalinger i norske kroner (NBO INST) med eurosystemets TIPS som plattform. Bruk av TIPS krever mer omfattende tilpasninger enn tidligere forutsatt, og fremdriftsplanen er under revisjon, i nært samarbeid med ECB og banknæringen i Norge.

Norwegian Interbank Clearing System (NICS)

NICS er bankenes felles system for mottak og avregning av betalingstransaksjoner mellom bankene før de sendes til NBO for endelig oppgjør. Finansnæringens infrastrukturselskap, Bits, har konsesjon fra Norges Bank til å være operatør av NICS, og Norges Bank fører tilsyn med NICS. For teknisk drift og forvaltning av NICS har Bits inngått avtale med Mastercard Payment Services Infrastructure (MPSI). Bits er systemeier og ansvarlig for systemet, også for de deler som er utkontraktert til MPSI.

NICS har hatt stabil drift i 2025. Det var enkelte avvikshendelser som resulterte i forsinkelser i avregningen, men hendelsene ble løst og oppgjøret ble gjennomført samme dag.

Totalt 95 banker deltar i NICS. De samlede verdiene som avregnes gjennom NICS, falt med 35,7 prosent i 2025 til 261 milliarder kroner i gjennomsnitt per dag. Dette skyldes at NICS i september 2025 avsluttet behandlingen av transaksjoner på SWIFT-format. Slike transaksjoner sendes nå direkte fra bankene til NBO. De siste bankene flyttet sin trafikk i august 2025.

Verdipapiroppgjør og sentrale motparter

Ved oppgjør av verdipapirhandler i norske kroner skjer levering av verdipapirer på konto i verdipapirsentralen og betaling via egne kontoer i NBO. For å ta bort risikoen i oppgjøret koordineres selgers overlevering av verdipapir mot kjøpers betaling gjennom Norges Banks og verdipapirsentralens systemer. Den norske verdipapirsentralen driftes av Verdipapirsentralen ASA (Euronext Securities Oslo).

Den samlede verdien av verdipapirer registrert i verdipapirsentralen utgjorde ved årsskiftet 7 698 milliarder kroner. Systemene hadde høy oppetid i 2025. To hendelser førte til forstyrrelser i verdipapiroppgjøret, men begge hendelsene hadde begrensede konsekvenser. Det er

Raskere verdipapiroppgjør i Europa

I dag er det krav om oppgjør av verdipapirhandler innen to dager etter gjennomført handel (T+2). Kommende krav om verdipapiroppgjør innen én virkedag etter handel (T+1) innebærer omfattende endringer i verdipapirmarkedet.

EU-kommisjonen og Den europeiske verdipapir- og markedstilsynsmyndigheten (ESMA) har lagt opp til at hele EU skal gå over til T+1 innen 11. oktober 2027. Finanstilsynet i Norge følger opp dette som EØS-relevant regelverk, og et forslag til lovendring har vært på høring våren 2026. Også Sveits og Storbritannia vil implementere T+1 på samme tid som EU. Innføring av krav om T+1 i Europa følger innføring av tilsvarende krav i USA og Canada i 2024.

Hensikten med kortere oppgjørssyklus er blant annet å redusere motpartsrisiko og marginkrav. Overgangen innebærer en effektivisering av verdipapiroppgjøret, men samtidig ressurskrevende endringer av driftsmønstre, rutiner og teknisk infrastruktur i hele verdipapirmarkedet. Overgangen vil også ha konsekvenser for avregningen i NICS og verdipapiroppgjøret i NBO og hos Euronext Securities Oslo, med utvidet åpningstid og flere avregninger og verdipapiroppgjør i løpet av dagen.

iverksatt tiltak som reduserer risikoen for tilsvarende hendelser i fremtiden.

Euronext Securities Oslo inngår i et konsern med flere andre verdipapir-registre i Europa. Konsernet er i gang med et moderniseringsprosjekt med mål om økt harmonisering på tvers av ulike registre og jurisdiksjoner. Løsningen som utvikles, er tilpasset ECBs løsning for verdipapiroppgjør T2S. Dersom Norges Bank fatter endelig beslutning om tilknytning til T2, vil dette aktualisere spørsmål om tilknytning til T2S.

Som beskyttelse mot mulige problemer hos motparten i perioden fra en handel avtales og frem til oppgjør, skjer oppgjør av mange handler gjennom en sentral motpart. Bruk av sentrale motparter i handlene fører til at de sentrale motpartene får posisjoner som må gjøres opp i det norske verdipapiroppgjøret. De mest brukte sentrale motpartene for norske aktører er for tiden CBOE, SIX x-clear, Euronext CCP og LCH Ltd, hvorav LCH i Storbritannia er særlig mye brukt.

Valutaoppgjør

I en valutahandel veksler partene to valutaer mot hverandre. Dette markedet domineres av de største internasjonale bankene. I et tradisjonelt oppgjør av valuta er det en risiko for at motparten ikke greier å oppfylle sin del av avtalen. For å redusere risikoen i valutaoppgjøret ble den amerikanske valutaoppgjørsbanken CLS (CLS – Continuous Linked Settlement) opprettet i 2002.

CLS håndterer globalt valutatransaksjonsoppgjør i 18 valutaer. 75 av de største bankene globalt gjør opp handler for seg og 38 000 indirekte deltakere. I gjennomsnitt gjøres det opp for 8 000 milliarder. USD per

dag. CLS har siden oppstart levert svært stabile tjenester, og 2025 ble et nytt stabilt år.

I forkant av oppgjøret beregnes alle deltakernes likviditetsbehov i form av nettoposisjoner for hver valuta basert på forhåndsinnmeldte transaksjoner. Nettingen reduserer deltakerbankenes likviditetsbehov med over 95 prosent. I 2025 gjorde bankene opp valutahandler som inkluderte norske kroner for 819 milliarder kroner i gjennomsnitt daglig gjennom CLS. Innbetalingsforpliktelsene til CLS ble redusert til 28 milliarder kroner i gjennomsnitt per dag gjennom beregning av nettoposisjoner.

Oppgjør av valutahandler som inkluderer norske kroner, skjer via CLS' konto hos Norges Bank. Deltakerbankene i CLS overfører sine innbetalingsforpliktelser og får utbetalt sitt tilgodehavende i norske kroner via denne kontoen. For å lette bankenes tilgang på likviditet, har Sveriges Riksbank, Danmarks Nationalbank og Norges Bank opprettet Scandinavian Cash Pool, som gir deltakerbanker i CLS adgang til å låne i SEK, DKK og NOK mot innskudd de har i en annen av de tre sentralbankene.

Elektronisk kunderettet betalingsformidling

Den elektroniske kunderettede betalingsformidlingen omfatter betalinger med bankinnskudd via betalingsinstrumenter som betalingskort og konto-til-konto overføring. Finanstilsynet har ansvar for tilsyn og overvåking av systemene for kunderettet betalingsformidling og publiserer regelmessig rapporter om tilstanden. Norges Bank følger utviklingen i bruken av ulike betalingsmidler og betalingsinstrumenter i den kunderettede betalingsformidlingen.

Måtene vi betaler på har endret seg mye de siste årene. Fortsatt skjer de fleste betalingene på fysiske utsalgssteder, men betalinger for netthandel utgjør en økende del av de samlede betalingene. Fra 2024 til 2025 økte bruken av mobilbetaling særlig mye, både ved handel på fysiske utsalgssteder og ved handel på internett. Den årlige rapporten Kunderetta betalingsformidling gir detaljer om utviklingen.

Mobilbetalinger i butikk fortsetter å vokse

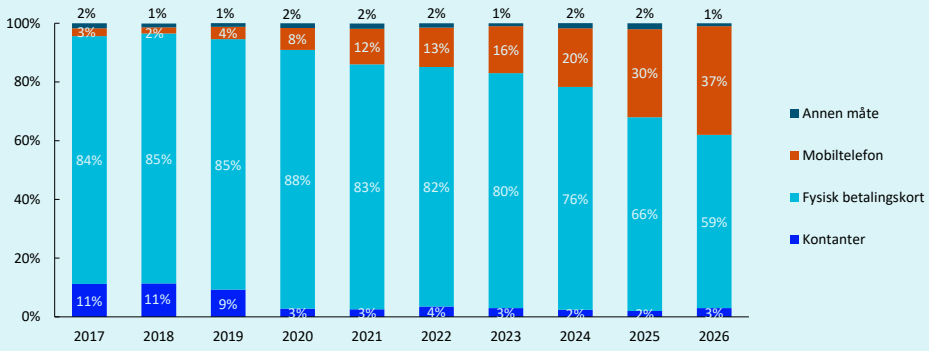
Flere nye løsninger for mobilbetaling i butikk har blitt tilgjengelig i løpet av de siste årene. I august 2024 ble en ny løsning for betaling i Norges-gruppens butikker, Trumf Pay, lansert. I desember 2024 slapp Vipps sin nye betalingsløsning for NFC-betalinger mot fysiske betalingsterminaler, Vipps NFC («tæpping»). I desember 2024 åpnet DNB og Eika-gruppen opp for at også deres kunder kunne betale med Apple Pay. Sommeren 2025 ble Apple Pay tilgjengelig for Sparebank 1s kunder. Utviklingen er tidligere beskrevet i mer detalj i Norges Bank (2025a).

I Norges Bank (2025a) så vi for oss at disse lanseringene ville føre til at veksten i mobilbetalinger i butikk tok seg ytterligere opp. Nå foreligger tall som viser den siste utviklingen. Figur A.1 viser resultater fra Norges Banks spørreundersøkelser. Andelen mobilbetalinger på utsalgssted økte fra 30 prosent i mars 2025 til 37 prosent i mars 2026. Tallene inkluderer både mobilbetalinger mot terminal og nettbaserte mobilbetalinger. Tallene for mobilbetalinger mot terminal alene økte fra 12 prosent i 2024 til 27 prosent i 2025.

I 2024 falt Bank Axepts andel av norske kortbetalinger under femti prosent for første gang siden etableringsfasen tidlig på 1990-tallet. Mye av fallet kan forklares med sterk vekst i netthandelen og økt bruk av kort i utlandet, områder der BankAxept ikke er tilgjengelig. Men også på BankAxepts kjerneområde, kortbetalinger på fysiske utsalgssteder, har den relative bruken gått ned. Dette skyldtes i stor grad sterk vekst i mobilbetalinger på fysiske utsalgssteder. Fram til 2024 var det kun kort fra internasjonale kortnettverk, som Visa og Mastercard, som var underliggende betalingsinstrument ved slike betalinger.

Fra våren 2024 ble BankAxept gradvis gjort tilgjengelig i Apple Pay. BankAxept kunne benyttes i Apple Pay fra desember 2024 for DNB-kunder og Eika-kunder og fra juni 2025 for Sparebank 1s kunder. BankAxept var tilgjengelig fra desember 2024 i Vipps.

Figur A.1 Betalingsmåter på utsalgssteder
I prosent av totalt antall betalinger

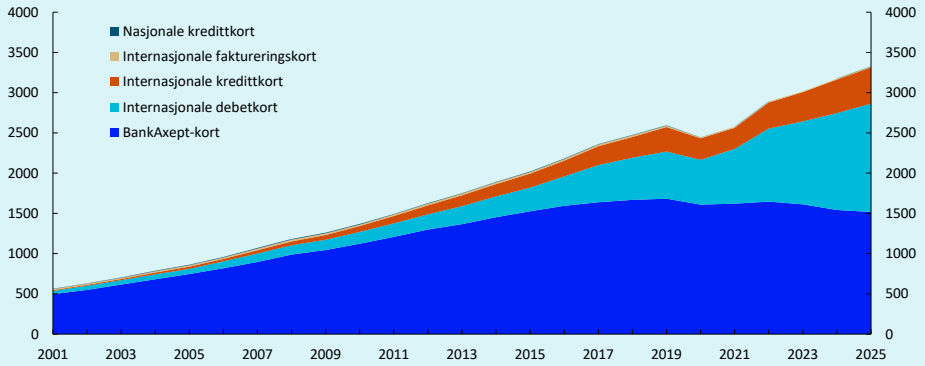


Kilde: Norges Bank

Bruken av de ulike kortnettverkene er ikke kun avhengig av tilgjengelighet. Bruken avhenger også av hva betaler og betalingsmottaker velger. I hovedsak er BankAxept kun tilgjengelig gjennom kombinerte kort, som regel i kombinasjon med et Visa debetkort. Når kombinerte kort, enten fysiske kort eller digitale kort i mobiltelefonen, benyttes i kortterminaler, er det utsalgsstedet som velger hvilket kortnettverk betalingen skal gå gjennom, men betaler kan overstyre dette valget. Trolig går de fleste betalinger med kombinerte kort gjennom BankAxept-nettverket, da dette i mange tilfeller er billigst for utsalgsstedet. De internasjonale kortnettverkene tilbyr også kredittkort, som er ikke-kombinerte kort.

Bruken av BankAxept fortsatte å falle i 2025, se figur A.2. BankAxepts andel av de samlede kortbetalingene gikk ned fra 49 prosent i 2024 til 46 prosent i 2025. BankAxepts del av kortbetalingene er høyere dersom vi kun ser på betalinger mot fysiske betalingsterminaler i Norge, men også her har BankAxept mistet andeler. Markedsandelen for dette segmentet falt fra 74 prosent i 2024 til 70 prosent i 2025. Nedgangen kan skyldes flere forhold. Blant annet er det fortsatt flere banker som ikke har lagt til rette for mobilbetaling med BankAxept. BankAxept er heller ikke tilgjengelig for andre NFC-baserte mobilbetalingsløsninger enn Apple Pay og Vipps NFC, slik som Google Pay og Samsung Pay.

Figur A.2 Bruk av norske betalingskort.
Etter utsteder og funksjon. I millioner transaksjoner



Kilde: Norges Bank

Kontanter

Norges Bank har ansvar for å dekke samfunnets etterspørsel etter kontanter både i normal- og krisesituasjoner gjennom å forsyne bankene med kontanter.

Mengden kontanter i omløp avhenger av bruk til betalinger og verdi-oppbevaring, men også av kontantinfrastrukturen og sirkulasjons-mønsteret. Den nominelle verdien av kontanter i omløp var stabil i perioden fra 2006 frem til 2015. Fra 2016 til 2025 har den sunket med rundt en fjerdedel. Årsgjennomsnittet for verdien av sedler i omløp i 2025 utgjorde 33,6 milliarder kroner, noe som er en nedgang på 0,8 milliarder kroner (2,2 prosent) fra 2024. Verdien av mynter i omløp viser en nedgang fra 4,19 til 4,14 milliarder kroner (1,3 prosent) fra 2024 til 2025.

