Norges Bank

3 | 2023

Norges Bank Memo

Digitale sentralbankpenger – eksperimentell testing i prosjektfase 4

RAPPORT FRA EN ARBEIDSGRUPPE

Innhold

1. Innledning og sammendrag

Dette er en delrapport fra fase 4 av Norges Banks prosjekt om digitale sentralbankpenger (DSP). Prosjektet startet i 2016. Rapporter fra de tidligere prosjektfasene er tilgjengelige på Norges Banks nettsider. Norges Bank har ikke tatt stilling til om DSP bør innføres og i tilfelle med hvilken teknologi og design.

I fase 4 av Norges Banks DSP-prosjekt ble arbeidet med å validere tekniske løsninger supplert av eksperimentell testing. Arbeidet er gjennomført av en Valideringsgruppe (VG)[1] som også har utarbeidet denne rapporten om den eksperimentelle testingen.

Hensikten med arbeidet har vært å validere om ulike teknologier kan realisere egenskapene DSP må ha for å kunne fylle sitt formål.[2] Videre har arbeidet vært et grunnlag for dialog med næringen, andre myndigheter og andre sentralbanker. Valideringsarbeidet har også bidratt til å bygge nødvendig kompetanse for å kunne vurdere hvordan arbeidet med DSP bør videreføres.

I tillegg til bruk av interne ressurser i Norges Bank har en ekstern prosjektkoordinator bistått i valideringsarbeidet. Fire IT-selskaper har blitt engasjert for å utvikle applikasjoner som ble benyttet for å teste egenskapene. I tillegg engasjerte Norges Bank en student for programmeringsoppgaver. Norges Bank har også hatt kontakt med studenter som har gjennomført studentprosjekter og skrevet masteroppgaver relatert til DSP.

I arbeidet har Norges Bank hatt dialog med en rekke private aktører (herunder blant annet norske og internasjonale teknologiselskaper og finansielle institusjoner som for eksempel banker etablert i Norge), myndigheter, andre sentralbanker og internasjonale organisasjoner, som BIS Innovation Hub (BISIH). Norges Bank har videre redegjort for DSP-utredningen på mange konferanser og seminarer, samt arrangert to konferanser og tre hackathons i samarbeid med andre.

Den eksperimentelle testingen ble gjennomført ved å konstruere en rekke testcaser som validerer aspekter ved en eller flere egenskaper. Testingen ble i hovedsak gjennomført i en prototype/sandkasse basert på åpen kildekode og blokkjedeteknologi (privat Ethereum nettverk) som ble utviklet av et av IT-selskapene. Den eksperimentelle testingen vurderes som vellykket i henhold til målsettingen med testingen, inkludert at egenskapslisten i tabell 1 dekkes. I tillegg til selve valideringen har testingen vært et springbrett for samarbeid med ulike aktører.

Teknologivalgene som ble gjort, herunder bruk av kjent teknologi basert på åpen kildekode, har vært en viktig faktor i måloppnåelsen. Dersom en mer ukjent og/eller proprietær teknologi hadde blitt valgt, er det lite sannsynlig at vi ville oppnådd samme resultater.

---

[1] Gruppen har bestått av Peder Østbye (leder), Espen Gjøs, Helge Syrstad, Terje Åmås, Suela Kristiansen og Kjetil Watne. Suela og Kjetil sluttet seg til gruppen underveis i arbeidet. I tillegg har Lasse Meholm fra selskapet Finansit deltatt som ekstern prosjektkoordinator. Knut Sandal og Anette Monshaugen har deltatt på aktiviteter i VG som assosierte medlemmer. IT-selskapene som er nevnt i teksten er Nahmii, Symfoni, NBX og Alpha Venturi.

[2] Egenskapene er definert i Norges Bank Memo 1/2021.

Mange tester ble gjennomført. Samtidig kan eksperimentell testing ved etablering av nye testcaser og videreutvikling av eksisterende testcaser i neste fase gi ytterligere innsikt nødvendig for en eventuell innføring av DSP. Blant annet vil løsninger som tilrettelegger for et godt personvern og regulatorisk etterlevelse kunne belyses videre. Det kan også utarbeides testcaser for ytelsestesting (for eksempel antall transaksjoner pr. sekund og tid til endelig oppgjør) og sikkerhetstesting. Det er også behov for å teste ut insentivstrukturer og nye forretningsmodeller for tredjeparter (bl.a. bankene), handelsstanden og forbrukere.

Testingen har vist at forskjellige typer teknologier og måter å vedlikeholde registre på har forskjellige egenskaper som i ulik grad er egnet til å oppfylle egenskapene en DSP må ha. For å utnytte fordeler og ulemper som ligger i ulike registerløsninger kan en mulig løsning være å benytte seg av flere registre som knyttes samme gjennom "broer". Gjennom slike broer kan de relative fordelene med ulike typer registre utnyttes. Broer reiser imidlertid enkelte særskilte utfordringer som er belyst i den eksperimentelle testingen.

I strategien for Norges Bank fram mot 2025 framgår det at sentralbanken skal gjøre seg klar til «eventuelt å kunne innføre digitale sentralbankpenger». Det vil innebære at man både må vurdere behovet for og konsekvenser av innføring av DSP, samt framskaffe informasjon om løsninger som kan innføres og anbefales for eventuell innføring.

VGs vurdering basert på testarbeidet omtalt og informasjon innhentet fra leverandører av DSP-løsninger til andre land, er at det per i dag ikke finnes tilgjengelige tilstrekkelig ferdig utviklede løsninger (også kjent som «hyllevare»- eller «white label»-løsninger) som på en tilfredsstillende måte kan oppfylle kravene/nødvendige egenskaper til norske DSP.

Å utvikle en fullverdig DSP-løsning er en omfattende oppgave og arbeidsgruppen vurderer det som lite aktuelt at Norges Bank selv utvikler en fullverdig løsning gitt ressursene det krever.

DSP-teknologiene utvikles raskt, og det vil trolig utvikles mer velegnede løsninger i løpet av strategiperioden, både i markedet og som en følge av utviklingsarbeid i andre sentralbanker. Det som utvikles i andre sentralbanker kan også være relevant teknologi for en eventuell norsk DSP.

I tillegg til denne delrapporten utgis det en sluttrapport fra prosjektfasen, som Norges Bank Memo 2/2023[3]. Det utgis også et Norges Bank Staff Memo om konsekvenser for likviditetsstyring og pengepolitikk[4]. Det er tidligere utgitt et Norges Bank Staff Memo[5] om nødvendige lovendringer for å kunne innføre DSP.

---

[3] Norges Bank Memo (2/2023). «Digitale sentralbankpenger – sluttrapport fra prosjektfase 4. Rapport fra en arbeidsgruppe.»

[4] Bernhardsen, T. og Kloster, A. (2023): «Digitale sentralbankpenger - konsekvenser for likviditetsstyringen og pengepolitikken», Norges Bank Staff Memo, https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Signerte-publikasjoner/Staff-Memo/20232/sm-19-2023-dsp/

[5] Syrstad, H. (2023): "Innføring av digitale sentralbankpenger - Nødvendige lovendringer", Norges Bank Staff Memo 4/2023, https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Signerte-publikasjoner/Staff-Memo/20232/sm-4-2023-dsp/