Også realverdien av kontantene i omløp har sunket betydelig i den samme perioden. I 2025 var omløpet målt i forhold til BNP Fastlands-Norge og i forhold til privat konsum henholdsvis 0,9 og 1,7 prosent. Dette er noe lavere enn i 2024, og en halvering siden 2016. Kontantenes andel av verdien av betalingsmidler disponert av publikum (M1) har også falt jevnt over tid. I 2025 var andelen på 1,3 prosent, mot 2,7 prosent i 2016. Dette er veldig lavt sammenlignet med de fleste andre land vi har statistikk fra. Utvikling og sammensetning av sedler og mynter i omløp er nærmere omtalt i Årsrapport sedler og mynter 2025.

Mengden kontanter i omløp forteller ikke hvor ofte disse kontantene brukes i betalinger eller hvem som betaler med kontanter. Norges Bank gjennomfører en årlig betalingsundersøkelse hvor vi spør hvordan respondentene betalte forrige gang de handlet på et fysisk utsalgssted eller betalte til privatperson. Undersøkelsen har vist at kontantandelen av betalingene har falt over tid, og har siden 2020 utgjort cirka 3 prosent. I desember 2025 gjennomførte Norges Bank en noe mer omfattende spørreundersøkelse om kontanter rettet mot forbrukere. Undersøkelsen viser at 25 prosent av befolkningen bruker kontanter månedlig eller oftere. Kontantenes rolle i betalingssystemet er nærmere omtalt i artikkelen «Det er fremdeles behov for kontanter», og bruken av kontant-tjenester er nærmere omtalt i den årlige rapporten Kunderetta betalingsformidling.

Et sikkert betalingssystem

Norge har et sikkert betalingssystem, men et mer alvorlig trusselbilde øker risikoen for alvorlige hendelser. Derfor må styrking av sikkerhet og beredskap i betalingssystemet prioriteres.

Sikkerheten og beredskapen i de enkelte virksomhetene er førstelinje-forsvaret i betalingssystemet og den finansielle infrastrukturen som helhet. Både myndighetene og de private aktørene har høy oppmerk-somhet om risiko, sårbarheter og nødvendigheten av å jobbe systematisk med sikkerhet og beredskap. Det er strenge krav til sikring og testing. Det er også krav til kontinuitets- og reserveløsninger. Øvelser gjennomføres regelmessig, og effektiv samhandling i hele sektoren bidrar til god hendelseshåndtering. Alle disse elementene har bidratt til høy motstands-kraft i den finansielle infrastrukturen. Uønskede hendelser og angrep har sjelden utviklet seg til alvorlige konsekvenser. Men for at dette skal være tilfelle også i fremtiden, må sikkerhet og beredskap styrkes ytterligere.

Et krevende trusselbilde fordrer tiltak langs flere spor

Åpne trusselvurderinger fra Nordic Financial CERT (NFCERT), Etterretnings-tjenesten, Politiets Sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet viser at Norge i 2026 står overfor den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. I trusselvurderingene fremstår særlig hybride trusler – der digitale og fysiske angrep kombineres –som stadig mer aktuelle. Fiendtlige stater og organiserte kriminelle driver mer etterretning. De har større evne og vilje til å iverksette sabotasje og påvirkningsoperasjoner – også mot norske interesser. I kraft av å forvalte store verdier og drifte samfunnskritiske tjenester er banker og andre nøkkelforetak i finansiell infrastruktur attraktive angrepsmål.

Geopolitiske spenninger påvirker nå også områder som tidligere ble betraktet som stabile. Når stormakter utfordrer internasjonale regler og avtaler, kan det forstyrre handel, finansmarkeder og den finansielle infrastrukturen. Mange tiår med økende globalisering og integrering har gitt gevinster, men samtidig skapt avhengigheter over landegrensene som kan brukes som politisk pressmiddel.

Oppbygging av sårbarheter i finansiell infrastruktur (se ramme) skjer over tid, men risikoene kan materialisere seg brått. Nyere tids utvikling har blant annet satt et søkelys på risiko knyttet til avhengighet av globale teknologigiganter. Som et av verdens mest digitaliserte samfunn er mange samfunnskritiske tjenester i Norge avhengig av globale leverandører og systemplattformer. Norske aktørers mulighet til å styre hvordan globale aktører opererer er begrenset. Muligheten til å erstatte dem i rimelig tid er også begrenset dersom de stanser eller begrenser sine tjenester her.

Et sikkert betalingssystem

Sårbarheter i finansiell infrastruktur

Mange avhengigheter
Den finansielle infrastrukturen består av mange komponenter som er avhengige av hverandre og av underliggende infrastruktur som strømforsyning og elektronisk kommunikasjon. Digitalisering og systemintegrasjon har gitt oss effektive betalingstjenester som gjør det mulig å betale raskt, billig og tilpasset brukernes behov og preferanser.

Samtidig innebærer dette at bortfall av kritiske komponenter raskt får store konsekvenser. I alvorlige krisescenarioer som sabotasje, naturkatastrofe eller krig kan selv godt beskyttede systemer bli utilgjengelige. Kompleksiteten knyttet til et høyt antall systemer og avhengigheter i betalingsløpene, med tilhørende komplekse leverandørkjeder, øker også antallet mulige angrepsflater. Geopolitiske spenninger øker risikoen for at avhengigheter over landegrenser brukes som politisk pressmiddel.

Utstrakt utkontraktering
Finansiell sektor utkontrakterer mange tjenester og oppgaver. Formålet er ofte mer kostnadseffektive og mer robuste løsninger. Stordriftsfordeler i systemer og spesialiserte kompetansemiljøer fører naturlig til konsolidering og konsentrasjon i markedet for disse tjenestene.

Samtidig innebærer økt grad av utkontraktering og konsentrasjon en sårbarhet på systemnivå når mange aktører benytter samme programvare, maskinvare og systemplattformer. Avhengighet av noen få leverandører innen skytjenester, systemprogramvare og kjernesystemer gjelder flere kritiske funksjoner i den norske finansielle infrastrukturen.

I takt med konsentrasjon i leverandørmarkedet har også selskapsstrukturen blitt mer komplisert og består gjerne av flere underselskaper som kan være underlagt forskjellige lands regelverk. Det gjør det mer krevende for myndigheter og systemeier å opprettholde innsikt i hvilke risikoer leverandøren er utsatt for innenfor teknologisk sikkerhet, personellsikkerhet og regulatoriske endringer i hjemlandet.

Attraktive angrepsmål
I kraft av å oppbevare og formidle store verdier er banker, sentrale aktører og systemer i det norske finansielle systemet attraktive angrepsmål for ulike trusselaktører.

Digital vinningskriminalitet øker, og organisert kriminalitet er en betydelig trussel mot finansinstitusjonene og deres kunder. Kortinformasjon, identiteter, tilganger og andre sensitive og verdifulle data er blant det som stjeles. Et mer spent geopolitisk landskap innebærer også at sammensatte trusler, der statlige og kriminelle aktører samarbeider, forekommer oftere. Teknologisk utvikling som kunstig intelligens gir angriperne nye verktøy, men kan også gi nye muligheter på forsvarssiden.

For å redusere risikoen knyttet til sårbarheter kreves systematisk og langsiktig arbeid langs flere spor:

- **Økt motstandskraft:** Det er viktig å fortsette kontinuerlig herding av eksisterende systemer, blant annet gjennom avansert trusselbasert testing.
- **Samarbeid:** For å møte både trusler og muligheter i en integrert internasjonal finansiell infrastruktur må samarbeidet styrkes, både nasjonalt og med nære allierte i Norden og Europa.
- **Diversifisering:** Både myndigheter, finansnæring og brukere har viktige roller i å redusere risiko gjennom å tilgjengeliggjøre alternative betalingsløp, etablere uavhengige beredskapsløsninger og god egenberedskap.

Økt motstandskraft

Arbeidet med å styrke motstandskraften i eksisterende systemer må videreføres. Virksomheter i finansiell sektor legger ned en betydelig innsats i å øke motstandskraften i egne systemer. Trusselbasert penetrasjonstesting (Threat-Led Penetration Testing – TLPT) er krevende tester, hvor kritiske funksjoner med tilhørende systemer og prosesser i den enkelte virksomhet blir utsatt for virkelighetsnære angrep fra avanserte angripere. Nettopp fordi testene er realistiske gir de god læring og systemspesifikke innsikter som raskt kan brukes til å tette hull og forsterke sikkerhets- og beredskapstiltak.

Ved innføringen av Lov om digital motstandsdyktighet i finanssektoren (DORA-loven) ble TLPT obligatorisk for utpekte virksomheter med krav til frekvens og rapportering.

I DORA-loven utpekes virksomheter etter kvantitative eller kvalitative kriterier av Finanstilsynet med innspill fra Norges Bank. Finanstilsynet har våren 2026 utpekt hvilke virksomheter som omfattes av kravet i første omgang, og Norges Bank er i gang med å planlegge for testing i samarbeid med de utpekte virksomhetene. Virksomheter som prioriteres, er de 15–20 største virksomhetene innenfor finansiell sektor med ansvar for kritisk infrastruktur.

Det europeiske TIBER-rammeverket gir retningslinjer og veiledning for gjennomføring av TLPT-tester. Finanstilsynet og Norges Bank har samarbeidet om den norske implementeringen av dette rammeverket, TIBER-NO. I tillegg til de virksomhetene som allerede var invitert til frivillig testing i tråd med TIBER-NO, blir også de største forsikringsselskapene pålagt TLPT-testing ved innføring av DORA-loven.

Norges Bank bistår virksomhetene med planlegging, koordinering av involverte aktører, risikovurderinger, gjennomføring og evaluering av TIBER-tester. En viktig del av arbeidet er å tilrettelegge for deling av erfaringer mellom virksomheter som har gjennomført slike tester.

Gjennom TIBER-forum kan deltakerne utveksle informasjon og erfaringer med hverandre i en fortrolig ramme som gir rom for diskusjoner om aktuelle og sensitive problemstillinger. Ved å dele erfaringer får flere anledning til å nyttiggjøre seg dem og fjerne eventuelle svakheter i egen virksomhet før disse kan utnyttes av trusselaktører. Dette styrker motstandskraften i den finansielle infrastrukturen som helhet. Noen av de generelle erfaringene som er høstet til nå er blant annet:

- Sikkerhetsnivået er gjennomgående høyt, særlig i systemer eksponert mot internett. Nivået er imidlertid ikke alltid like høyt på innsiden av ytre forsvarsverk. I slike tilfeller er virksomheten sårbar for at angriper kan eskalere egne tilganger eller bevege seg fra sted til sted i IT-systemene.
- I testene benyttes sosial manipulasjon over e-post, SMS eller telefon for å vurdere hvordan angripere kan utnytte menneskelige svakheter. Slike angrep kan være svært krevende å oppdage. Sosiale medier som LinkedIn kan gjøre det enklere å identifisere nøkkelpersoner med tilganger til de mest sensitive systemene og rette målrettede angrep mot disse.
- Virksomhetene investerer mye i sikkerhetsteknologi, men teknologien er ikke alltid godt nok tilpasset eget IT-miljø. Manglende tilpasning av oppsett svekker evnen til å fange opp varselsignaler ved cyberangrep, og kan gi falsk trygghet.
- Testene har avdekket en konsentrasjonsrisiko knyttet til utstrakt bruk av de samme sikkerhetsleverandørene og tilsvarende sikkerhets-programvare på tvers av virksomheter. Når mange aktører baserer seg på like løsninger, kan sårbarheter få bredere konsekvenser enn for den enkelte virksomhet. Dette kan skape betydelige utfordringer dersom flere av en leverandørs kunder rammes av et angrep samtidig, for eksempel ved at hendelseshåndtering, brukerstøtte og gjenoppretting blir flaskehalser.
- Foretak med fragmenterte IT-miljøer har ofte svakere samlet sikkerhet. En stor og sammensatt systemportefølje gir økt angrepsflate, samtidig som sikkerhetsarbeidet blir mer krevende å skalere og prioritere. Foretak med mer sentraliserte og harmoniserte løsninger står derfor ofte bedre rustet.

Fremveksten av stadig kraftigere KI-modeller endrer risikobildet for cybersikkerhet, særlig gjennom økt tempo og skala i identifisering og utnyttelse av sårbarheter i programvare. Dette er en utvikling vi har sett over tid, men som er aktualisert ved introduksjon av nye, avanserte KI-modeller som Claude Mythos.

Slike avanserte modeller har inntil nylig i hovedsak vært tilgjengelige for et begrenset antall aktører, særlig store internasjonale teknologi-leverandører. Dette kan styrke sikkerheten i deres systemer, men kan samtidig forsterke avhengigheter og konsentrasjonsrisiko knyttet til noen få globale teknologileverandører.

De nye modellene har vist seg å kunne analysere store datamengder på kort tid og har blant annet kunnet identifisere såkalte nulldagssårbarheter, det vil si sårbarheter som har vært ukjente for leverandørene. Økt utbredelse av slike verktøy øker risikoen for at sårbarheter kan utnyttes før de blir utbedret. Samtidig gir teknologien nye muligheter til å styrke cybersikkerheten, blant annet gjennom bedre overvåking, automatisert testing og raskere utbedring. Over tid kan dette bidra til økt robusthet i systemene.

På kort sikt kan utviklingen innebære økt frekvens, tempo og skala i cyberangrep. Systemeiere vil i mange tilfeller få kortere tid til å identifisere og rette sårbarheter. Dette øker behovet for god oversikt over egne systemer og leverandørkjeder, rask respons ved hendelser og robuste kontinuitets- og gjenopprettingsløsninger.

Utviklingen er global og berører alle sektorer. Det arbeides nasjonalt og internasjonalt med å etablere felles situasjonsforståelse og styrke samordningen av tiltak. Finans Norges anbefalinger til finanssektoren bidrar til en samordnet tilnærming til håndtering av KI-relatert cyberrisiko. For Norges Bank innebærer dette at arbeidet med å styrke motstandskraften i betalings- og oppgjørssystemene prioriteres høyt. Det legges vekt på tidlig identifisering av sårbarheter, tydelige krav til leverandører og oppfølging gjennom overvåking og tilsyn.

Et annet tema som berører motstandskraften i eksisterende systemer, er kryptografi. Grunnleggende sikkerhetsprotokoller i den finansielle infrastrukturen bygger i stor grad på kryptografiske algoritmer som har vært ansett som sikre i flere tiår. Men på sikt kan fremvekst av kryptografisk relevante kvantedatamaskiner utgjøre en trussel mot disse sikkerhetsprotokollene. Overgangen til kvantesikker kryptografi i finansiell infrastruktur er et omfattende arbeid, men i motsetning til mange tidligere problemer med kryptografi som ofte måtte løses på kort varsel, er denne overgangen planlagt og gradvis. Viktige fremskritt er allerede gjort, men arbeidet er langt fra ferdig. Arbeidet er nærmere omtalt i artikkelen «Trusselen fra kvantedatamaskiner og tiltak i finanssystemet».

Styrket samarbeid nasjonalt og internasjonalt

Den finansielle infrastrukturen handler om samhandling – nasjonalt og internasjonalt. Dette er vesentlig for både effektiviteten og sikkerheten i infrastrukturen. Samarbeid mellom aktørene styrker forsvarsverkene, og utvikling av alternative betalingsløp og beredskapsløsninger skjer i et samspill mellom næringen og myndighetene. God hendelseshåndtering forutsetter også tett samarbeid og koordinering, ettersom integrering av ulike systemer og aktører gjør at hendelser raskt kan få store konsekvenser på tvers av foretak og landegrenser.

I Norge har myndighetene og næringen samarbeidet om beredskap og hendelseshåndtering i lang tid. Beredskapsutvalget for finansiell

infrastruktur (BFI) ble etablert i 2000 for å kunne samle relevante aktører i Norge ved en større hendelse, utveksle informasjon og koordinere respons. Gjennom BFI møtes myndighetene og næringen også regelmessig for felles øvelser. I 2025 deltok BFI i den tverrsektorielle øvelsen Digital 2025. Øvelsen simulerte blant annet et omfattende cyberangrep mot finanssektoren og var en opptakt til det nasjonale øvelsesprogrammet Totalforsvarsåret 2026. Dette programmet skal styrke Norges evne til å forebygge og håndtere sikkerhetspolitiske kriser og krig gjennom en rekke ulike aktiviteter. Finanssektoren deltar i dette fra både myndighetenes og næringens side.

Regjeringen varslet i Totalberedskapsmeldingen at det skal etableres en ny rådsstruktur for departementenes arbeid med beredskapsplanlegging og tilstandsvurderinger i sivile sektorer. Finansielle tjenester er ett av samfunnsområdene hvor det skal være et slikt råd. Finansdepartementet vurderer nå, i samråd med Finanstilsynet og Norges Bank, hvordan formålet med beredskapsråd kan oppfylles på beste måte i finans-sektoren, og herunder i hvilken grad etablerte rådsstrukturer som Beredskapsutvalget for finansiell infrastruktur kan bygges videre på.

NFCERT er et samarbeids- og etterretningssenter for cybersikkerhet og finansiell kriminalitet som bistår nordiske finansforetak med analyse og håndtering av digitale angrep. En betydelig andel av foretakene i den norske finanssektoren er medlem av NFCERT, inkludert Norges Bank. Bred og aktiv deltakelse i NFCERT styrker finansiell sektor og den finansielle infrastrukturen. NFCERT er sammen med Finanstilsynet sektorvis responsmiljø for IT-sikkerhetshendelser og er i likhet med Norges Bank partnere i Nasjonalt cybersikkerhetssenter.

For å styrke vurderinger av systemiske IT-risikoer som kan true finansiell stabilitet har Finanstilsynet og Norges Bank sammen etablert en analysegruppe som også inkluderer andre sentrale aktører i det finansielle systemet. Analysegruppen har utviklet en metode for slike vurderinger, som bygger på en modell utviklet av European Systemic Cyber Group (ECSG). I 2025 er det gjennomført en pilot for å teste metoden. Finanstilsynet og Norges Bank besluttet i 2026 å videreføre samarbeidet i analysegruppen.

Samarbeid og dialog er ikke utelukkende knyttet til beredskap. Gjennom Betalingsforum samles et bredt sett av interessenter i betalingssystemet: myndigheter, finansnæring og representanter for forbrukere og ikke-finansielle bedrifter. Formålet med forumet er utveksling av informasjon om aktuelle saker og drøfting av innspill til hvordan betalingssystemet kan forbedres.

Internasjonalt er også samarbeidet styrket. Det er nå etablert flere fora for å utveksle informasjon og koordinere respons mellom myndighetene på tvers av landegrensene. EU Systemic Cyber Incident Coordination Framework (EU-SCICF) ble etablert i november 2024 gjennom EUs DORA-forordning artikkel 49, og implementert i Norge fra 1. juli 2025.

Working Group on Operational Resilience (WGOR) ble etablert i 2025 som et nytt samarbeidsforum under Nordic Baltic Stability Group (NBSG), og gir nordisk-baltiske myndigheter en arena for å koordinere sin aktivitet i EU-SCICF og gjennomføre felles øvelser. Gjennom NFCERT har den nordiske finansnæringen etablert et velfungerende samarbeid om trusseletterretning, informasjonshåndtering og hendelseshåndtering.

Harmonisering av systemer, operasjonelle rammeverk og rutiner på tvers av landegrenser kan gi store effektiviseringsgevinster. Spesialiserte kompetansemiljøer og robuste systemer lokalisert utenfor Norge kan gi verdifulle bidrag i arbeidet med å styrke drift, utvikling og sikkerhet i norsk finansiell infrastruktur. Norges Bank mener samarbeid med nordiske og andre europeiske sentralbanker er det beste valget for sikker og stabil drift av oppgjørssystemet i et langsiktig perspektiv. Arbeidet med å koble norske kroner til det europeiske straksbetalingssystemet TARGET Instant Payment Settlement (TIPS) pågår, men krever mer omfattende tilpasninger enn opprinnelig forutsatt. Dette har gjort det nødvendig å revidere fremdriftsplanen. Parallelt med dette jobbes det også med nødvendige avklaringer for eventuell norsk deltakelse i oppgjørssystemet T2.

Samtidig som samarbeid med andre er en styrke, er det avgjørende å kunne stå på egne ben dersom det skulle bli nødvendig. Dersom lokale kompetansemiljøer blir for små og avstanden til drift og utvikling av kritiske systemer for stor, kan lokal evne til å styre og kontrollere leveranser bli svekket. I en tilspisset geopolitisk situasjon kan avhengigheter av ressurser i andre land bli en alvorlig sårbarhet. Utenlandsk eierskap, tjenesteutsetting til utlandet og avhengighet av nøkkelressurser fra andre land kan svekke norske aktørers styringsevne og handlefrihet, særlig i en krise-, krigs- eller konfliktsituasjon.

Det er viktig å kunne opprettholde kritiske funksjoner i den finansielle infrastrukturen, også i en krise-, krigs- eller konfliktsituasjon. Identifisering av grunnleggende nasjonale funksjoner etter sikkerhetsloven gir viktig innsikt i kritiske funksjoner og foretak som understøtter disse. Norges Bank mener likevel at det er behov for en bredere gjennomgang for å vurdere om det er tilstrekkelig styringsevne og handlefrihet for kritiske funksjoner i finansiell sektor i fred, krise og krig. En slik gjennomgang bør også belyse avhengigheter og konsentrasjonsrisiko. Det kan gi et bedre grunnlag for å vurdere behov for tiltak, som for eksempel uavhengige beredskapsløsninger. Slik gjennomgang kan også gi myndighetene et bedre grunnlag for å vurdere konsekvensene av potensielle endringer, slik som oppkjøp og fusjoner.

Datagrunnlaget for å gjøre slik kartlegging vil fremover bli bedre. Det er nå krav om at alle virksomheter som er omfattet av DORA, skal ha et register over IKT-tjenesteavtaler (RoI), og at registeret skal inn-rapporteres til Finanstilsynet. Alle foretakets IKT-tjenesteavtaler skal fremgå av RoI og det skal blant annet fremgå hvilke avtaler som er kritiske eller viktige. Frist for rapportering til registeret var 13. mars 2026. I tråd med DORA vil det samles et register også på europeisk nivå.

Sikkerhet og effektivitet gjennom diversifisering

Den finansielle infrastrukturen blir samlet sett både sikrere og mer effektiv når det er flere betalingsløp tilgjengelig, og det er gode beredskapsløsninger ved svikt i ett eller flere ledd.

I Norge samarbeider myndighetene og finansnæringen om hvordan beredskapen i betalingssystemet bør styrkes for å kunne stå imot mer alvorlige hendelser. Samarbeidet har resultert i flere anbefalte tiltak som omfatter hele betalingskjeden: hos bankene, i systemene for avregning og oppgjør, og hos utsalgsstedene og husholdningene. Mange av tiltakene innebærer styrking av eksisterende reserveløsninger eller etablering av nye. Gjennom 2025 og 2026 har Finansdepartementet gjennomført flere møter og mottatt rapporteringer fra finansnæringen, Norges Bank og Finanstilsynet om oppfølgingen av tiltakene som er anbefalt. Det jobbes nå med å gjennomføre de anbefalte tiltakene. Tiltakene har ulik grad av kompleksitet, og mange av tiltakene krever ytterligere utredning av næringen eller myndighetene før de eventuelt kan gjennomføres.

Et av tiltakene som ble fullført våren 2026, er nye anbefalinger om egenberedskap for betalinger. Disse inkluderer nå også anbefalinger for utsalgssteder. Anbefalingene er nærmere omtalt i artikkelen «Egenberedskap for betalinger». Et gjennomgående tema er at både mottaker og betaler bør sette seg i stand til å benytte flere ulike betalingsformer.

Kontanter benyttes mindre enn før, men har likevel fortsatt en viktig funksjon i betalingssystemet, særlig av beredskapshensyn. Dagens digitale beredskapsløsninger er ikke tilstrekkelige til at kontantenes rolle i beredskap kan reduseres. Kontantenes rolle i betalingssystemet er nærmere omtalt i artikkelen «Det er fremdeles behov for kontanter».

Det dominerende betalingsmiddelet i Norge i dag er bankinnskudd gjennom kontobetalinger og kortbetalinger. Begge disse betalingsformene kan gjøres med mobiltelefon, og omfanget av mobiltelefonbetalinger fortsetter å øke. Mobil har lenge hatt en dominerende andel av betalinger mellom privatpersoner og utgjør nå nær fire av ti betalinger på fysiske utsalgssteder (se omtale under «Et effektivt betalingssystem»). Veksten indikerer at brukerne opplever mobilbetalinger som både effektive og sikre. Men for å ivareta hensyn til konkurranse, kostnadseffektivitet og beredskap er det viktig at ulike betalingskort og kontobetalinger er tilgjengelig som underliggende betalingsløsning. Mobiltelefonens økende betydning for betalinger tilsier også prioritering av arbeidet med å utvikle robuste beredskapsløsninger for mobilbetalinger for tilfeller der kommunikasjonslinjer er nede.

Parallelt med endringer i tradisjonelle betalingsformer lanseres det også nye betalingssystemer med alternative betalingsmidler. Dersom disse

oppfattes å ha attraktiv funksjonalitet, dekker kundebehov og oppnår tilstrekkelig tillit, kan de få vesentlig utbredelse. Noen av de nye systemene kan bidra til at grensekryssende betalinger blir billigere og raskere. Samtidig kan globale aktører få en enda større rolle i betalingssystemet. Såkalte stablecoins er et alternativt betalingsløp som foreløpig har en ubetydelig rolle i det norske betalingssystemet. Stablecoins bruker åpne blokkjeder som transaksjonsinfrastruktur. Det gir muligheter, men både tjenesteutvikling og ytterligere reguleringer er nødvendig for at slike infrastrukturer kan brukes som allmenne betalingsmidler. Stablecoins har heller ikke vært stabile nok til å kunne være allmenne betalingsmidler. Nye reguleringer kan motvirke prisfall som følge av tillitssvikt, men avhjelper ikke verdisvingninger som følge av friksjoner i markedet. Temaet er nærmere omtalt i artikkelen «Kan stablecoins svinge seg frem til allmenn bruk?»

Norges Bank har i flere år utredet hvorvidt det er behov for digitale sentralbankpenger (DSP) for at det også i fremtiden skal være sikkert, effektivt og attraktivt å betale med norske kroner. Utredningen har konkludert med at det nå ikke er grunnlag for å innføre DSP, men at det kan bli aktuelt i fremtiden. Norges Bank vil fortsette å utrede tokenisering og ulike former for DSP for å være klar til å kunne innføre DSP dersom det blir nødvendig for et effektivt og sikkert betalingssystem. Banken vil utrede muligheter og konsekvenser av tokenisering blant annet gjennom teknisk og funksjonell testing av teknologi, også i samarbeid med andre aktører i finanssektoren. Arbeidet er nærmere omtalt i artikkelen «Tokenisering og digitale sentralbankpenger».

I fokus

Egenberedskap for betalinger

Gode beredskapsløsninger hos banker og andre aktører i betalingssystemet er førstelinjeforsvaret for å håndtere avvik og større hendelser i den elektroniske betalingsformidlingen. Men også hver enkelt bruker spiller en viktig rolle i å begrense negative konsekvenser av hendelser. Ved å følge anbefalinger om egenberedskap kan både betalere og mottakere av betalinger bidra til økt motstandskraft i betalingssystemet.

Selv om betalingssystemet fungerer godt i Norge, kan ulike hendelser føre til at tjenester og funksjoner som tas for gitt blir utilgjengelige i kortere eller lengre perioder. Slike hendelser kan være alt fra teknisk feil, ekstremvær, sabotasje og i verste fall krigshandlinger.

Gjennom god egenberedskap bidrar hver enkelt først og fremst til at en selv og ens nærmeste blir mindre påvirket av alt fra små hendelser til større kriser. Samtidig letter dette presset på systemet som helhet.

Egenberedskap for å betale

Norges Bank har i flere år publisert praktiske råd om egenberedskap for betalinger. Disse setter søkelyset på hvilke betalingsalternativer hver enkelt bør ha tilgjengelig:

- Flere og ulike betalingskort
- Noe kontanter
- Konto i flere banker

Rådene understreker at det er viktig å ha minst ett fysisk BankAxept-kort, da enkelte av dagens beredskapsløsninger for kortbetaling bygger på denne typen kort. Videre er det viktig at fysiske betalingskort jevnlig brukes med chip (ved å sette kortet inn i terminalen) og PIN-kode. Dette sikrer at informasjonen som er lagret på kortet holdes oppdatert, herunder eventuell ny beredskapsfunksjonalitet som gjøres tilgjengelig. Også enkelte internasjonale betalingskort har beredskapsfunksjonalitet som aktiveres når kortet brukes på denne måten. Beredskaps-funksjonaliteten i et kort varierer mellom ulike korttyper og etter hvem som har utstedt kortet.