2. Metode anvendt i valideringsarbeidet

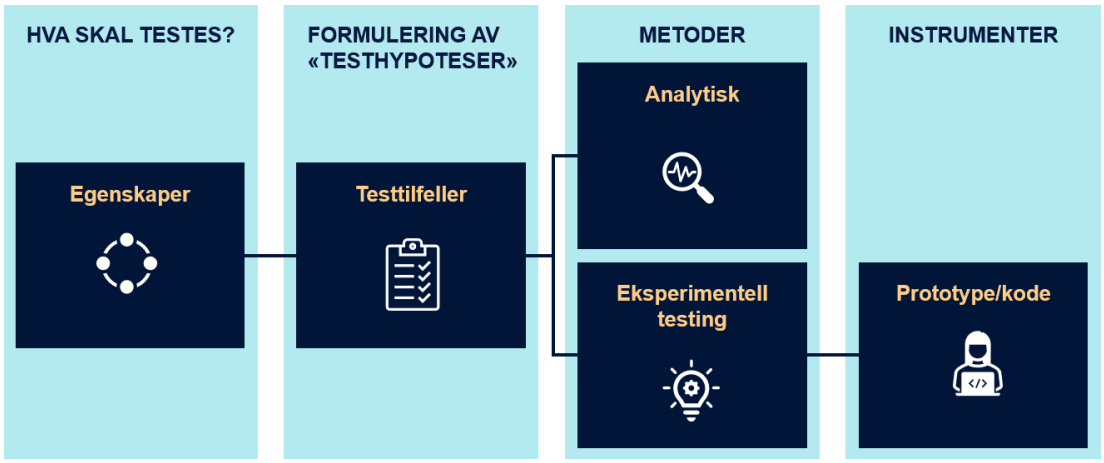
Valideringsarbeidet har bestått av eksperimentell testing og analyser. Formålet har vært å undersøke om tekniske løsninger kan oppfylle egenskapene i tabell 1 identifisert i Norges Bank Memo 1/2021.

Tabell 1: Egenskaper DSP må ha, identifisert i Norges Bank Memo 1/2021

E1	Fordring på Norges Bank
E2	Par verdi mot kontanter og bankinnskudd
E3	Kunderettet fokus
E4	Tilstrekkelig friksjon mot bankinnskudd
E5	Kontrollert av Norges Bank
E6	Kan fungere som tvungent betalingsmiddel
E7	Samsvar med EØS-forpliktelser
E8	Betalinger umiddelbare og endelige
E9	Samsvar med gode IT-arkitekturprinsipper
E10	Tilfredsstiller krav til teknisk uavhengighet og mulighet for betaling offline
E11	Kundekommunikasjon og -kontroll foretas av tredjeparter
E12	Fleksibilitet for ulike personvernløsninger
E13	Plattform for tredjepartstilbydere
E14	Ivareta gjennomslaget av pengepolitikken
E15	Relevant informasjon i NBs makroøkonomiske overvåking
E16	DLT-kompatibelt
E17	Attraktiv nisjeløsning

Testingen har vært gjennomført ved hjelp av testcaser siden det er vanskelig å teste egenskapene direkte. Egenskapene har derfor indirekte blitt testet gjennom test-caser som belyser om egenskapene oppfylles, se figur 1.[6]

[6] Testcasene har derfor vært en analytisk formidler («mediator») mellom teknologien og egenskapene.



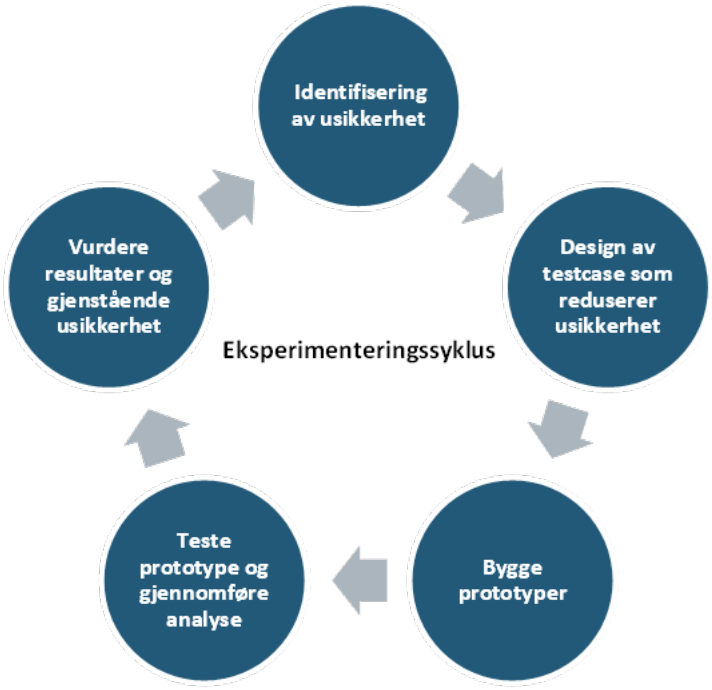
Figur 1 Gjennomføring av testing

Kilde: Norges Bank

Analysearbeid og eksperimentell testing har komplementert hverandre. På områder der vi ikke har testet tilstrekkelig selv, slik som for eksempel innen offline-løsninger, har prosjektet dratt nytte av eksternt arbeid. Dette omfatter både analytisk arbeid og tester gjennomført av andre. Egen eksperimentell testing har også fungert som et ytterligere kildetilfang til analyser gjennomført av andre, og dermed muliggjort kilde- og metodemangfold i testingen og kvalitetssikring av resultater.

Det har også vært en iterativ prosess mellom tester og prioriteringer og konstruksjon av testcaser, som illustrert i figur 2 under. Gjennomføringen av enkelte testcaser har blant annet identifisert nye usikkerheter, som har blitt redusert med nye testcaser.

Som figur 2 indikerer er enkelte tester gjennomført ved at vi har designet testcaser basert på ulike funksjonsområder for DSP. Det reduserer usikkerhet om egenskaper kan oppfylles. Et eksempel på et testcase er utstedelse og destruksjon av DSP som beskrevet i kapittel 3.3(A) under. Utstedelse og destruksjon av DSP var nødvendig for å kunne teste egenskapene. Vi utarbeidet en kravspesifikasjon på hva som skulle utvikles og fikk deretter utviklet prototypen av innleide IT-konsulenter. Deretter testet vi prototypen. Til sist vurderte vi resultatet og identifiserte gjenstående usikkerhet. Ved å starte med et behov kunne vi også vurdere om egenskapene i tabell 1 var tilfredsstilt.



Figur 2 Eksperimenteringssyklus

Kilde: Norges Bank

Gjennomføringen av testcasene er i hovedsak gjort ved hjelp av en prototype basert på et privat Ethereum-nettverk og åpen kildekode som kalles Hyperledger Besu. Denne teknologien er beskrevet nærmere nedenfor. Bruk av åpen kildekode har gjort det enkelt å kunne dele arbeidet med andre og engasjere norske fintech- og utviklingsmiljøer. I september 2022 ble kildekoden til prototypen offentliggjort på Github, noe som dannet grunnlag for en teknisk sandkasse som deltakerne i testingen - både interne og eksterne - kunne benytte seg av.

Vi har også gjennomført mer avgrensede tester på andre teknologier, herunder openCBDC som er en åpen kildekode-infrastruktur utarbeidet av Massachusetts Institute of Technology (MIT) i samarbeid med Boston Fed.

Testingen innebar også at Norges Bank finansierte utviklingsprosjekter og deltok i samarbeider med aktører som ønsket og hadde kapasitet til å delta i testingen. Det omfattet banker og andre betalingsaktører, herunder fintech-selskaper, myndighetsorganer, samt akademia. Et mangfold av aktører og interessenter har dermed på ulike måter deltatt i eller bidratt til testingen.

VG har hatt en åpen tilnærming og har hatt møter med en rekke aktører der det er informert om arbeidet. Sammen med disse aktørene har vi i løpet av høsten/vinteren 2022-23 blant annet arrangert to konferanser kombinert med hackathon/ideathon samt en idemyldring.

3. Gjennomføring av eksperimentell testing

3.1 Teknologivalg i den eksperimentelle testingen

I Norges Bank Memo 1/2021 ble det anbefalt å teste flere teknologier. Dette følger også av mandatet for valideringsarbeidet. Det var særlig behov for å teste teknologien i tokenbaserte løsninger. Den har noen fellestrekk med teknologien som brukes i kryptovalutaer/blokkjeder, og som bygger videre på innovasjoner i kryptografi og desentraliserte systemer.