Du kan lese mer om de praktiske rådene om egenberedskap for betalinger på norges-bank.no og på Direktoratet for samfunnssikkerhet og beredskap (DSB) sine nettsider for egenberedskap.

Egenberedskap for å motta betaling

I fokus

For at en betaling skal kunne gjennomføres må både betaler og mottaker av betaling ha ulike betalingsalternativer tilgjengelig. Egenberedskap for mottak av betaling er særlig viktig for utsalgssteder som selger nødvendighetsvarer.

Som oppfølging av anbefalt tiltak fra en arbeidsgruppe som på oppdrag fra Finansdepartementet har vurdert beredskapen i det digitale betalingssystemet, har Norges Bank koordinert et samarbeid om å utarbeide veiledende generelle anbefalinger om egenberedskap for utsalgssteder (se ramme). Samarbeidet har inkludert representanter fra Virke, NHO Service, NorgesGruppen, Coop, Rema 1000 og Circle K. Anbefalingene er nå publisert på norges-bank.no, og hver enkelt virksomhet oppfordres til å konkretisere og tilpasse anbefalingene til egen situasjon.

Egenberedskap for betalinger på utsalgssteder

I Norge har vi et effektivt og sikkert betalingssystem, og norske utsalgssteder opplever sjelden alvorlige feil i sine betalingsløsninger. Men selv om løsningene er sikre og det er etablert kontinuitetsløsninger, kan avvik likevel oppstå. For å gi økt trygghet for at utsalgssteder kan motta betaling fra kunder også ved avvik i ordinære betalingsløsninger, anbefaler Norges Bank at utsalgsstedene vurderer følgende egenberedskapstiltak:

Flere kortløsninger: Støtte for flere kortløsninger via både fysiske kort og digitale kort på mobil i utsalgsstedets betalingsterminal gir beredskap for tilfeller der én spesifikk kortløsning ikke fungerer.

Alternativer til betalingsterminal: Støtte for alternative betalingsløp gir beredskap for tilfeller der kunden ikke kan gjennomføre kortbetaling på terminal. Eksempler på et slike alternative betalingsløp er generering av betalingsforespørsel via QR-kode og mobilapplikasjoner.

Offline betaling: Støtte for offline betaling i betalingsterminalen gir beredskap for tilfeller der terminalen ikke oppnår kontakt med sentral infrastruktur. Betalingen blir sendt videre fra terminalen når kontakt er gjenopprettet.

Reserve kassasystem: Tilgang til en uavhengig reserveløsning for både kassasystem og betalingsterminal gir støtte for tilfeller der ordinært kassasystem ikke fungerer.

Kontanter: Kontant betaling gir beredskap for tilfeller der andre betalingsløsninger svikter, og forbrukere har lovbestemt rett til å betale med kontanter på et utsalgssted. Både ordinært kassasystem og reservekassasystem må derfor støtte kontant betaling. Utsalgssteder bør også ha noe veksel tilgjengelig for begge.

Generell beredskap understøtter betalingsberedskap
I noen scenarioer vil effekten av beredskapstiltakene over avhenge av at også mer generelle beredskapstiltak er på plass. I tråd med generelle anbefalinger fra DSB bør utsalgsstedene også vurdere følgende beredskapstiltak:

Alternative kommunikasjonslinjer: At utsalgsstedets kassasystem og betalingsterminaler kan benytte flere kommunikasjonslinjer, gir beredskap for tilfeller der primær kommunikasjonslinje faller ut.

Nødstrøm: Selv om reserveløsninger for kommunikasjon, kassasystem og betalingsterminal kan driftes i noe tid på batteri, kan andre funksjoner gjøre det nødvendig med nødstrømforsyning.

Innøvd beredskapsplan: For at beredskapsløsninger skal fungere, må ansatte på utsalgsstedet vite hvordan de tas i bruk. En beredskapsplan som øves regelmessig er et viktig verktøy for å oppnå dette.

Det er fremdeles behov for kontanter

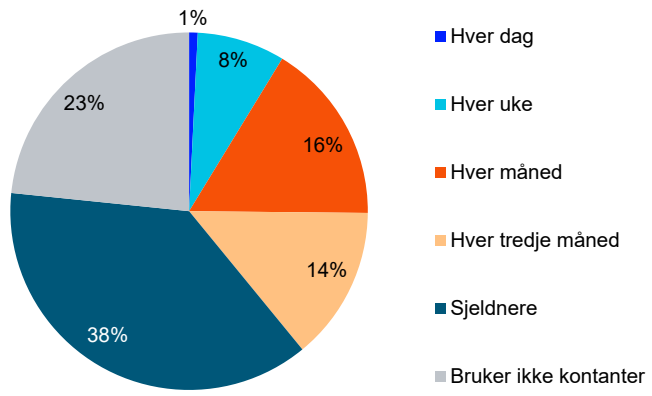
Norge er blant landene med lavest kontantandel i verden. Betalinger foregår i all hovedsak digitalt, og et effektivt og sikkert betalingssystem sikres først og fremst gjennom gode digitale løsninger. Kontantene har likevel fortsatt en viktig rolle i betalingssystemet. Kontanter er særlig viktig av beredskapshensyn, og for personer som ikke behersker eller ikke har mulighet til å bruke digitale løsninger. For at kontanter skal kunne fylle sine funksjoner, er det avgjørende at de er tilgjengelige og anvendelige.

Styrkingen av forbrukeres rett til å betale med kontanter, som trådte i kraft i 2024, og bankenes lovbestemte plikt til å sørge for et tilstrekkelig kontanttjenestetilbud til sine kunder, er viktige bidrag til å sikre dette. Samtidig er kontanttjenestetilbudet sårbart og har noen svakheter. Dersom bankene ikke sikrer tilfredsstillende løsninger, bør det utformes mer detaljert regulering av bankenes kontanttjenestetilbud.

Kontantandelen er lav, men mange bruker kontanter jevnlig

Bruken av kontanter gikk over lang tid ned og falt ytterlige under korona-pandemien. Siden 2020 har andelen av betalinger gjort med kontanter på fysisk utsalgssted og person til person vært stabil på rundt 3 prosent.

Figur B.1 Hvor ofte bruker du kontanter?



Kilde: Norges Bank

For å få et mer utfyllende bilde av bruken av og holdninger til kontanter gjennomførte Norges Bank i 4. kvartal 2025 en noe mer omfattende spørreundersøkelse rettet mot privatpersoner.[1]

Undersøkelsen viser at selv om flertallet av befolkningen sjelden eller aldri bruker kontanter, er det likevel en betydelig andel som bruker kontanter jevnlig. En av fire bruker kontanter månedlig eller oftere. Kontantbruk er vanligere blant personer med lavere utdanning eller lavere inntekt enn blant personer med høyere utdanning eller høyere inntekt.

I overkant av 90 prosent av kontantbrukerne har tilgang til nettbank, betalingskort og Vipps og bruker disse løsningene oftere enn de bruker kontanter. Tilgangen til disse betalingsmåtene er imidlertid jevnt over noe lavere (4–5 prosentpoeng) i gruppen kontantbrukere enn for befolkningen generelt.

Undersøkelsen viser at et stort flertall mener det er viktig å ha kontanter som alternativ hvis elektroniske betalingsmåter svikter. Et flertall er også helt eller ganske enig i at kontanter bidrar til økt forståelse av hva penger er, og at utsatte grupper vil få det vanskeligere uten kontanter. En fjerdedel av befolkningen mener vi ikke har behov for kontanter lenger.

36 prosent av befolkningen har kontanter tilgjengelig til løpende bruk, mens 42 prosent oppgir at de har satt av kontanter til beredskapsformål. Blant dem som har kontanter til løpende bruk, er den gjennomsnittlige beholdningen i underkant av 800 kroner, mens medianverdien er 500 kroner. For beredskapsbeholdninger er nivåene høyere. Blant dem som oppgir å ha dette, er gjennomsnittlig beholdning i overkant av 4 000 kroner, mens medianverdien er 2 000 kroner. Et stort flertall av

Figur B.2 Hvor enig er du i følgende påstander om betydningen av å ha kontanter tilgjengelig i samfunnet?
Prosent som har svart «helt enig og «ganske enig»

Kilde: Norges Bank

1 Se Norges Bank (2026e) for nærmere omtale. Undersøkelsen ser nærmere på befolkningen generelt, og på kontantbrukere. I undersøkelsen er en kontantbruker definert som en som bruker kontanter månedlig eller oftere.

innbyggerne, 79 prosent, mener det er viktig å ha mulighet til å ta ut og sette inn kontanter, uavhengig av egen bruk. Kun 5 prosent oppgir at dette ikke har betydning.

1000-kroneseddelen er fremdeles gyldig betalingsmiddel

Norges Bank har foretatt en ny vurdering av valørsammensetningen og besluttet at 1000-kroneseddelen forblir gyldig som betalingsmiddel og kan brukes som før. Samtidig er det besluttet å stanse bankenes mulighet til å bestille slike sedler fra Norges Bank. Antallet 1000-kronesedler i omløp vil dermed gradvis synke i årene som kommer.

Bakgrunnen for vurderingen er at det har skjedd store endringer i kontantbruken og i betalingssystemet siden forrige vurdering, som ble gjort i forbindelse med utgivelsen av dagens seddelserie. Finans-departementet ba også Norges Bank om å foreta en slik vurdering, med henvisning til at Økokrim har tatt til orde for å avvikle den høyeste valøren, og at bruken av kontanter har endret seg vesentlig i løpet av de siste årene.[2]

I vurderingen har Norges Bank lagt vekt på kontantenes rolle og funksjon både i normalsituasjoner og i beredskapssituasjoner, en effektiv og sikker kontanthåndtering, samt hensynet til å motvirke økonomisk kriminalitet. 1000-kroneseddelen utgjør i dag en liten andel av det totale antallet sedler i omløp. I normalsituasjoner har den derfor begrenset betydning for effektiviteten i kontantbetalinger. I alvorlige beredskapssituasjoner kan det imidlertid oppstå behov for å distribuere større kontantbeløp over lengre avstander, og for å gjennomføre flere og større betalinger med kontanter enn normalt. I slike situasjoner kan 1000-kroneseddelen være viktig. Ved behov kan Norges Bank åpne for tilførsel av 1000-kronesedler igjen.

Regelverksbegrensninger må være forholdsmessige

Kontanter har egenskaper som gjør dem egnet til bruk i enkelte former for kriminalitet, deriblant hvitvasking. Det er blant annet derfor innført bestemmelser i ulike regelverk som setter beløpsgrenser og andre rammer for bruk av kontanter. Norges Bank anerkjenner behovet for slike rammer. Samtidig er det viktig at slike tiltak er forholdsmessige. Regelverket og praktiseringen av dette må ikke svekke kontantenes rolle i beredskap og finansiell inkludering og publikums tillit til kontanter som et allment tilgjengelig og anvendelig betalingsmiddel.

I høringen om gjennomføring av EUs nye antihvitvaskingspakke i norsk rett foreslås det å senke og harmonisere beløpsgrensene for betalinger i kontanter i antihvitvaskingsloven (i dag 40 000 kroner), og for retten til å

2 Se brev fra Finansdepartementet til Norges Bank datert 15. januar 2026.

betale med kontanter i finansavtaleloven (i dag 20 000 kroner). Foreslåtte beløpsgrenser er 20 000 kroner, eventuelt 10 000 kroner.[3]

Norges Bank ser at en reduksjon av kontantgrensen i anti-hvitvaskingsregelverket fra 40 000 til 20 000 kroner kan være forsvarlig, gitt hensynene som ligger til grunn for bestemmelsen. Det vil da fremdeles være mulig å gjennomføre de fleste kjøp som gjøres som en del av dagliglivet med kontanter, også av varer som kjøpes sjeldnere, men som det er behov for i dagens samfunn. Norges Bank ser også at det kan foreligge avveininger som tilsier at beløpsgrensen for retten til å betale med kontanter etter finansavtaleloven kan settes noe lavere enn dette igjen, for eksempel 10 000 eller 15 000 kroner. Forbrukerne vil da fortsatt ha en rett til å betale med kontanter for de fleste nødvendige innkjøp i det daglige. Sammen med en beløpsgrense i hvitvaskingsloven på 20 000 kroner kan dette gi nødvendig fleksibilitet til at hensynet til finansiell inkludering og beredskap kan ivaretas.

Norges Bank påpeker samtidig at en beløpsgrense på 20 000 kroner eller lavere innebærer en betydelig innskrenkning i partenes avtalefrihet, og muligheten for forbrukere og forhandlere av varer og tjenester til å benytte kontanter som oppgjørsmiddel. Norges Bank er kritisk til om en harmonisert grense på 10 000 kroner vil være i tråd med proporsjonalitetskravet og mener en beløpsgrense så lavt som 5 000 kroner ikke er forsvarlig.

En reduksjon i beløpsgrenser for kontantbetalinger innebærer ikke i seg selv en reduksjon i hva som kan anses som et tilfredsstillende kontanttjenestetilbud.

Bankene har ansvar for et tilstrekkelig kontanttjenestetilbud

Finansforetaksloven § 16-4 slår fast at «banker skal, i samsvar med kundenes forventninger og behov, motta kontanter fra kundene og gjøre innskudd tilgjengelig for kundene i form av kontanter». Plikten innebærer at privatpersoner skal ha tilstrekkelig mulighet til å kunne ta ut og sette inn kontanter, og at næringsdrivende skal kunne få tak i veksel og sette inn kontantomsetning. Dette forutsetter både tilstrekkelig geografisk dekning og annen nødvendig funksjonalitet. Bankene kan oppfylle plikten i egen regi eller gjennom avtaler med andre tilbydere av kontanttjenester.

Norges Bank har tidligere påpekt at dagens kontanttjenestetilbud er sårbart og har noen svakheter. Store deler av kontanthåndteringen og kontanttjenestetilbudet utføres og tilbys i dag av aktører som ikke har lovpålagte plikter til å gjøre det. Det har over tid blitt stadig færre bankfilialer som tilbyr kontanttjenester over skranke, og stadig færre minibanker. Kontanttjenester i butikk (KiB), en tjeneste for uttak og innskudd av kontanter som er tilgjengelig i om lag 1450 av Norgesgruppens butikker, har blitt en vesentlig del av bankenes kontanttilbud.

3 Høring – arbeidsgrupperapport om EUs antihvitvaskingspakke – regjeringen.no

Løsningen gir i hovedsak et tilfredsstillende tilbud til de fleste forbrukere, men er bare tilgjengelig for personer som har BankAxept-kort. Den dekker heller ikke næringslivets behov for veksel og større kontantinnskudd.