En viktig motivasjon for å teste tokenteknologi, er at den har potensial til å replisere viktige egenskaper ved kontanter, herunder være en uavhengig infrastruktur for sentralbankpenger tilgjengelig for publikum, og samtidig gjøre det mulig å benytte sentralbankpenger til nett-/avstandsbetaling. I tillegg til dette kan digitale tokenbaserte penger tilby innovativ funksjonalitet som for eksempel programmerbarhet. Det er imidlertid usikkerhet knyttet til slik teknologi, og det er behov for mer kunnskap før en kan konkludere på om denne teknologien er egnet for en eventuell DSP-løsning i Norge. Derfor har denne teknologien fått særlig oppmerksomhet i den eksperimentelle testingen.

Som nevnt har den eksperimentelle testingen i hovedsak benyttet teknologi basert på åpen kildekode. Det har flere årsaker. Mye av teknologien bak og rundt kryptovalutaer og tokenbaserte løsninger er basert på åpen kildekode og det finnes mange utviklingsmiljøer, også i Norge. Åpen kildekode gir også frihet til å gjennomføre testing uten å være avhengig av tilgang til enkeltaktørers proprietære teknologier. Det gjør samarbeidet med leverandører og andre aktører enklere og mer fleksibelt. Videre er det utviklet en rekke tilgjengelige matematiske modeller og simuleringsverktøy som kan supplere testingen. Selv om ikke åpen kildekode nødvendigvis vil bli valgt for en eventuell endelig løsning for DSP, kan man lære mye gjennom åpen kildekode som er overførbart til andre teknologier.

Nedenfor følger en oversikt over teknologiene som er benyttet i den eksperimentelle testingen.

Ethereum-teknologi
Ethereum er kjent som en åpen og offentlig blokkjede med den innebygde kryptovalutaen Ether. Men det finnes også private varianter av Ethereum som ikke har noen tilknyttet kryptovaluta, slik som Hyperledger Besu. I et slikt blokkjede-nettverk finnes det såkalte noder installert på datamaskiner som sørger for at transaksjonene valideres (at betaler har penger på "konto" og har signert transaksjonen) og at smartkontraktene prosesseres. Nodene i nettverket kan drives sentralisert eller desentralisert. Selv om nettverket/registeret ikke benytter en åpen og offentlig blokkjede, kan man benytte øvrig Ethereum-teknologi. En slik privat variant av Ethereum ble benyttet for prototypen som ble utviklet og som utgangspunkt for testcasene. Det innebærer at betalingssystemet er implementert i et testnettverk av noder som benytter programvaren Hyperledger Besu.[7]

[7] https://www.hyperledger.org/use/besu

I denne teknologien representeres penger ved en såkalt ERC-20-token.[8] Dette innebærer at penger er representert som balanser på registeradresser som kan sammenlignes med bankkontoer. Disse registeradressene kan potensielt kobles til identifiserbare personer gjennom en separat database («aliasbase» se 3.3.E).

Teknologien legger til rette for den programmeringsfunksjonaliteten (dvs. implementere smartkontrakter) som tilbys på Ethereum (gjennom «Ethereum Virtual Machine»-EVM).[9] Programmeringsfunksjonalitet innebærer at dataprogram kan kjøres i registeret.[10] Blant annet kan programmeringsfunksjonaliteten legge til rette for betingelser for utstedelse og destruksjon, anonyme betalinger (ved hjelp av kryptografi), og betingede betalinger (betalinger som avhenger av at en eller flere predefinerte hendelser inntreffer).

Det er utviklet mye komplementær programvare i "markedet" (også basert på åpen kildekode) som for eksempel digitale lommebøker, personvernløsninger, analyseverktøy og systemer for regulatorisk etterlevelse. Slik komplementær programvare har blitt benyttet i testingen.

Mange såkalte «stablecoins» og infrastrukturer innen blokkjedeteknologi har valgt å basere seg på blant annet ERC-20-tokens og Ethereums programmeringsspråk, slik at teknologien er forholdsvis velprøvd. Det er derfor en rask utvikling av ulike infrastrukturer som kan kombineres med Ethereum-teknologi. Hyperledger Besu og ERC-20-token benyttes også av andre sentralbanker og BISIH i testing av DSP.

OpenCBDC/Project Hamilton
OpenCBDC/Project Hamilton[11] er et samarbeid mellom den amerikanske sentralbankens avdeling i Boston (Boston FED)[12] og MIT Digital Currency Initiative.[13] I en første fase har de testet kapasiteten til noen alternative infrastrukturer. I denne testingen har penger en litt annen representasjon enn i Ethereum-teknologien benyttet i vår prototype. Verdier er representert ved token som eieren disponerer ved hjelp av kryptografiske koder som følger en gyldig transaksjonskjede (såkalt "unspent transaction output" – UTXO[14]) fra opprinnelig utstedelse. Pengene akkumuleres derfor ikke i balanser som de gjør i Ethereum-teknologien omtalt over. Denne måten å representere verdi på benyttes i ulike Bitcoin-varianter og i flere andre kryptovalutaer.

Programvaren som Hamilton-prosjektet benytter i sin testing er basert på åpen kildekode som er tilgjengeliggjort for ekstern testing. Flere andre sentralbanker har benyttet anledningen til å gjennomføre tester på denne kildekoden. Vårt DSP-prosjekt har kun gjennomført noen svært begrensede tester av OpenCBDC-teknologien. En av egenskapene til openCBDC-teknologien er at den kan behandle

[8] https://ethereum.org/en/developers/docs/standards/tokens/erc-20/. ERC står for «Etherum Request for Comments»
[9] https://ethereum.org/en/developers/docs/evm/
[10] Med at et vilkårlig program kan kjøres, menes at EVM er såkalt «Turing-komplett», som betyr at et hvilket som helst mulig program kan kjøres.
[11] https://dci.mit.edu/project-hamilton-building-a-hypothetical-cbdc
[12] https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx
[13] https://dci.mit.edu/
[14] https://www.ledger.com/academy/glossary/unspent-transaction-output-utxo

1,8 millioner transaksjoner i sekundet, noe som er avgjørende for store land som USA.

Informasjonsinnhenting om teknologi benyttet av hyllevareleverandører
Noen private aktører har utviklet DSP-løsninger som er satt i produksjon eller inngår i pilottester. BISIH[15] har deltatt i flere av disse pilottestene. Noen av løsningene er basert på Ethereum-teknologi, andre er basert på varianter av «UTXO», mens noen har utviklet helt egne teknologier. Løsningene har ulike innslag av proprietær teknologi.

Som en del av den eksperimentelle testingen i denne fasen gjennomførte prosjektet noen tester på overordnet nivå av løsningene til to slike hyllevareleverandører. Det har gitt innsikt i teknologiene, hvordan løsningene fungerer ende-til-ende og gitt grunnlag for å «benchmarke» teknologiene mot prototypen Norges Bank selv har fått utviklet. Konkret har vi gjennomført to workshoper med to ulike internasjonale aktører.

Samvirket mellom pengerepresentasjoner og registre (broer og "swaps")
En overordnet erfaring fra testarbeidet er at det neppe vil være ett register/database eller én teknologi som dekker alle behov knyttet til DSP. Ulike typer registre og teknologier dekker ulike funksjoner og behov, for eksempel programmerbarhet, massebetalinger, betalinger mellom ting/maskiner og offline-betalinger.

Ulike registre kan også ha forskjellige tilgangsrettigheter. For eksempel kunne en tenke seg at bare Norges Bank, andre sentralbanker og banker hadde tilgang til registeret der DSP utstedes og slettes – slik at dette kjerneregisteret i praksis fungerte som et såkalt "wholesale" DSP (DSP for oppgjør - kun tilgjengelig for aktører med konto i sentralbanken) som omgjøres til "retail" DSP (kunderettet DSP som er allment tilgjengelig) i andre registre.

En kan også i prinsippet tenke seg at DSP kan flyttes over til private registre (ved bruk av en «bro»), herunder desentraliserte registre, selv om det reiser egne problemstillinger. Et viktig element i testingen har derfor vært å teste såkalte broer mellom ulike registre. En bro innebærer forenklet at man kan flytte DSP-tokens fra ett register til et annet, slik at ulike typer registre kan virke sammen. En mulig type helhetlig arkitektur som kan generaliseres fra testcasene, er et mangfold av registre som er knyttet sammen gjennom broer.