Bankenes kontantplikt gjelder også i situasjoner med økt etterspørsel etter kontanter som følge av svikt i tilgangen til de elektroniske betalingssystemene. I beredskapssammenheng er det en svakhet at KiB ikke fungerer når BankAxept-reserveløsningen[4] er i bruk. Det innebærer at en stor del av bankenes kontantforsyning skrus av når butikkterminaler er offline, og dermed at publikums mulighet til å ta ut kontanter blir vesentlig redusert.

Dagens generelle regelverk kan gjøre det vanskelig å fastslå hva som utgjør et tilstrekkelig kontanttjenestetilbud. Det er likevel å foretrekke at bankene i fellesskap, uten en mer detaljert regulering, sørger for tilfredsstillende dekning av kontanttjenester over hele landet. Norges Bank understreker samtidig at bankenes ansvar ikke er betinget av et velfungerende leverandørmarked. Dersom bankene ikke sikrer tilfredsstillende løsninger, bør det utformes mer detaljert regulering av bankenes kontanttjenestetilbud. Forrige kartlegging av kontanttjenestetilbudet i Norge ble gjort i 2020/2021. Det er nå behov for en ny kartlegging.

4 En elektronisk reserveløsning som trer i kraft blant annet når kommunikasjonen faller ut på brukersteder.

Tokenisering og digitale sentralbankpenger

Norges Bank utreder om innføring av digitale sentralbankpenger er nødvendig for at det også i fremtiden skal være sikkert, effektivt og attraktivt å betale med norske kroner. Mot slutten av 2025 konkluderte Norges Bank med at det nå ikke er grunnlag for å innføre slike penger i Norge. Behovet kan imidlertid endre seg, og utredningen fortsetter slik at Norges Bank kan være klar til å kunne innføre digitale sentralbankpenger dersom det blir nødvendig for å sikre et effektivt og sikkert betalingssystem. For eksempel kan det bli behov for å legge til rette for oppgjør i sentralbankpenger for transaksjoner mellom bankene i tokeniserte verdier. Bruken av tokenisering har kommet relativt kort i Norge sammenliknet med enkelte andre land. Utviklingen kan gå raskt om den først starter. Norske banker bør følge aktivt med på teknologiutviklingen. Norges Bank vil utvide samarbeidet med aktører i finansnæringen om utforskning av gevinster og utfordringer ved teknologien og vil blant annet involvere bankene i teknisk testing av tokenisering og digitale sentralbankpenger.

Digitale sentralbankpenger

Digitale sentralbankpenger (DSP) er elektroniske penger utstedt av sentralbanken i den offisielle pengeenheten. DSP kan ha to hovedformer: kunderettede DSP og DSP for oppgjør. Kunderettede DSP vil være allment tilgjengelige for publikum på linje med kontanter og bankinnskudd. De skal kunne benyttes til betalinger på kundenivå, for eksempel på utsalgssteder, mellom privatpersoner og ved netthandel.

DSP for oppgjør er tokeniserte sentralbankreserver og vil kun være tilgjengelige for banker og andre foretak i finansiell sektor med konto i sentralbanken. Denne typen DSP vil kunne benyttes til oppgjør mellom banker mv. på tilsvarende måte som reservene i dagens interbanksystem, men i en annen teknologisk form. Denne typen DSP kan være nødvendig for å sikre at oppgjør av transaksjoner med for eksempel tokeniserte bankinnskudd, eller oppgjør knyttet til handler med tokeniserte verdipapirer, gjennomføres effektivt og uten uønsket risiko. Tokenisering drøftes nærmere under.

Norges Bank går ikke inn for DSP nå

Norges Bank utreder om innføring av DSP er nødvendig for at det også i fremtiden skal være sikkert, effektivt og attraktivt å betale med norske kroner.

Det norske betalingssystemet er i dag både effektivt og sikkert. Driften er stabil og betalinger kan gjennomføres raskt, til lave samfunnsøkonomiske kostnader og på måter som er tilpasset brukernes behov. Beredskapen i betalingssystemet er god, og det arbeides med tiltak for å styrke den ytterligere. Anvendelsen av tokeniseringsteknologien har kommet kort i norsk finans.

Dette er bakgrunnen for at Norges Bank mot slutten av 2025 konkluderte at det ikke er grunnlag for å innføre noen form for DSP i Norge nå.[1] Behovet for DSP i Norge kan imidlertid endre seg. Den teknologiske utviklingen i finanssystemet skjer raskt, og nye tjenester og aktører kommer til. I fremtiden kan behovet for slike penger endre seg. Derfor skal Norges Bank være klar til å kunne innføre DSP senere, dersom det blir nødvendig for et effektivt og sikkert betalingssystem. Norges Bank fortsetter derfor utredningen om DSP og tokenisering.

Kunderettede DSP er lite utbredt

Kun noen få sentralbanker har utstedt DSP. Sentralbankene i Nigeria, på Jamaica og Bahamas har utstedt kunderettede DSP, blant annet med formål om finansiell inkludering og reduksjon av kostnadene ved kontant-distribusjon. Bruken er så langt relativt begrenset. Den kinesiske sentral-banken har utstedt DSP i en pilot med mange brukere. Bruken skal ha tatt seg opp etter at renteavkastning på publikums beholdning av DSP ble innført. Sentralbanker i mange land vi sammenligner oss med har, som Norges Bank, foreløpig konkludert med at det ikke er grunnlag for å utstede kunderettede DSP.

Den europeiske sentralbanken (ECB) er trolig den sentralbanken i utviklede økonomier som har kommet lengst i sin utredning av kunde-rettede DSP – en digital euro. Ett av argumentene for innføring av digital euro er at europeerne vil få tilgang til et betalingssystem som ikke er avhengig av betalingstjenestetilbydere hjemmehørende utenfor Europa. Dermed vil det styrke Europas strategiske autonomi i en tid med økt geopolitisk usikkerhet.[2] En innføring av digital euro er avhengig av at det gjøres endringer i lovgivningen i EU. ECB vil ta stilling til om en digital euro skal innføres etter at lovgrunnlaget er etablert. ECB oppgir at dersom nødvendig regulering vedtas i EU i år, kan digital euro bli innført i 2029.

ECB/eurosystemet har også utredet og testet oppgjørsløsninger i sentralbankpenger for transaksjoner og handel i tokeniserte verdier. I den sammenheng har ECB publisert en plan der første etappe er å

1 Se Norges Bank (2025b) og Norges Bank (2026a).
2 Se for eksempel Cipollone (2026) og Norges Bank (2026b) for en oversikt over digital euro-prosjektet.

tilpasse det ordinære oppgjørssystemet for euro (T2) slik at transaksjoner i tokeniserte verdier kan gjøres opp i sentralbankpenger der. En slik mulighet skal etter planen være tilgjengelig ved slutten av tredje kvartal 2026.

På lengre sikt utreder ECB gevinstene og utfordringene ved å etablere en egen blokkjedebasert plattform for oppgjør i sentralbankpenger av tokeniserte transaksjoner. Det er mer usikkert om og eventuelt når en slik løsning vil innføres.

Tokenisering – egenskaper og bruksområder

Tokenisering innebærer at en eiendel representeres som en digital enhet – et token – i et register basert på blokkjedeteknologi.[3] Token og blokkjeder er mest kjent fra kryptovalutaer, men teknologien kan også brukes til å registrere og overføre eierskap til andre eiendeler som verdipapirer, bankinnskudd, eiendom og sentralbankpenger. Før dette kan skje, må eiendelene «tokeniseres» og registreres på en blokkjede, slik at transaksjoner kan gjennomføres digitalt og sporbart. Et token kan være et digitalt speilbilde av en eksisterende eiendel eller utstedes som en ny eiendel på en blokkjede.

Omfanget av tokenisering i det tradisjonelle betalings- og finanssystemet er fortsatt svært begrenset. Blokkjedeteknologi har så langt i hovedsak vært anvendt utenfor tradisjonell finans. Teknologien er særlig benyttet som grunnlag for kryptovalutaer, der noe av hensikten har vært å etablere et økosystem eller infrastruktur som er uavhengig av tillit til en sentral aktør – som en bank, en sentralbank eller et annet selskap eller myndighetsorgan. I noen tilfeller kan motivasjonen være at slike overføringer i mindre grad er gjenstand for regulering, kontroll og innsyn fra offentlige myndighetsorganer. Slike motiver ligger selvsagt ikke til grunn dersom en sentralbank deltar i etableringen av tokeniserte finansielle infrastrukturer.

En av de viktigste fordelene med tokeniserte eiendeler og blokkjedeteknologien er muligheten til programmerbarhet ved bruk av «smarte kontrakter». Smarte kontrakter er dataprogrammer som automatisk utfører transaksjoner når forhåndsdefinerte betingelser er oppfylt. Automatisering kan redusere behovet for mellomledd og effektivisere prosesser som verdipapir- og valutahandel.

Smarte kontrakter kan også legge til rette for «atomiske oppgjør», hvor en transaksjon kun gjennomføres hvis og bare hvis begge/alle parter oppfyller sine forpliktelser, og der eiendomsoverføringen av alle elementer i transaksjonen skjer umiddelbart. Dette kan være en robust og effektiv måte å oppnå levering-mot-betaling og betaling-mot-betaling. Slike egenskaper fjerner motparts- og oppgjørsrisiko ved oppgjør av handel med blant annet valuta og verdipapirer.

3 Se Cipollone (2026). En blokkjede er et register eller datasystem som er designet for å drives på en desentralisert måte. Enhetene i registeret disponeres gjennom kryptografiske koder.

Programmerbarheten og andre egenskaper ved blokkjedeteknologien kan innebære at de har et fortrinn på enkelte nye betalingsområder. Flere stablecoinstilbydere har en ambisjon om få en større rolle i tradisjonelle betalinger og tradisjonell finans. Se nærmere omtale av dette i artikkelen «Kan stablecoins svinge seg frem til allmenn bruk?» Samtidig har aktører innen tradisjonell finans startet testing av handel med tokeniserte verdipapirer der stablecoins inngår som oppgjørsmiddel. Sentralbanker legger vekt på at oppgjørsmiddelet ved slik handel er sentralbankpenger, fordi alternativer som stablecoins og andre private oppgjørsmidler kan innebære en viss risiko.

Tokenisering kan gi nye muligheter

Hvilke fordeler kan bruk av tokenisering og blokkjedeteknologi i betalings- og finanssystemet gi? Er det egenskaper ved teknologien som gjør at disse fordelene ikke kan realiseres gjennom forbedringer av dagens betalingsløsninger og dagens teknologi?

Mange sentralbanker, foretak og internasjonale organisasjoner gjennomfører tester og analyser for å svare på disse spørsmålene. Noen sentralbanker foretar utprøving av forretningsmodeller i pilottester med blant annet reelle verdipapirer og penger. Mye av testingen tar utgangspunkt i utformingen av eksisterende betalingsfunksjoner og -tjenester, for eksempel i forbindelse med grensekryssende betalinger og oppgjør for verdipapirhandel. Likevel kan det like godt være at de virkelig store gevinstene kommer av at teknologien gir helt nye og mer effektive måter å gjennomføre de grunnleggende tjenestene på, og som medfører flere tilleggsgevinster som vi ikke nå har oversikt over.

Omlegging av teknologi kan være omfattende, og vil være mer krevende jo flere institusjoner og funksjoner som må endres for å realisere gevinstene ved teknologien. Det taler for at en omfattende omlegging til tokenisering først kan forsvares dersom nye og langt mer effektive betalingstjenester kan utvikles. Mindre forbedringer av eksisterende tjenester vil derimot ikke være tilstrekkelig til å forsvare omfattende omlegginger. De største gevinstene ved teknologien vil sannsynligvis først kunne verifiseres når teknologien modnes og utviklingen har kommet vesentlig lenger. Slike gevinster kan komme dersom betalings-funksjoner knyttes til andre funksjoner, slik at den totale brukeropp-levelsen og --nytten blir bedre og antallet parter og systemer involvert i en transaksjon kan reduseres.

Videre utredning om tokenisering og DSP

Norges Bank vil fortsette å utrede tokenisering og DSP for å være klar til å kunne innføre DSP dersom det blir nødvendig senere. Derfor vil vi blant annet følge med på det som skjer internasjonalt på området og utviklingen innen tokenisering i norsk finans. For å realisere potensielle gevinster av tokenisering kreves en omlegging av flere elementer i det finansielle økosystemet, noe som berører mange interessenter.

Potensielle gevinster og kostnader ved tokenisering vil i stor grad komme utenfor sentralbanken og som en følge av et samordnet teknologiskifte hos flere aktører. Følgelig har det lite for seg om sentralbanken er den eneste aktøren i den finansielle infrastrukturen som innfører løsninger knyttet til tokenisering. Derfor vil vi i det videre arbeidet legge enda mer vekt på involvering og samarbeid med banker og andre aktører i betalingssystemet. Vi kommer til å fortsette med teknisk og funksjonell testing av ulike testcases i våre teknologiske sandkasser, og håper å få flere banker og finansaktører med på denne testingen.[4]

Den norske finansnæringen har lang og god tradisjon for være tidlig ute i utviklingen av effektive betalingstjenester og implementering av ny teknologi i den finansielle infrastrukturen. Gevinstene har kommet som et resultat av samhandling om felles infrastruktur, som ligger til rette for konkurranse på tjenestenivå. En slik samordning kan også være en forutsetning for å få realisert gevinstene ved tokenisering.

At omfanget av tokenisering er begrenset så langt, kan blant annet skyldes at risikobildet er uklart. Tilgang til et oppgjørsmiddel markedet har tillit til – slik som sentralbankens reserver – vil kunne være en viktig faktor i utbredelsen av tokenisering og smartkontrakter i det finansielle systemet. Samtidig kan det være risiko for eksempel knyttet til teknologien som er grunnlaget for eierskap registrert i blokkjeder. Videre er det fremdeles uavklarte juridiske spørsmål knyttet til om eierskap til token i blokkjeden også gir uomtvistelig eierskap til eiendelen. Slike juridiske uklarheter må løses for at transaksjoner som involverer tokeniserte eiendeler skal kunne få vesentlig utbredelse i den regulerte delen av finanssystemet. Internasjonale standarder på området kan komme som følge av markedsutvikling og/eller regulering.

Norges Bank har for tiden formelle diskusjoner med ECB om deltakelse i eurosystemets oppgjørssystem T2. Eurosystemets eventuelle løsninger for DSP og andre måter å gjøre opp i sentralbankpenger på kan være aktuelle på et senere tidspunkt, dersom Norges Bank inngår avtale om å benytte T2.

4 Norges Banks testing av tekniske løsninger så langt er blant annet drøftet i Norges Bank (2026c) og Norges Bank (2023).

Kan stablecoins svinge seg frem til allmenn bruk?

Bruken av stablecoins er i all hovedsak knyttet til investeringer i kryptoeiendeler, men noen andre bruksområder er gryende. Stablecoins har fått mye oppmerksomhet for mulige gevinster de kan bidra med i betalingssystemet og risikoer de kan føre med seg. Flere land har innført reguleringer. I Norge gjelder det europeiske regelverket gjennom kryptoeiendelsloven. Reguleringene motvirker mange av risikoene knyttet til stablecoins, men er utilstrekkelige for at stablecoins skal kunne bli stabile allmenne betalingsmidler.

Stablecoins brukes i hovedsak til krypto-handel, men nye bruksområder prøves ut

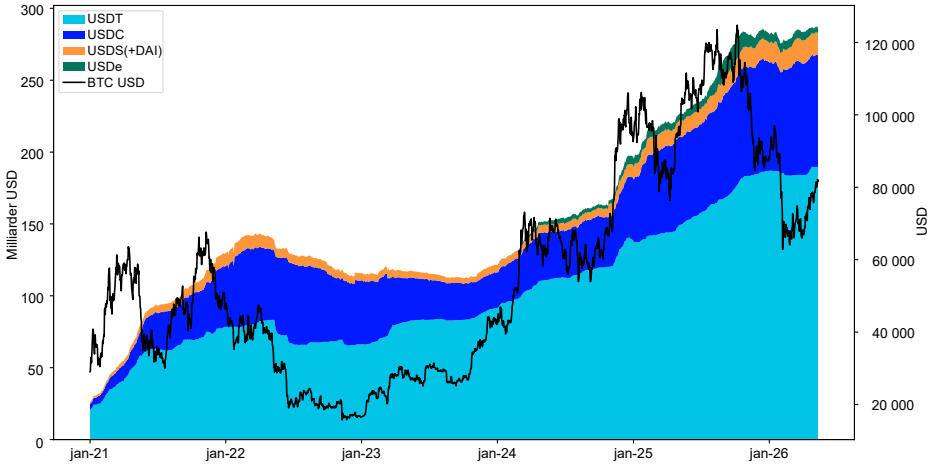
Stablecoins er kryptoeiendeler som er designet for å holde stabil verdi mot en referanse. De fleste bruker amerikanske dollar som referanse, og slike utgjør 99 prosent av total markedsverdi på rundt 300 milliarder dollar. Trump-administrasjonen i USA har fremhevet stablecoins som et virkemiddel for å bevare og styrke dollarens internasjonale rolle og sikre etterspørsel etter amerikanske statspapirer. Markedet for euro-denominerte stablecoins utgjør omkring 0,5 milliarder euro.

Bruksområdene for stablecoins har i hovedsak vært knyttet til spekulasjon i kryptoeiendeler. Stablecoins brukes både som oppgjørsmiddel og verdioppbevaring, herunder plassering i ulike rentebærende tjenester. Historisk har samlet verdi av stablecoins svingt i takt med markedet for kryptoeiendeler, se figur C.1. I senere tid har stablecoinsmarkedet fortsatt å vokse selv om verdien på bitcoin og mange andre kryptoeiendeler har falt, noe som indikerer nye bruksområder. Mange aktører har spådd en betydelig vekst for stablecoins fremover, også på nye bruksområder.[1]

Det er imidlertid ikke trivielt å anslå hva de nye bruksområdene er og hvor mye de utgjør i verdi. McKinsey og Artemis Analytics (2026) peker på at transaksjonsvolumene for stablecoins på blokkjedene utgjør over 35 billioner amerikanske dollar årlig, men at mesteparten av dette er urelatert til vanlige betalinger og pengeoverføringer. Analysen finner at slike betalinger bare utgjør omkring 390 milliarder dollar, og at dette utgjør omkring 0,02 prosent av tradisjonelle betalinger globalt. Av

1 IMF (2025) s. 27.

Figur C.1 Markedsverdien av de største stablecoinene (venstre akse) og bitcoinpris (høyre akse)



Kilde: Coingecko

betalinger i stablecoins er den største andelen mellom privatpersoner, inkludert grensekryssende betalinger. Noen andre typer betalinger, som betalinger mellom bedrifter, har en lavere andel, men vokser mer.

En barriere mot allmenn bruk er at stablecoins er utstedt av aktører som ikke er bredt kjent blant publikum og at de ikke er tilgjengelige gjennom brukergrensesnitt kundene bruker til vanlige betalinger. Dette kan være i ferd med å endre seg. Nye reguleringer som stiller krav til utstedere og gir brukerne rettigheter kan generelt øke tilliten til stablecoins. Tilliten vil antakeligvis bli enda sterkere dersom de utgis eller formidles av aktører brukerne har tillit til fra før. Høsten 2025 ble det kjent at ni europeiske banker har planer om å sammen utgi en stablecoin denominert i euro, og siden har flere banker sluttet seg til. Det ble også kjent at betalingsselskapet Klarna planlegger å utstede en stablecoin.

Stablecoins har en ubetydelig rolle i det norske betalingssystemet. Norges Bank har gjennomført undersøkelser om kjennskap til og bruk av kryptoeiendeler i 2024 og 2026.[2] Begge undersøkelsene viser lav kjennskap til og bruk av stablecoins. Undersøkelsen fra 2026 viser at 19 prosent av befolkningen[3] har hørt om stablecoins og av disse hadde 72 prosent aldri brukt stablecoins. De tre hovedgrunnene som oppgis for å kjøpe stablecoins, er til bruk ved handel med annen kryptovaluta (55 prosent), til verdioppbevaring (30 prosent) og for å lære mer om og/eller teste teknologien (22 prosent).

2 Norges Bank (2024) og Norges Bank (2026d). Undersøkelsene omfatter individer og ikke foretak.
3 16 år eller eldre.

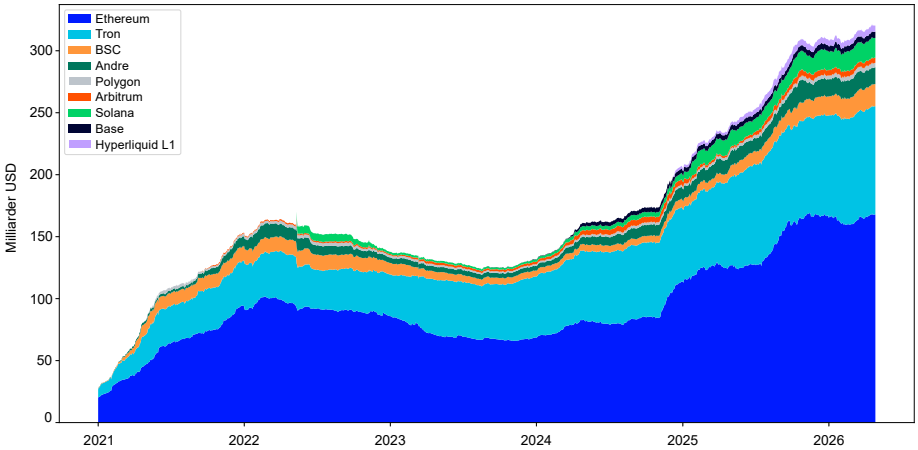
Åpne blokkjeder gjør stablecoins tilgjengelige, men medfører også noen utfordringer

Stablecoins bruker åpne blokkjeder som grunnleggende transaksjonsinfrastruktur. Et fortrinn med dette er at de i likhet med andre kryptoeiendeler kan overføres hele døgnet alle ukedager uten avhengighet av sentrale mellomledd. De største stablecoinverdiene benytter Ethereum-blokkjeden som transaksjonsinfrastruktur, men andre blokkjeder har også en vesentlig andel av verdiene. I tillegg finnes det såkalte tolagsløsninger som ligger på toppen av andre blokkjeder og som samler transaksjoner, slik at det blir mindre trengsel på selve blokkjeden, se figur C.2.

En utfordring knyttet til bruk av åpne blokkjeder for stablecointransaksjoner er at transaksjonsgebyrene må betales i den kryptoeiendelen som er tilknyttet den aktuelle blokkjeden. Hvis Ethereum brukes som transaksjonsinfrastruktur, må gebyrene betales i kryptoeiendelen Ether. Disse gebyrene bidrar til å belønne de som deltar i konsensusmekanismen for å oppdatere blokkjeden. Dette innebærer at brukerne må holde disse kryptoeiendelene for å gjennomføre transaksjoner, og at kostnadene kan bli uforutsigbare og høye, særlig hvis blokkjeden opererer nær kapasitetsgrensen. Dette har imidlertid blitt et mindre problem med nye skaleringsløsninger. Enkelte stablecoinutstedere, slik som Circle, utvikler egne blokkjeder der gebyrene kan betales i stablecoins. Dette reduserer avhengigheten av frittflytende kryptoeiendeler for å gjennomføre transaksjoner, men kan også forsterke monopoltendenser ved å øke nettverksfordelene knyttet til enkelte stablecoins.

Stablecoins fungerer som ihendehaverinstrumenter knyttet til kryptografiske koder og kan overføres til enhver uten at de behøver å ha et kundeforhold til stablecoinutstederen på forhånd. Dette øker tilgjengeligheten sammenliknet med andre elektroniske penger, men det er også noen ulemper. Hvis de kryptografiske kodene mistes eller

Figur C.2 Markedsverdi av stablecoins fordelt på ulike blokkjeder



Kilde: DeFiLama

tilgjengeliggjøres for andre gjennom cyberkriminalitet, kan pengene være tapt. BIS (2025a) peker på at stablecoins mangler den nødvendige kunde- og transaksjonskontrollen som gir det tradisjonelle betalingssystemet integritet.

Det utvikles en rekke tjenester som kan bidra til at stablecoins blir lettere å bruke. Tredjeparter kan skjerme brukerne fra den underliggende teknologien slik at kunden slipper å forholde seg til blokkjedene. For eksempel tilbyr ulike betalingsapplikasjoner betaling med stablecoins der stablecoins fremgår på brukerens konto og kan brukes på samme måte som e-penger eller bankpenger. I disse tilfellene vil ofte betalingsapplikasjonene forvalte de kryptografiske kodene. Ofte vil betalinger mellom kundene kun gjennomføres som betalinger mellom kontoer i betalingsaktørenes interne regnskapssystem, uten at det gjøres endringer på blokkjeden. Endringer på blokkjeden vil kun skje dersom kunden ønsker å ta ut stablecoinene fra det interne regnskapssystemet. Selv om dette kan være en forenkling for brukerne, vil brukerne få en motpartsrisiko mot disse aktørene.

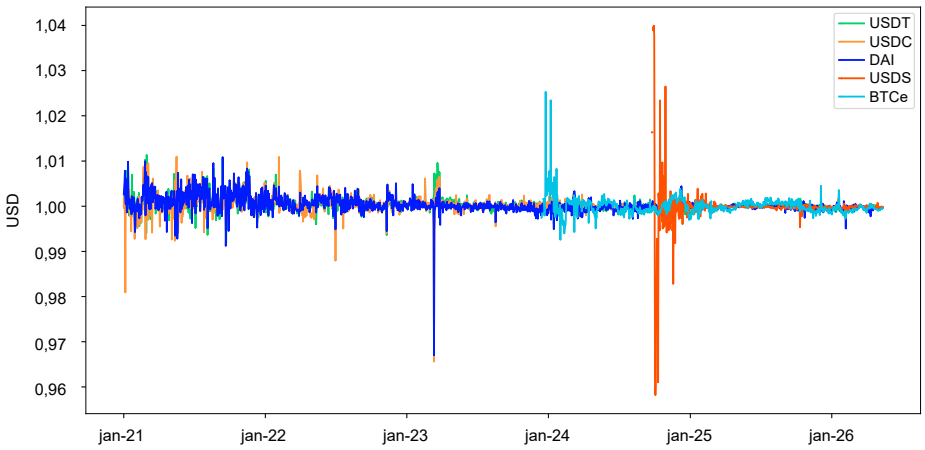
Det finnes også aktører som utvikler underliggende betalingsløyper basert på stablecoins uten at brukere behøver å forholde seg til dette. For eksempel kan en betaler og betalingsmottaker gjennomføre en internasjonal transaksjon der betaler overfører fra sin bankkonto og mottaker får beløpet på sin bankkonto med et underliggende oppgjør i stablecoins. De store kortselskapene utvikler også betalingsløsninger der stablecoins benyttes som underliggende betalingsinfrastruktur.

Å bruke åpne blokkjeder som finansielle infrastrukturer reiser en rekke utfordringer. Blant annet vil desentraliseringen kunne reise utfordringer knyttet til den styringen og kontrollen som kreves for finansielle infrastrukturer. Det vil kunne kreve andre typer reguleringer og at forpliktelser må legges på tjenestetilbyderne og brukerne. I den tradisjonelle finansielle infrastrukturen er det klare reguleringer om risikofordeling og ansvar for etterlevelse. Dette regelverket er ikke direkte anvendelig når åpne blokkjeder brukes som transaksjonsinfrastruktur. Dersom stablecoins blir mer utbredt, er det behov for videre regelverksutvikling for betalinger med stablecoins.

Reguleringer kan ikke enkelt gjøre stablecoins stabile

BIS (2025a) peker på at ustabilitet og uelastisk pengetilbud hindrer stablecoins i å kunne fungere som et allment pengealternativ. Stabil og enhetlig verdi på ulike penger i samme valuta er en helt sentral egenskap ved penger, ved at brukerne slipper å bruke ressurser på verdsetting av pengene i seg selv og at ulike mottakere kan sette lik verdi på betalingsmiddelet. Brukerne vil kanskje akseptere mindre verdisvingninger for enkelte transaksjoner med lav verdi, dersom bruken gir andre besvarelser og gevinster. Men verdisvingninger vil være problematiske

Figur C.3 Svingninger i verdien på stablecoins som skal være stabile mot USD



Kilde: Coingecko

for et allment brukt betalingsmiddel som også brukes til større betalinger. Figur C.3 viser at selv de største stablecoinene i markedet har vært utsatt for verdisvingninger, noe som innebærer både usikker verdi på den enkelte stablecoin og at de har forskjellig verdi mot hverandre.