Som en del av testingen av broer har vi testet hvordan DSP kan veksle mellom ulike tokenrepresentasjoner innenfor Ethereumteknologien som prototypen er bygget på (en såkalt "swap"). Testcase 3.3.C er et eksempel på en slik form for bro.

En annen type bro som har vært testet (testcase 3.3.H), er mellom prototypen og et register basert på IOTA-teknologi. IOTA er et betalingssystem basert på desentralisert teknologi, særlig tilpasset for IoT (tingenes internett) og automatiserte prosesser som gjennomfører transaksjoner i store volum med små beløp og foretar finansielt oppgjør/betaling uten manuell medvirkning. Tokenbaserte penger som er programmerbare fungerer godt i en slik mekanisme.

[15] https://www.bis.org/about/bisih/about.htm

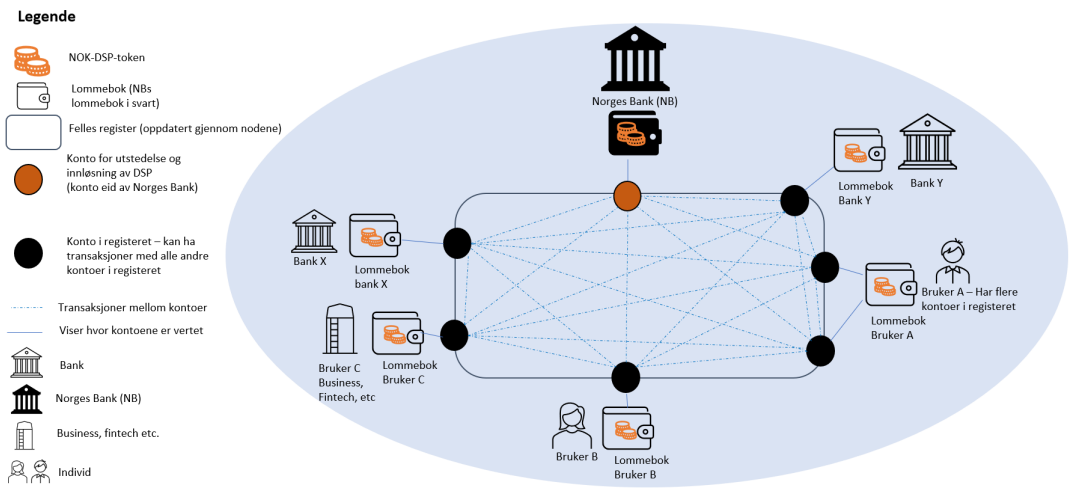
3.2 Utviklingen av prototypen

Et av de nevnte IT-selskapene fikk etter en anbudskonkurranse våren 2022 i oppgave å utvikle en prototypeinfrastruktur basert på et privat Ethereum-nettverk som omtalt over, for å kunne gjennomføre testcaser. I dette dokumentet omtales prototypen også som en sandkasse. Kildekoden ble publisert på offentlig Github i september 2022.

Selskapet fikk også i oppgave å drive nettverket på vegne av Norges Bank. Dette innebar at selskapet opprettet seks noder (omtalt over) som hver inneholder en full versjon av registeret/databasen med alle transaksjonene. Et oppsett med flere noder bidrar til redundans og reduserer risikoen for nedetid ved bortfall av enkeltnoder.

Prototypen er konfigurert slik at transaksjoner initiert av brukerne samles i blokker (blokkjede) som legges til registeret hvert femte sekund. Transaksjonene legges til registeret og konsolideres mellom nodene ved hjelp av en konsensusmekanisme basert på såkalt “proof-of-authority". Dette betyr at nodene, som er under Norges Banks kontroll, men driftet av IT-selskapet, validerer og godkjenner alle transaksjonene som legges til registeret. Dette er en vesentlig forskjell fra åpne blokkjeder som eksempelvis benyttes i Bitcoin, der det kreves en konsensusmekanisme som muliggjør at enhver kan delta i valideringen av transaksjoner på en desentralisert måte uten behov for en sentral aktør som driver registeret (såkalt “proof-of-work"). Teknologien i prototypen åpner imidlertid opp for mer desentraliserte valideringsmåter (konsensusmekanismer) dersom det skulle være ønskelig. “Proof-of-authority" krever svært lite energi/kostnader sammenlignet med “proof-of-work”. Vi valgte for øvrig å la betalingene være gratis, uten det som kalles “gas” (transaksjonskostnad) i Ethereum.

Figur 3 viser overordnet arkitektur for prototypen.



Figur 3 Visualisering av prototypen

Kilde: Norges Bank

Tilgang til testmiljøet er passordregulert, og eksterne aktører som ønsket å delta i testingen fikk tildelt brukernavn og passord for å kunne delta. For å interagere og bruke registeret må brukeren ha en digital lommebok. Vi valgte å benytte en såkalt "soft-wallet"[16] med "key-store-file" der brukernes kryptografiske koder ligger i en fil som er beskyttet med et passord.[17] Lommeboken oppbevarer kodene for brukerne, og er dermed en digital lommebok uten forvalter (såkalt "self-hosted/self-custodial wallet").

Alle brukere er i prinsippet likeverdige. Det innebærer at alle brukere har tilgang til registeret og kan sende transaksjoner fra den ene til den andre, og se transaksjoner i registeret med en såkalt blokkutforsker ("blockexplorer").[18] Selv om alle brukere i utgangspunktet er likeverdige, kan dette endres gjennom å utnytte programmeringsfunksjonaliteten som ligger i EVM.

I prototypen er det kun Norges Bank som kan utstede og destruere DSP. Tanken som ligger til grunn, er at Norges Bank overfører DSP til banker og potensielt andre private aktører, som så igjen overfører DSP til sine kunder. Dette kalles to-lags arkitektur. Ulike tilgangsnivåer har vært utforsket nærmere i noen av testcasene.

Prototypen er ikke utviklet med tanke på senere å kunne bli en produksjonsløsning for DSP. Det vil i så fall kreve omfattende videre utvikling og testing. Det har for eksempel ikke blitt gjennomført ytelsestester eller sikkerhetstester av prototypen, som vil være viktig for en produksjonsløsning. Det finnes mange eksperimentelle og analytiske arbeider utført av andre som belyser disse sidene ved teknologien mer generelt. Slik testing vil eventuelt være del av senere arbeid.

3.3 Testcaser knyttet til prototypen

Tabell 2 gir en summarisk oversikt over de gjennomførte testcaser knyttet til prototypen og hvilke egenskaper som ble testet i testcasene. Noen av testcasene har vært relevante i forhold til flere egenskaper mens andre dekker "bare" en av egenskapene. Likevel innebærer dette ikke at alle forhold ved egenskapene har blitt testet.

[16] En wallet er en digital lommebok.
[17] Et alternativ er å bruke en såkalt «seed phrase» dvs. en «tilfeldig» generert rekke av ord som deterministisk genererer private nøkler. Brukeren må da huske denne rekken av ord for å gjenskape de kryptografiske nøklene.
[18] Blockscout ble benyttet som blokkutforsker i testingen.