Verdisvingninger, og særlig verdifall, kan skyldes tap av tillit til at stablecoinutstederen har tilstrekkelige reserver. Et eksempel er verdifallet på USDC da Silicon Valley Bank kollapset i mars 2023, som følge av at Circle hadde deler av sine reserver i denne banken. Dersom brukerne mister tilliten til at en stablecoin holder verdien, vil det kunne føre til massesalg som vil føre prisen ytterligere ned. Det ville også kunne føre til hasteinnløsninger som fører til verdifall på eiendeler som sikrer verdien av stablecoinen. Et slikt verdifall kan smitte til andre deler av finansiell sektor og true finansiell stabilitet. Stablecoins er i dag antakeligvis for små i økonomisk omfang og tradisjonelle finansinstitusjoner er i dag for lite eksponert til at slike verdifall kan true finansiell stabilitet. Det kan endre seg.

Tillit til verdien kan styrkes gjennom reguleringer. Kvalitetskrav til verdipapirer som skal sikre en stablecoin, vil styrke tilliten. Krav til sikring er sentralt i det europeiske regelverket for kryptoeiendelsmarkeder – MiCAR – som også gjelder som norsk lov fra 1. juli 2025 etter kryptoeiendelsloven. Krav til sikring er også sentralt i det nye stablecoinregelverket i USA – GENIUS Act.

Om stablecoins blir store nok, kan det imidlertid være utfordrende å sikre tilliten med selv de mest sikre verdipapirene i reservene. I litteraturen er det dokumentert at stablecoinutstedere allerede i dag holder en så stor andel av amerikansk kortsiktig statsgjeld at utstedelse og innløsning kan påvirke prisen og dermed renten på disse verdipapirene.[4] Bank of

4 Ahmed og Aldasoro (2026).

England har foreslått[5] at systemviktige stablecoins med britiske pund som referanse delvis skal sikres med konto i sentralbanken og gis tilgang til sentralbankens lånefasiliteter for å sikre tilliten til stablecoins. Vi er ikke kjent med at andre sentralbanker har foreslått tilsvarende.

Verdisvingninger kan også skyldes ubalanser i tilbud og etterspørsel. Stablecoins kan ikke fleksibelt utstedes ved å gi lån på forespørsel slik bankpenger kan, og de er ikke interoperable med hverandre i form av oppgjør i sentralbankpenger slik bankpenger er. Hver stablecoin som utstedes må være sikret på forhånd og det kan ofte ta tid å innløse stablecoins mot bankpenger. Mens stablecoins brukes og omsettes 24/7, vil markedene for de verdipapirene som inngår i reservene være påvirket av begrensede åpningstider. Det vil også kunne gå noe tid til oppgjør.

Det er dermed ikke friksjonsfritt å utstede nye stablecoins og ta eksisterende ut av sirkulasjon. Dersom det for eksempel er overskudds-etterspørsel etter en stablecoin, vil prisen kunne overstige par verdi. Siden hver enkelt stablecoin er et «lukket system» for hver enkelt utsteder med eget tilbud og etterspørsel, vil stablecoins variere i verdi mot hverandre. Verdisvingninger som følge av misforhold mellom tilbud og etterspørsel kan forsterkes av at en utsteder ofte har utstedt en stablecoin på forskjellige blokkjeder med forskjellig likviditet. Det kan medføre at en stablecoin ikke bare svinger i verdi, men kan omsettes til forskjellig verdi på ulike blokkjeder.

Krav som settes til forhåndssikring kan øke friksjoner for utstedelse og destruksjon. Dette innebærer at krav som settes for å unngå verdifall som følge av tillitssvikt, kan øke verdisvingninger som følge av ubalanse i tilbud og etterspørsel.

Tokeniserte bankpenger lener seg på et omfattende regulatorisk og institusjonelt rammeverk og kan være et mer stabilt tokenisert penge-alternativ enn stablecoins. Betalinger med tokeniserte bankpenger bør gjøres opp i sentralbankpenger. Utviklingen i tokenisering av penger og andre eiendeler og oppgjør i sentralbankpenger er nærmere beskrevet i «Tokenisering og digitale sentralbankpenger».

5 Bank of England (2025).

Trusselen fra kvante-datamaskiner og tiltak i finanssystemet

Kvantedatamaskiner representerer en trussel mot sikkerheten i dagens IT-systemer. For å møte denne utfordringen arbeides det globalt og nasjonalt med å innføre kvantesikker kryptografi. Organisasjoner i og utenfor finanssystemet bør prioritere nødvendige tiltak for å opprettholde sikkerheten i sine IT-systemer.

Hvorfor truer kvantedatamaskiner IT-sikkerheten?

Kvantedatamaskiner bygger på andre fysiske prinsipper og kan i noen tilfeller foreta beregninger på andre og mer effektive måter enn det som er tilfelle for klassiske datamaskiner. De kan ha mange anvendelser som er til nytte, men byr også på sikkerhetsutfordringer.

De fleste nettverk i det finansielle systemet er helt avhengige av krypto-grafi for å sikre konfidensialitet, integritet og autentisitet. Grunnleggende sikkerhetsprotokoller bygger på kryptografiske algoritmer som har vært ansett som sikre i flere tiår. Sikkerhetsfundamentet i dem trues av utviklingen av kvantedatamaskiner i viktige tilfeller.[1] Utviklingen av disse maskinene har kommet langt nok til at angrep som benytter dem i økende grad betraktes som sannsynlige.

Konsekvensene kan bli store. Sikkerhetsmyndigheter i Norge og andre land[2] har derfor gitt råd og i noen tilfeller stilt krav om at problemet skal håndteres før det blir kritisk. Noen legger til grunn en overgang til kvantesikre algoritmer innen 2035, mens andre tar sikte på en raskere innfasing.

Løsninger finnes og flere er på vei

Kvantesikker kryptografi (post-quantum cryptography – PQC) er kryptografiske algoritmer som er konstruert for å være sikre mot angrep ved bruk av kvantedatamaskiner i tillegg til klassiske datamaskiner.[3]

1 Faktorisering av heltall og diskret logaritme ved Shors algoritme.
2 Blant andre NSM, ENISA, NIST, BSI, ANSSI og NCSC.
3 Se NIST CSRC PQC (2024).

De krever ingen form for kvanteteknologisk utvikling og de er ment å fungere i infrastrukturen man har på plass fra før.

Det er verdt å legge til at det ikke er alle former for kryptografi som kan knekkes ved hjelp av kvantedatamaskiner.[4] Trusselen fra slike maskiner er særlig knyttet til to komponenter av kryptografiske protokoller:

- Nøkkelutveksling som brukes for å etablere en felles hemmelig nøkkel mellom parter (eksempelvis mellom klient og server).
- Digitale signaturer som brukes til å autentisere parter som samhandler.

I begge tilfeller foreligger det nye kvantesikre alternativer[5] til eldre kryptografiske algoritmer. Disse vil dekke mange brukssituasjoner.

Det kan imidlertid komme flere alternativer[6] og det må derfor avklares hvilke løsninger som er hensiktsmessige i ulike bruksscenario. Den generelle anbefalingen er uansett å bruke standardiserte algoritmer.

Noen utfordringer

Finanssystemet er stort og sammensatt og det er sannsynlig at det finnes undersystemer som ikke er fleksible nok til å bruke de nye byggesteinene direkte. Siden anbefalinger om å planlegge innførselen av kvantesikre algoritmer allerede foreligger, blir det viktig å sikre at fremtidige systemer kan ta dem i bruk.

Overgangen kan ta tid hvis det er systemtekniske forhold som gjør det vanskelig. Eksempelvis er kvantesikre signaturer betydelig større enn dagens signaturer. Resultatet kan være høyere ressursbruk generelt. Dette vil håndteres over tid, men kan være en utfordring der hvor standardformater[7] eller maskinvare[8] må oppgraderes. Produkter som skal håndtere nye standarder må i noen tilfeller også sertifiseres, og dette kan forlenge bytteprosessen ytterligere.

Hvem har ansvaret for kvantesikkerhet?

Det er den enkelte virksomhet som har ansvaret for å sikre egne systemer. I finanssystemet vil dette blant annet gjelde banker, andre finansforetak og eiere av systemer innenfor finansiell infrastruktur. Dette ansvaret gjelder alle former for IT-sikkerhet, herunder kvantesikkerhet.

Cyberangrep som rammer kritiske funksjoner eller gir omfattende tillitssvikt, kan true finansiell stabilitet. Det motiverer tiltak fra bransjeorganisasjoner og myndigheter.

4 Symmetrisk kryptografi som blokkchiffer eller kryptografiske hash-funksjoner treffes eksempelvis ikke på faretruende vis.

5 Se NIST CSRC PQC (2024).

6 NIST, ISO og andre organer kan ende opp med alternative algoritmer.

7 ISO 8583 er ett eksempel.

8 Det kan for eksempel dreie seg om chipper i betalingskort eller HSM (Hardware Security Module – hardware som implementerer kryptografi) som er tilpasset eldre algoritmer.

Finans Norge har utarbeidet et veikart for arbeidet med kvanterisiko i norsk finansnæring.[9] Veikartet skal gi et felles, strukturert og risikobasert utgangspunkt for arbeidet med overgangen til kvantesikkerhet. Her anbefales det at aktørene i finanssystemet har innført kvantesikker kryptografi innen 2035.

NSM har sektorovergripende ansvar for å rådgi i prosessen med å bytte til nye algoritmer. Det er også utgitt en veileder som skal være hjelp til planlegging og gjennomføring.[10] NSM publiserte 7. juni 2026 et posisjonsnotat som oppfordrer alle virksomheter til å imøtekomme kvantetrusselen innen 2030.[11]

Finanstilsynet følger opp håndteringen av kvanterisiko i finanssystemet gjennom tilsyn med enkeltforetak i finansiell sektor. Temaet drøftes også i Finanstilsynets årlige rapport Risiko- og sårbarhetsanalyse.[12]

Norges Bank følger opp kvantesikkerhet i egne systemer, og vil gjøre det i tilsynet med interbanksystemer og i overvåkingen av betalingssystemet mer generelt.

Hva skjer på internasjonalt nivå?

G7 Cyber Expert Group[13] publiserte i januar 2026 felles strategiske anbefalinger for overgangen til kvantesikker kryptografi.[14] Disse inkluderer tidlig kartlegging av kryptografiske avhengigheter, testing av PQC-algoritmer og styrket samarbeid mellom banker, infrastrukturer og leverandører, med særlig fokus på risiko forbundet med data med lang levetid og tredjepartsavhengigheter.

Parallelt legger BIS Innovation Hub[15] til rette for praktisk utprøving gjennom Project Leap.[16] Her har BIS, europeiske sentralbanker og SWIFT demonstrert at kvantesikre digitale signaturer kan benyttes i faktiske betalingsmeldinger, og at hybride kryptografiske løsninger kan støtte en sikker overgang fra dagens systemer. Erfaringene herfra peker også på noen av utfordringene man møter: Siden signaturer og nøkler kan være store, er det ikke nødvendigvis plass nok i standardiserte meldingsformat og tidsbruken i hver transaksjon kan stige betydelig.

Arbeidet i internasjonale fora har direkte betydning for norske aktører. SWIFT-infrastrukturen er sentral i både europeiske og norske betalingssystemer, og norske institusjoner vil som følge av EØS-tilknytningen og regelverk som DORA være pålagt å etterleve europeiske krav til kryptografisk robusthet og IKT-risikohåndtering.

9 Se Finans Norge (2026).

10 Se NSM (2023).

11 Posisjonsnotat om kvantenøkkeldistribusjon – Nasjonal sikkerhetsmyndighet.

12 Se Finanstilsynet (2026).

13 Dette er en arbeidsgruppe med representanter fra finansmyndigheter i G7-landene og EU, som koordinerer policy og deler informasjon knyttet til cybersikkerhet.

14 Se G7 CEG (2026).

15 BIS Innovation Hub søker å fremme samarbeid blant sentralbanker om innovativ finansiell teknologi. BIS Innovation Hub har sentre rundt om i verden, herunder et nordisk senter i Stockholm.

16 Se BIS (2025b).

Veien videre

Overgangen til kvantesikker kryptografi er en av de mer omfattende sikkerhetsendringene man har sett i elektroniske systemer. I motsetning til mange tidligere problemer med kryptografi som ofte måtte løses på kort varsel, er denne overgangen planlagt og gradvis.[17] Viktige fremskritt er allerede gjort, men arbeidet er langt fra ferdig. Ved å ta fatt på testing og integrasjon av kvantesikre løsninger tidlig, kan man sikre at dagens systemer forblir trygge – også i møte med fremtidens kvantedatamaskiner.

Det er viktig for sikkerheten i betalings- og finanssystemet at overgangen skjer med god kvalitet og til rett tid. Man må kartlegge, klargjøre og gjennomføre et bytte til kvantesikker kryptografi. Dette må skje i hele sektoren og i samarbeid med parter man er avhengig av for å få et samlet system til å fungere som det skal.[18]

I mange tilfeller er overgangen til kvantesikker kryptografi forholdsvis lett å håndtere: Det er snakk om å få rullet ut nye eller oppdaterte produkter fra leverandører når de er klare. I andre tilfeller må nye standarder på plass. Leverandører av viktige komponenter er i forskjellige løp for å tilpasse sine produkter, og det kan ta tid å bli ferdig. Det kan også finnes spesielle situasjoner hvor mer må gjøres. Alt dette må håndteres, tidlig heller enn sent.

Sikkerheten i egne systemer er den enkelte virksomhets ansvar. Det er samtidig viktig at prosessen i finanssektoren går ryddig for seg og sørger for at aktørene ender opp med felles systemer som virker i tråd med målbildet.[19] Partene som skal bruke kryptografi må bli enige om hva de skal bruke når, ellers vil nettverkene ikke fungere slik de skal. Det må derfor koordinering til for å få landet overgangen på en god måte.

17 Tiden man har på å fullføre byttet er likevel knapp, da mange systemer må oppdateres.

18 Avhengighetene kan være omfattende og inkludere leverandørindustri, støttende nettverk med mer.

19 Et kvantesikkert system bør ha en form for smidighet som gjør at man kan bytte ut algoritmer som knekkes i fremtiden.

Vedlegg

Tabeller[1]

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

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
NICS											
NICS Brutto	772	980	1 021	1 567	1 859	2 028	2 278	2 483	2 419	2 458	956
NICS Netto (millioner)	9,1	9,5	9,9	10,5	11,1	10,1	9,7	10,0	10,0	9,7	9,6
NICS Real[1]						333 255	510 180	583 183	588 816	582 349	575 228
NBO											
Totalt antall transaksjoner	1 565	1 835	1 958	2 555	2 745	2 935	3 175	3 540	3 782	4 595	13 577
RTGS bruttotransaksjoner utenom NICS	658	700	793	841	859	930	828	898	1 182	1 924	12 420

[1] Daglig gjennomsnitt for NICS Real er beregnet på antall kalenderdager.