Teststrømmer	Testcaser	Utvalg av egenskaper som er testet
i) Utvikling av prototype infrastruktur basert på privat Ethereum nettverk (open source)	A. Utstedelse og destruksjon av DSP	E1, E5, E8, E9, E11, E15, E16
	B. Overføring til og mellom digitale lommebøker	E1, E5, E8, E9, E11, E15, E16
ii) Videreutvikling av og funksjonalitet i prototype infrastruktur	C. Overføring mellom tokenstandarder	E3, E13, E16, E17
	D. Masseutbetalinger	E3, E6, E11, E16, E17
	E. Aliasbase	E3, E7, E11, E12, E16
	F. Digital identitet/ eIDAS2	E3, E7, E12, E11, E12, E16
	G. Renteberegning	E4, E14
	H. Broer mellom DSP i prototypen og andre registre	E7, E13, E16, E17
	I. Beløpsgrenser ved betalinger og beholdning	E13, E17
	J. Antihvitvasking m.m.	E7, E11
	K. Anonyme betalinger	E3, E7, E12, E17

Tabell 2 Oversikt over teststrømmer og testcaser

i. Utvikling av prototype infrastruktur basert på privat Ethereum nettverk (med åpen kildekode)

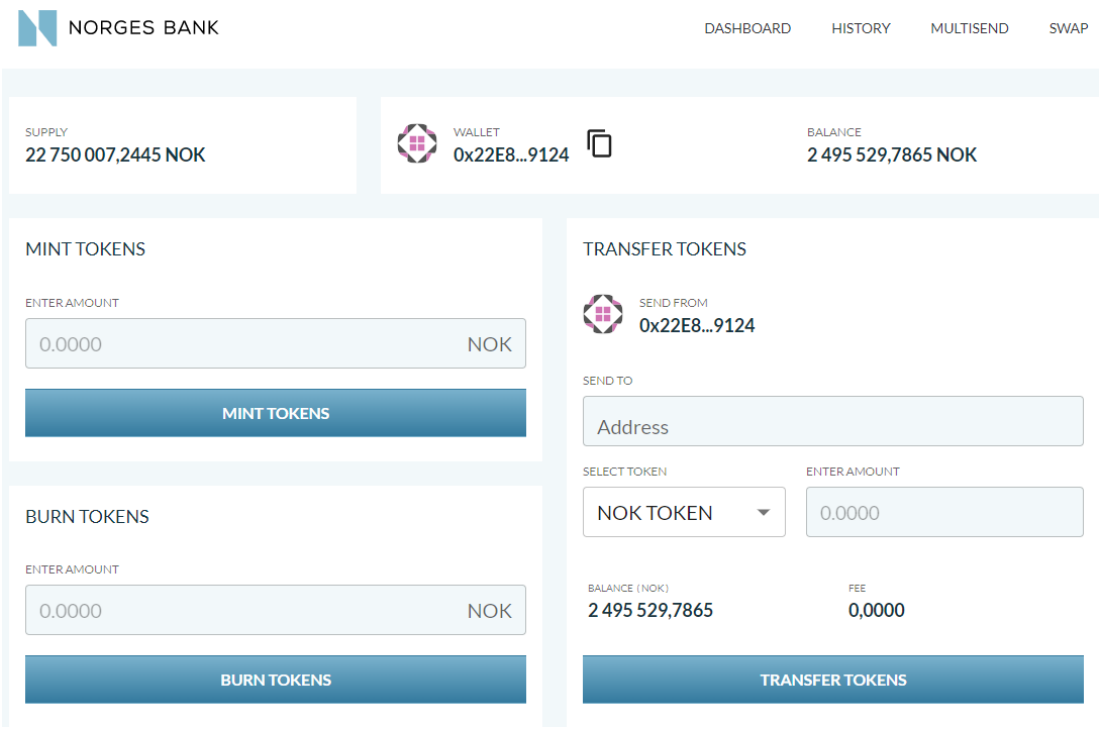
Opprettelse av sandkasse, noder, digital lommebok/wallet med brukergrensesnitt for Norges Bank og banker.

A. Utstedelse og destruksjon av DSP

Dette testcaset er knyttet til flere ønskede DSP-egenskaper, bl.a. at kun Norges Bank kan utstede og destruere DSP. Den digitale lommeboken som ble utviklet ga Norges Bank alene rettigheter til å utstede og destruere DSP. Det ble også utviklet en enkel digital lommebok/wallet og et dashboard for sentralbankens overvåkning av blokkjeden og sirkulasjon av DSP. Figur 4 viser skjermbildet av

brukergrensesnittet. Som det vises på bildet, er det mulig for Norges Bank å utstede («mint») og destruere («burn») DSP-tokens.

Testen bekreftet at kun Norges Bank kunne utstede og destruere DSP. Skjermbildet under viser “Balance” oppe til høyre som er hvor mye DSP sentralbanken har i sin beholdning og “Supply” oppe til venstre viser verdien av DSP som er i omløp.



Figur 4 Skjermbilde fra den digitale lommeboken til Norges Bank

B. Overføring til og mellom digitale lommebøker

I prototypen er det mulig å overføre NOK-tokens fra én register-adresse (konto) til en annen. Balansen oppdateres fortløpende. Det har blitt testet med flere adresser og transaksjoner og gjennomført i sanntid (betalinger umiddelbare og endelige). Dette kan være en vennebetaling mellom to personer med DSP- lommebøker. Det kan også være to næringsdrivende som betaler til hverandre eller en kunde som betaler fysisk i butikk eller på nett. Dette vises på høyre side i skjermbildet over.

Testen bekreftet at transaksjoner mellom digitale lommebøker kunne gjennomføres.

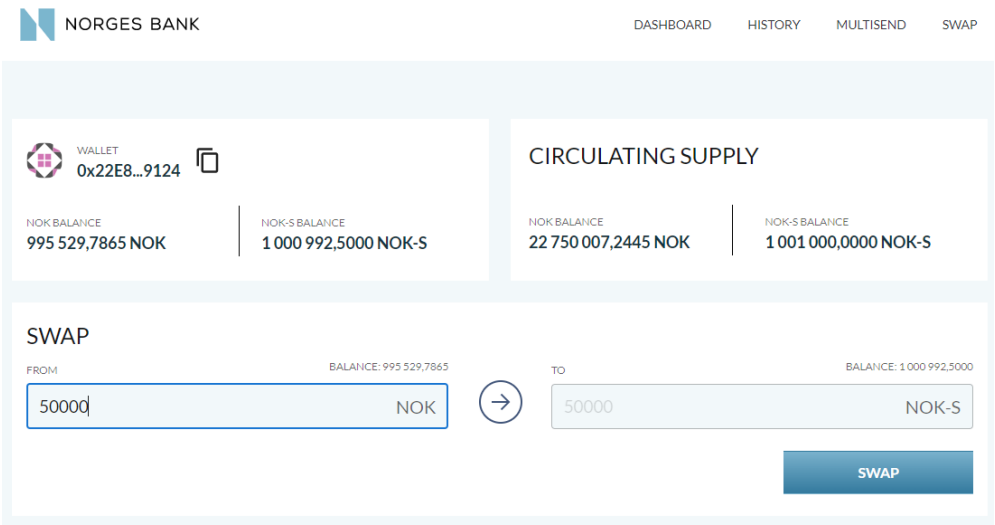
ii) Videreutvikling av og funksjonalitet i prototype infrastruktur

C. Overføring mellom tokenstandarder - broer

Formålet med dette testcaset var å undersøke om tokens kan overføres mellom registre med ulike tokenstandarder innenfor prototypen. Dette er et eksempel på å teste om tokens kan flyttes fra en teknologi til en annen med uforandrede egenskaper. Ulike tokenstandarder kan ha ulike fordeler og ulemper. For eksempel

kan innebygget programmeringsfunksjonalitet og informasjon som kan følge token være forskjellige. En type token kan for eksempel være særlig nyttig i fordelsprogrammer i detaljhandelen.

I testcaset ble DSP konvertert i sanntid fra en type token til en annen (som eksemplet referert til her – fra ERC-20 token til ERC-1400 token). Ved bro/swapping justeres i sanntid mengden av tokens tilgjengelig i de ulike nettverk/øko-systemene i forskjellige former: konvertering fra ERC-20 token til ERC-1400 token skjer ved å låse token i ERC-20 (locked) nettverket og samtidig utstede (mint) token i ERC-1400 nettverket. Når NOK føres tilbake, skjer det ved å destruere (burn) token i ERC-1400 nettverket og låse opp samme verdi i ERC-20 nettverket.



Figur 5 Utveksling av NOK-token med S-NOK-token

Testen bekreftet at det var mulig å overføre DSP mellom registre basert på ulike standarder.

D. Masseutbetalinger

Formålet med dette testcaset var å undersøke om prototypen kunne benyttes til gjennomføring av masseutbetalinger. En slik funksjonalitet kan bidra til å gjøre DSP til en effektiv og kundevennlig betalingsløsning for utbetalinger til mange mottakere i en og samme prosess. Som eksempelet nedenfor viser, kan det også gjøre DSP til en attraktiv nisjeløsning for spesielle betalingssituasjoner.

Løsningen bør kunne benyttes til masseutbetalinger til flere millioner betalingsmottakere, men vi valgte av praktiske grunner å begrense til ca. 200. Videre testing med flere mottakere vil være avhengig av videre utvikling av sandkassen med gyldige adresser til flere mottakeres digitale lommebøker.

En slik funksjonalitet kan eksempelvis være aktuell ved utbetaling av strømstøtte. For eksempel i form av en utbetaling på 500 kroner i støtte til elektrisitetskostnader til alle med mindre enn 750 000 kroner i inntekt og flere enn to barn (dette vil kreve

integrasjon med for eksempel skattetall for å kunne automatisk avdekke hvem som er berettiget til slik støtte). I slike tilfeller kan det vurderes om utbetaling gjennomføres via DSP.[19] Et annet eksempel er utbetaling av lønn fra store selskaper.

Selv om denne testen ble gjennomført med massebetalinger til et begrenset antall mottakere, vil funksjonaliteten også kunne benyttes til utbetalinger til langt flere mottakere.

E. Aliasbase

Formålet med dette testcaset var å få validert muligheten for å knytte betalinger opp mot eier av digital lommebok. Det ble utviklet en løsning med en database (MYSQL) som ligger på en server utenfor blokkjeden (off-chain) hvor informasjon om eier av lommebok med navn, personnummer og mobiltelefonnummer ble lagret. Det gjør det mulig for en betaler å få opp navnet på mottaker i skjermbildet for betaling for å unngå å betale til feil person. En slik database kan og bør muligens lagres (slik som i dag) i hver kundens hovedbank som er ansvarlig for at KYC/AML ("Know Your Customer"/"Anti Money Laundering") skjer på en sikker måte og i henhold til EØS-forpliktelsene. Dette bekrefter også at det er mulig å skille privat informasjon fra betalingstransaksjoner.

Testen bekreftet at tilknytning til en aliasbase er mulig.

F. Digital identitet/ eIDAS2

EU arbeider med løsninger for digital identitet og lommebok i tilknytning til eIDAS2-reguleringen[20] (bruk av eIDAS2 er også kjent som «verified credentials» (VC) / «verifisert identitet»). I samarbeid med Digitaliseringsdirektoratet (Digdir) utviklet vi en løsning, som benytter samme mekanisme som eIDAS2 ved å utvikle et såkalt «orakel» i tilknytning til ID-porten. Det gjør det mulig å verifisere at en person er den vedkommende utgir seg for å være. Det kan forenkle og forbedre arbeid med KYC og AML for banker og tredjeparter. Vår løsning i testen benyttet det faktum at DSP er programmerbar hvor pengene programmeres (smartkontrakt) til å ikke være eid av noen uten verifisert identitet. Norges Bank er så vidt vi vet den første sentralbanken i verden som tester en slik mulighet.

Digital identitet er en forutsetning for at digitale betalinger foretas på en sikker måte og for å redusere risiko for at DSP benyttes ved hvitvasking og til terrorfinansiering. Betaler og mottaker må være kjent og midlenes opprinnelse må dokumenteres.

---

[19] Flere regulatoriske problemstillinger er knyttet til dette testcaset. Dersom utenlandske arbeidstakere ikke har mulighet for å legitimere seg, kan tilgang til DSP være problematisk i forhold til AML-reglene. Men man kan vurdere at i noen tilfeller kan standardisert europeisk tilgang (for eksempel, som forventet med eIDAS2) redusere barrierene. I tillegg, selv om en legitimeringsløsning er på plass, kan det være slik at utenlandske aktører ikke har tilgang til DSP.

[20] eIDAS står for «**E**lectronic **ID**entification, **A**uthentication and Trust **S**ervices Regulation». Mer informasjon om EIDAS kan finnes her: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation og her: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.

Utfordringene blir større for grensekryssende betalinger. Ulike land har ulike løsninger, og det er så langt lite standardisering. Dette er et tema som diskuteres mye internasjonalt.

Testen bekreftet at verifisering av identitet via «verified credentials» var mulig.

G. Renteberegning

Formålet med dette testcaset var å få belyst muligheten for renteberegning på beholdninger av DSP. Det er ikke tatt stilling til om Norges Bank ønsker å ha renter på eventuelle DSP eller ikke. Prosjektet hadde likevel fått i oppdrag å teste om renter på DSP var teknisk gjennomførbart. Det ble utviklet og testet renter på DSP, både positive og negative renter. Prosjektet fikk derfor programmert og testet renter på DSP i sandkassen. Testen viste at det var mulig å gjennomføre renteberegninger over en simulert periode på to år, hvor det var diverse renteendringer, og med både positive og negative rentesatser.

I gjennomføringen valgte vi å utnytte muligheter ny teknologi gir for å gjennomføre renteberegning. Istedenfor å beregne renter periodevis, for eksempel etterskuddsvis en gang i året, valgte vi kontinuerlig forrentning. Renteberegningen ble utviklet basert på arkitekturen til DeFi protokollen Aave.[21] Renteberegning ble lagt inn i smartkontrakten i ERC-20 token, dermed testet vi også programmerbarheten til DSP. I prinsippet betyr det at det er pengene selv som beregner rentene, ikke sentralbanken eller bankene. Renter beregnes i prinsippet ved gjennomføringen av hver transaksjon. Saldoen i den digitale lommeboken multipliseres med rentefot pr. sekund som igjen multipliseres med antall sekunder siden siste transaksjon. Renten i kroner som kommer frem kan brukes umiddelbart av eieren av den digitale lommeboken. Det vil være sentralbanken som fastsetter rentesatsen.

Det ble også utviklet løsning som kan oppdatere ferdigutfylt skatteseddel ved årsskifte med renter for avsluttet år, slik bankene gjør i dag, om behov.

Renter kan benyttes som en mekanisme for å påvirke insentivene til å holde DSP og dermed regulere volumet av DSP i befolkningen. For eksempel vil negative renter på DSP redusere ønske om å ha penger i DSP-wallet.

Vi har i et annet testcase testet maksimalgrenser på DSP per person i ulike varianter.

Gjennomføringen av testcaset viste at det det var mulig å beregne renter i sanntid via Aave-protokollen.

Denne renteberegningen er et eksempel på programmerbarhet.[22] Programmerbarhet kan være i kjernen eller på toppen av et token som ved betalingstjenester (for eksempel betingede betalinger). Programmerbarhet kan i noen tilfeller også ha negative konsekvenser, samtidig som det kan gi muligheter på

[21] https://aave.com/

[22] Se https://www.bis.org/publ/bisbull72.htm for en drøfting av ulike aspekter ved programmerbarhet av tokens.

flere bruksområder. En eventuell videre testing av programmerbare DSP bør derfor akkompagneres av en analyse av konsekvenser.

H. Broer mellom DSP i prototypen og andre registre

Formålet med dette testcaset var å teste om det er mulig å overføre ERC-20 token til et annet register[23] der tokens er representert som UTXO ved hjelp av en bro. En slik teknologi er IOTA. IOTA-teknologien er spesialutviklet for tingenes internett (IoT) og maskin til maskin-betalinger hvor beløpene er veldig små (mikrobetaling), men i store volumer. Mange ser på dette som en nødvendighet i deler av fremtidens forretningsmodeller der det bl.a. betales samtidig som det forbrukes. Eksempler er veibetaling pr. tilbakelagt distanse i byer mens man kjører, istedenfor bompengebetalinger etterskuddsvis en gang i måneden som i stor grad benyttes i dag. Eller at to maskiner kommuniserer om å produsere et produkt og at de betaler hverandre fortløpende. En bro mellom ERC-20 og UTXO gjør at videre testing av offline-løsninger kan forenkles i fremtiden.