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

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

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
NICS	**285,9**	**284,1**	**297,0**	**315,3**	**323,2**	**347,0**	**351,7**	**408,7**	**417,5**	**404,8**	**259,9**
NICS Brutto	160,1	158,7	163,3	175,2	176,0	196,1	189,3	232,4	236,2	219,4	73,7
NICS Netto	125,8	125,4	133,7	140,1	147,2	150,6	162,0	175,8	180,9	185,0	185,8
NICS Real[1]						0,2	0,4	0,4	0,4	0,4	0,4
NBO	**219,3**	**221,2**	**235,8**	**247,6**	**259,3**	**458,1**	**327,4**	**338,6**	**355,0**	**350,0**	**359,0**
NICS Brutto	157,5	156,1	159,0	172,2	158,0	178,5	169,7	203,0	204,9	204,1	71,5
RTGS bruttotransaksjoner utenom NICS	46,0	40,4	42,1	57,3	81,7	261,5	136,8	114,0	123,5	119,0	263,6
NICS Netto	11,9	12,4	13,1	13,3	13,5	13,4	14,6	12,1	15,8	19,0	15,4
NICS Real[1]						0,0	0,0	0,0	0,0	0,0	0,0
VPO	3,8	3,7	4,2	4,8	6,0	4,7	6,2	9,5	10,8	9,7	8,4

[1] Daglig gjennomsnitt for NICS Real er beregnet på antall kalenderdager.

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

1 Tabeller som viser utviklingen i kunderettet betalingsformidling, er publisert i rapporten Kunderetta betalingsformidling 2025.

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

	2020	2021	2022	2023	2024	2025
Norges Banks oppgjørssystem (NBO): Banker med konto i Norges Bank	122	118	118	111	104	95
Norges Banks oppgjørssystem (NBO): Banker med masseoppgjør i Norges Bank	21	21	21	20	19	19
DNB	87	86	83	82	76	66
SpareBank 1 SMN	10	9	8	7	6	6
Norwegian Interbank Clearing System (NICS)	119	118	114	111	103	95

Kilder: Bits og Norges Bank

Norges Banks ansvar

Norges Bank skal fremme finansiell stabilitet og et effektivt og sikkert betalingssystem.[1] I denne sammenhengen omfatter betalingssystemet alle måter, ordninger og innretninger som kan benyttes til å utføre eller formidle betalinger, både med kontanter og kontopenger og andre betalingsmidler. Dette er en videre definisjon enn betalingssystemlovens definisjon (se ramme).

Norges Bank ivaretar sitt ansvar ved å blant annet:

- Legge til rette for et stabilt og effektivt system for betaling, avregning og oppgjør mellom foretak med konto i banken.
- Utstede sedler og mynter og sørge for at de kan fungere effektivt som betalingsmiddel.
- Overvåke betalingssystemet og annen finansiell infrastruktur og bidra til beredskapsløsninger.
- Føre tilsyn med interbanksystemer.

Som operatør sørger Norges Bank for effektive og sikre driftsløsninger og setter vilkår for tjenestene banken tilbyr. Som tilsynsmyndighet stiller Norges Bank krav til konsesjonsbelagte interbanksystemer. Gjennom overvåkingen oppfordrer Norges Bank aktørene til å følge prinsipper og standarder for beste praksis og å gjennomføre endringer som bidrar til å

1 Se sentralbankloven § 1-2 og betalingssystemloven § 2-1.

Finansiell infrastruktur

Finansiell infrastruktur kan defineres som et nettverk av systemer som sørger for at finansielle transaksjoner blir gjennomført. Det innebærer at betalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp, og at informasjon om beholdningsstørrelser blir oppbevart.

Den finansielle infrastrukturen omfatter betalingssystemet, verdipapiroppgjørssystemet, verdipapirsentraler, sentrale motparter og transaksjonsregistre.

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 svikt i infrastrukturen kan bli vesentlig større enn de bedriftsøkonomiske kostnadene for systemeierne. Derfor er den finansielle infrastrukturen underlagt regulering, tilsyn og overvåking fra myndighetene.

opprettholde en sikker og effektiv finansiell infrastruktur. Med effektivitet menes at betalinger kan gjennomføres raskt, til lave kostnader og på måter som er tilpasset brukernes behov.

Norges Banks bruk av virkemidler på de ulike områdene vil variere over tid og være tilpasset utviklingen i betalingssystemet og den finansielle infrastrukturen. Norges Bank skal gi Finansdepartementet råd når det er behov for tiltak av andre enn banken for å oppfylle formålet for sentralbankvirksomheten.

Norges Banks arbeid med tilsyn og overvåking

Norges Bank er konsesjons- og tilsynsmyndighet for den delen av betalingssystemet som kalles interbanksystemer, se tabell 1. Det er systemer for avregning og oppgjør mellom kredittinstitusjoner. Dersom et konsesjonsbelagt interbanksystem ikke er innrettet i tråd med betalingssystemloven eller konsesjonsvilkårene, vil Norges Bank kreve at systemeier retter opp dette. Formålet er å bidra til at interbanksystemer organiseres slik at hensynet til finansiell stabilitet blir ivaretatt. Norges Bank kan gi unntak fra kravet om konsesjon til interbanksystemer som vurderes å ha begrenset betydning for finansiell stabilitet.

Overvåking innebærer å følge med på enkeltsystemer og utviklingstrekk og å være en pådriver for forbedringer. Gjennom dette arbeidet kan Norges Bank oppfordre aktørene til endringer som kan gjøre betalingssystemet og annen finansiell infrastruktur sikrere og mer effektiv. Norges Bank overvåker betalingssystemet som helhet, og sentrale enkeltsystemer er underlagt et fast og regelmessig overvåkingsopplegg, se tabell 1.

Tabell 1 Finansiell infrastruktur underlagt tilsyn eller overvåking av Norges Bank

System		Instrument	Operatør	Norges Banks rolle	Andre ansvarlige myndigheter
Interbanksystemer	Norges Banks oppgjørssystem (NBO)	Penger	Norges Bank	Tilsyn (Norges Banks representantskap) og overvåking	Tilsyn: Nasjonal sikkerhetsmyndighet
	Norwegian Interbank Clearing System (NICS)	Penger	Bits	Konsesjon og tilsyn	Tilsyn: Nasjonal sikkerhetsmyndighet
	DNBs oppgjørsbanksystem	Penger	DNB Bank	Konsesjon og tilsyn	Konsesjon og tilsyn med hele bankens virksomhet: Finanstilsynet og Finansdepartementet
	SpareBank 1 SMNs oppgjørsbanksystem	Penger	SpareBank 1 SMN	Overvåking	Konsesjon og tilsyn med hele bankens virksomhet: Finanstilsynet og Finansdepartementet
	CLS	Penger	CLS Bank International	Overvåking i samarbeid med andre myndigheter	Konsesjon: Federal Reserve Board Tilsyn: Federal Reserve Bank of New York Overvåking: Sentralbanker med valuta i CLS (blant andre Norges Bank)
Verdipapiroppgjørs-systemer	Euronext Securities Oslos verdipapirsentral-virksomhet	Verdipapirer og penger	Euronext Securities Oslo og Norges Bank	Overvåking	Konsesjon og tilsyn med Euronext Securities Oslo: Finanstilsynet
	LCHs sentrale motpartsystem	Finansielle instrumenter	LCH	Overvåking i samarbeid med andre myndigheter	Tilsyn: Bank of England Overvåking: EMIR College og Global College (blant andre Norges Bank)
	Cboe Clear Europes sentrale motpartsystem	Finansielle instrumenter	Cboe Clear Europe	Overvåking i samarbeid med andre myndigheter	Tilsyn: Den nederlandske sentralbanken Overvåking: EMIR College (blant andre Norges Bank)

Betalingssystemlovens definisjoner

Betalingssystemer er interbanksystemer og systemer for betalingstjenester.

Interbanksystemer er systemer for overføring av penger mellom banker med fellesregler 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.

Norges Bank vurderer systemer under tilsyn og overvåking etter prinsipper utarbeidet av Committee on Payments and Market Infrastructures (CPMI) og International Organization of Securities Commissions (IOSCO).[2] CPMI er en komité bestående av representanter for sentralbanker. IOSCO er den internasjonale organisasjonen for tilsynsmyndigheter for verdipapirmarkedene. Målet med prinsippene er å sikre en robust finansiell infrastruktur som fremmer finansiell stabilitet.

Flere av systemene som Norges Bank fører tilsyn med eller overvåker, følges også opp av andre myndighetsorganer. Overvåkingen av internasjonale systemer som er viktige for finansiell sektor i Norge, foregår gjennom deltakelse i internasjonale samarbeidsfora.

Finanstilsynet fører tilsyn med systemer for betalingstjenester. Det er kunderettede systemer som publikum generelt har tilgang til, som kontanter, kortordninger og betalingsapplikasjoner. I sentralbankloven fra 2019 tydeliggjøres det at Norges Bank har et ansvar for overvåking av betalingssystemet som helhet, herunder de kunderettede systemene som Finanstilsynet fører tilsyn med. Det følger av forarbeidene til sentralbankloven at Norges Bank i overvåkingen av betalingssystemet bør kunne nyttiggjøre seg Finanstilsynets vurderinger av de kunderettede systemene på en egnet måte, særlig når det gjelder sikkerheten i disse systemene.

Det felleseuropeiske regelverket Central Securities Depository Regulation (CSDR) pålegger Norges Bank enkelte oppgaver som supplerer Norges Banks ansvar for å overvåke Euronext Securities Oslo etter sentralbankloven. Finanstilsynet er kompetent (besluttende) myndighet for Euronext Securities Oslo etter CSDR, mens Norges Bank er relevant (rådgivende) myndighet.

2 Principles for financial market infrastructures. Se CPMI-IOSCO (2012).

En nærmere beskrivelse av de enkelte systemene som Norges Bank fører tilsyn med eller overvåker, er gitt i Norges Bank (2025c).

Fokusområder i Norges Banks tilsyn- og overvåkingsarbeid

Prioritere arbeidet med å styrke motstandskraft mot alvorlige cyberangrep

I tilsyn og overvåking vil Norges Bank legge økt vekt på systemeiernes arbeid med å styrke motstandskraften mot cyberangrep. Dette er spesielt viktig i lys av den rasle teknologiske utviklingen innenfor kunstig intelligens og kvanteteknologi. Vi vil gjennomgå av FMIers trussel- og risikovurderinger innen cybersikkerhet. Videre vil det legges vekt på virksomhetenes rutiner for beredskap, kontinuitet og hendelses-håndtering, herunder planer for og gjennomføring av tester og øvelser.

Prioritere arbeidet med beredskap for kritiske funksjoner

Foretakene må i større grad forberede seg på mer alvorlige hendelser enn tidligere. Norges Bank vil i tilsyn og overvåking følge opp at det etableres tilstrekkelig uavhengige beredskapsløsninger for kritiske funksjoner.

Leverandøravhengighet og leverandørkjeder

Norges Bank vil følge opp hvordan virksomhetene håndterer avhengig-heter til kritiske leverandører og leverandørkjeder. Det er viktig at virk-somhetene har god styring og kontroll med leverandører og utkontraktert virksomhet. Det vil legges vekt på håndtering av avhengighet til felles kritiske tjenesteleverandører, samt virksomhetenes planlegging for håndtering av risiko for brudd i leveransekjeder, herunder tilgang på kritiske innsatsfaktorer som maskinvare og nøkkelkompetanse. Videre er det sentralt at det foreligger realistiske exit-strategier for kritiske leverandører.

Referanser

Ahmed, R. og Aldasoro, I. (2026) Stablecoins and safe asset prices, BIS Working Papers No 1270

Bank of England (2025) Proposed regulatory regime for sterling-denominated systemic stablecoins, Consultation Paper

BIS (2025a) The next-generation monetary and financial system, BIS Annual Economic report 2025

BIS (2025b) Project Leap: quantum-proofing the financial system

Cipollone (2026) The digital euro in a fragmenting world: ensuring Europe's resilience and autonomy in payments, tale 01.04.2026

CPMI-IOSCO (2012) Principles for Financial Market Infrastructures (PFMI)

Finans Norge (2026) Veikart for en kvantesikker finansnæring | Finans Norge, veikart 23.03.2026

Finanstilsynet (2026) Risiko- og sårbarhetsanalyse 2026 – Finanstilsynet.no, rapport

G7 CEG (2026) G7 Cyber Expert Group Releases Roadmap for Coordinating the Transition to Post-Quantum Cryptography in the Financial Sector | U.S. Department of the Treasury, nyhetsmelding 12.01.2026

IMF (2025) Global Financial Stability Report, October 2025, «Shifting Ground beneath the Calm», rapport

McKinsey og Artemis Analytics (2026) Stablecoins in payments: What the raw transaction numbers miss

NIST CSRC PQC (2024) National Institute of Standards and Technology – Computer Security Resource Center – Post-Quantum Cryptography

Norges Bank (2023) Digitale sentralbankpenger – eksperimentell testing i prosjektfase 4, Norges Bank Memo 2/2023

Norges Bank (2024) Undersøkelse om kryptoeiendeler i Norge, Norges Bank Memo 2/2024

Norges Bank (2025a) Kunderetta betalingsformidling 2024

Norges Bank (2025b) Norges Bank går ikke inn for digitale sentralbankpenger nå, nyhetsmelding 10.12.2025

Norges Bank (2025c) Det norske finansielle systemet 2025, rapport

Norges Bank (2026a) Digitale sentralbankpenger – sluttrapport fra prosjektfase 5, Norges Bank Memo 1/2026

Norges Bank (2026b) Vurdering av konsekvenser for Norge av en innføring av digital euro, Norges Bank Memo 2/2026

Norges Bank (2026c) Digitale sentralbankpenger – eksperimentell testing i prosjektfase 5, Norges Bank Memo 3/2026

Norges Bank (2026d) Undersøkelse om kryptoeiendeler i Norge, Norges Bank Memo 6/2026

Norges Bank (2026e) Husholdningers bruk av og holdninger til kontanter. Norges Bank Memo 7/2026

NSM (2023) Kvantemigrasjon – veileder – Nasjonal sikkerhetsmyndighet, veileder 10.10.2023

NSM (2026) Posisjonsnotat om kvantenøkkeldistribusjon.

Norges Bank
Finansiell infrastruktur 2026
Oslo 2026

Adresse: Bankplassen 2
Post: Postboks 1179 Sentrum, 0107 Oslo
Telefon: 22316000
E-post: central.bank@norges-bank.no
www.norges-bank.no

Ansvarlig redaktør: Ida Wolden Bache

Design: TRY
Layout: Aksell AS
ISSN 1894-8316