En utfordring med å gjennomføre denne testen var at teknologi i IOTA (EVM-kompatibilitet gjennom en såkalt «layer 2», L2) for å gjennomføre slike broer ikke var ferdig utviklet. Ved hjelp av forutsetninger og simulering var det likevel mulig å gjennomføre testcaset.

I. Beløpsgrenser ved betalinger og beholdning

Det ble testet to ulike grenser. Den første grensen er en maksimalgrense for beholdning, dvs. for hvor mye DSP en bruker kan ha i sin digitale lommebok. I en produksjonsløsning vil det overskytende sendes til kundens bankkonto. For å kunne replikere en bankkonto ble det opprettet en egen digital lommebokadresse som det overskytende ble sendt til. Det ble også testet en grense for betalt beløp pr. uke. I et reelt system kan det også være aktuelt med beløpsgrense og eventuelt transaksjonsbegrensninger pr. dag, uke, måned etc. Men en beløpsgrense pr. uke var tilstrekkelig for å teste mekanismen.

Testene bekreftet muligheten for å sette beløpsgrenser ved betalinger og beholdningsgrenser for lommebøker.

J. Antihvitvasking m.m.

Banker og andre aktører som tilbyr betalingstjenester i Norge og mot utlandet er underlagt særskilte lovpålagte regler for AML-tiltak, avdekking av skatteunndragelser og anti-terrorfinansiering (kjent som «Counter Financing of Terrorism», CFT). Samfunnet har et behov for å beskytte seg mot betalinger fra illegal virksomhet. Samtidig har samfunnet behov for et godt personvern, og alle typer virksomheter som behandler opplysninger som kan knyttes til enkeltpersoner i EU/EØS er underlagt regelverk slik som General Data Protection Regulation (GDPR). Ulike hensyn, behov og krav må på denne måten ses i sammenheng og balanseres mot hverandre.

[23] Dette står i motsetning til «swap» omtalt over der testcaset var å flytte tokens mellom ulike tokenstandarder i samme register.

I arbeidet med å teste DSP i Norges Bank er det gjennomført flere tester relatert til disse utfordringer, mest av alt for å skaffe erfaring om hvilke muligheter teknologien gir. For det første er det testet at transaksjonene kan monitoreres på en strukturert måte for å automatisk avdekke mulige mistenkelige transaksjoner. I tillegg er det testet at beløp under en viss grense ikke blir gjenstand for monitorering, forutsatt at det ikke utføres for mange små transaksjoner innen en viss tidsperiode. Ettersom prototypen bruker en ren blokkjedeteknologi er det mulig å monitorere både betaler og mottaker i samme prosess. Prosjektet testet også om det er mulig å stoppe mistenkelige betalinger i sanntid før de når mottaker. Til sist ble det testet at det er teknisk mulig å beslaglegge midler og overføre verdier til en digital lommebok, som for eksempel kunne være eid eller kontrollert av Økokrim.

Testene bekreftet muligheten for tilrettelegging for flere AML/CFT-relaterte prosesser.

Som beskrevet nedenfor (testcase K) har prosjektet også testet anonyme betalinger. Anonyme betalinger kan teknisk påvirke hvor effektivt AML/CFT-mekanismen fungerer.

K. Anonyme betalinger

Personvern er som nevnt et viktig hensyn i forbindelse med DSP. Det å beskytte enkeltindividers rett til privatliv må balanseres mot kravene knyttet til AML/CFT. Et omfattende tema i internasjonale fora for DSP er om noen betalinger bør kunne være fullstendig anonyme. Noen sentralbanker har foreslått at betalinger under en viss beløpsgrense kan være helt anonyme. Uansett om det blir aksept for anonymitet ved betalinger eller ikke i Norge, er det behov for å teste hva teknologien gir mulighet til.

Prosjektet har testet muligheten for at alle betalinger er anonyme, alternativt at betalinger under en viss grense er anonyme. En av teknologiene som ble undersøkt var basert på Zero Knowledge Proof (ZKP). En annen var den såkalte “tornado cash”- mekanismen. Den teknologien som ble testet mest var basert på mekanismen “Basic stealth addresses”[24]. Teknologiene for anonyme betalinger er i utvikling og ingen løsninger for dette er i dag perfekte. For eksempel kan den mye brukte ZKP skape utfordringer for programmerbarheten til DSP. Konklusjonen fra testene er at teknologien som ble benyttet kan muliggjøre anonyme betalinger, i den grad man ønsker å legge til rette for det.

3.4 Grensekryssende DSP-betalinger

Prosjekt *Icebreaker*[25] ble initiert i 2022 i samarbeid mellom Norges Bank, Sveriges Riksbank, Bank of Israel og BISIH Nordic Centre. Prosjektet utviklet en teknisk løsning for grensekryssende betalinger med DSP. De tre sentralbankenes «Proof of Concept» (PoC)/prototyper ble knyttet sammen gjennom en felles hub for å sende

[24] Som også med små endringer i algoritmene kan være kvante-motstandsdyktige.
[25] Se Norges Bank nyhetsmelding her: https://www.norges-bank.no/tema/finansiell-stabilitet/digitale-sentralbankpenger/prosjekt-icebreaker/ og nyhetsmelding fra BIS her: https://www.bis.org/about/bisih/topics/cbdc/icebreaker.htm.

beskjeder/meldinger relatert til grensekryssende betalinger med DSP mellom wallet-tilbydere og flere aktører i valutamarkedet.

Prosjektet bidrar til DSP-arbeidet på flere måter:

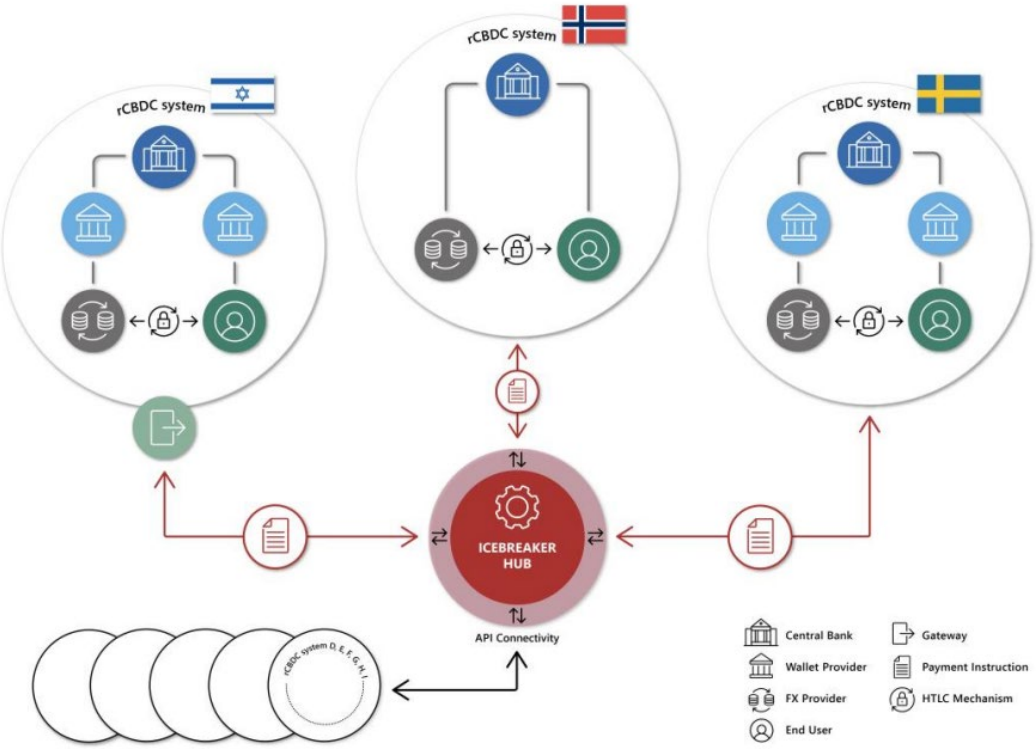
1. det viser DSP-muligheten til å effektivisere og forenkle flervaluta grensekryssende betalinger;
2. det tester for interoperabiliteteten den nåværende prototypen har med flere DSP-prototyper fra andre land;
3. det viser at det er mulig å gjennomføre grensekryssende betalinger selv om ulike land bruker ulik DSP-teknologi[26];
4. det presenterer et testcase for FXP[27]-aktører hvor oppgjørsmiddel kan være i DSP i de jurisdiksjonene de opererer i;
5. det viser at det er teknisk gjennomførbart å skape konkurranse mellom flere aktører om å levere den beste valutakursen for sluttkundene.

Løsningen krever at DSP «by design» ikke forlater jurisdiksjonen den hører til og løsningen er basert på en «hub-and-spoke»-modell. «Hub-and spoke»-løsningen er mer effektiv enn når mange lands systemer knyttes sammen én-til-én (i bilaterale modeller).

Rapporten[28] fra prosjektet ble sammen med en video[29] offentliggjort 6. mars 2023. En beskrivelse av «hub-and-spoke»-modellen utviklet under *Icebreaker* vises i figur 6.

Prosjektet har medført at Norges Bank har skaffet seg verdifull erfaring og kompetanse fra andre sentralbankers DSP-prosjekter. Prosjektet beviste også at en «teknologiagnostisk» tilnærming er mulig, idet hvert land kan benytte ulike teknologier i deres design av DSP. «Huben» vil i prinsippet kunne hente inn valutakurser fra et stort antall FXP-aktører som gjør at betaler kan velge den beste valutakursen i markedet. FXP kan være en bank eller en annen type aktør som tilbyr valutaveksling. Den valgte FXP har beholdninger av DSP i minst to lands DSP og er ansvarlig for å gjennomføre valutavekslingen/betalingen. Det benyttes en teknologi som kalles Hashed Timelock Contract (HTLC) som sørger for at pengene ikke kommer på avveie og grensekryssende betalinger kan gjennomføres på sekunder.

[26] Sentralbankene har ulike teknologier i bruk i deres PoC/prototyper - Riksbanken bruker Corda, mens Bank of Israel bruker Quorum.
[27] Foreign Exchange Providers.
[28] https://www.bis.org/publ/othp61.htm
[29] https://www.bis.org/about/bisih/topics/cbdc/icebreaker.htm



Figur 6 Hub-and-spoke modell i Icebreaker

Kilde: Prosjekt *Icebreaker*

Flere implikasjoner kan utledes av eksperimentet avhengig av videre policy- og tekniske justeringer. *Icebreaker*-prosjektet utforsket kun én måte å bidra til effektivisering av grensekryssende betalinger via DSP.

Bygging av en slik «hub-and-spoke»-løsning er drevet av et ønske om en «happy path» (tester ikke for mulige tekniske problemer), uten at denne løsningen blir veid mot andre tekniske løsninger som kan være mer effektive i drift til tross for høy investering i oppbygningsfasen.

3.5 Utforskning av løsninger for betalinger offline

Prosjektet har ikke gjennomført direkte tester av offline-løsninger. En offline-betaling er i denne sammenheng en betaling med DSP som kan gjennomføres selv om det ikke er mulig for begge parter i en transaksjon å kommunisere med Norges Banks register når betalingen gjennomføres. Prosjektet har likevel vært involvert i enkelte prosjekter som har gitt mer informasjon om offline-løsninger.

To masterstudenter ved NTNU skrev en masteroppgave[30] om designvalg for offline-løsninger for en norsk DSP. I den forbindelse gjennomførte studentene en simulering av offline-systemer, herunder hvordan deling av transaksjonsdata mellom brukere kan bidra til å gjøre et offline-system sikrere enn dersom brukere kun lagrer sin egen transaksjonshistorikk. Studentene gjennomførte intervjuer med deltakere i DSP-prosjektet underveis i arbeidet. Dette samarbeidet er et godt eksempel på hvordan studentprosjekter kan supplere valideringsarbeid.

Prosjekt Polaris er et prosjekt som ledes av BISIH Nordic Centre og har som hovedformål å utrede ulike offline-aspekter knyttet til DSP. Norges Bank er deltakende observatør i dette prosjektet.

Polarisprosjektet har så langt blant annet utarbeidet en offline-håndbok og en designguide.[31] Håndboken tar for seg sentrale problemstillinger som må avklares i prosessen med å bygge et offline-system.

Blant annet er det viktig å avklare formålet med offline-betalinger før man designer og bygger et slikt system. Er det beredskap som er hovedformålet, og hvilke beredskapssituasjoner skal løsningen eventuelt være rettet mot. Er for eksempel finansiell inkludering eller anonymitet viktigere enn beredskap? Andre viktige designvalg som må vurderes er:

- Om systemet skal være basert på hardware eller software?
- Om det skal være ett eller flere offline-systemer (og eventuelt om disse skal være interoperable)?
- Hvordan skal overføring mellom online- og offline-systemet skje? Må pengene representeres på samme måte i de to modulene? Må brukerne på forhånd overføre en del av sine DSP i en egen lomme i lommeboken for bruk ved betalinger offline?
- Når er offline-betalinger endelige? Kan offline-modulen selv gi finalitet? Kan man gjøre mange offline-betalinger etter hverandre, eller må man «sjekke inn» med online-modulen mellom hver betaling?
- Bør det være begrensninger i antallet betalinger eller verdien av betalinger som kan gjennomføres offline?

4. Samarbeidsaktiviteter som har belyst valideringsarbeidet

En oversikt over viktige aktiviteter i samarbeid med partnere er gitt i tabell 3. Aktivitetene har hatt flere hensikter:

- Norges Bank synliggjør sitt arbeid med DSP og øker dermed muligheten for engasjement og bidrag fra et bredt spektrum av aktører (akademia, samt private og offentlige aktører);

[30] Sjur Brekke Espedal og Dennis Aleksander Janzso.“Design Choices for Offline Transactions in a Norwegian Central Bank Digital Currency". Master’s thesis in Communication Technology and Digital Security, Norwegian University of Science and Technology (NTNU), juni 2022.
[31] Project Polaris: Part 1. Handbook for offline payments with CBDC tilgjengelig her: https://www.bis.org/publ/othp64.htm. Project Polaris: Part 4. High-level design guide for offline payments tilgjengelig her: https://www.bis.org/publ/othp79.htm.

- Metodisk aktivitet hjelper flere fora med å bidra til et «åpen innovasjon»-perspektiv;
- Etablert dialog kan være verdifull i videre arbeid Norges Bank gjør med DSP.

Aktivitet[32]	Beskrivelse	NBs rolle
DSP-prosjekt i detaljhandelen	Prosjekt der noen store aktører i dagligvarehandelen utforsket brukscaser for DSP.	- Observatør
Konferanse & hackathon i Bergen 21. oktober 2022 i samarbeid med Simula/Universitetet i Bergen (UiB)	Konferanse om DSP, særlig tekniske sider. Konferansen var også «kick-off» for hackathon om broer mellom registre.	- Medarrangør - Jurymedlem
Idemyldring 22. november 2022 og hackathon 19. januar 2023 i samarbeid med Digdir	Norges Bank og Digdir gjennomførte en idemyldring 22. november 2022. Det var også starten på en hackathon som fikk sin avslutning og presentasjon i auditoriet i Norges Bank 19. januar 2023. Her var det flere grupper som presenterte mange interessante brukscaser.	- Medarrangør
Workshop på Universitetet i Oslo (UiO) 10. januar 2023	Teknisk workshop om DSP og IoT/M2M	- Medarrangør
Møter, arrangementer og hackathon i samarbeid med Fintech Norway	Vi har hatt flere møter med Fintech Norway og Virke. Hackathon ble gjennomført 15.-17. mars 2023 fysisk i Oslo.	- Medarrangør

Tabell 3 Oversikt over aktiviteter

Formatet på aktivitetene varierer avhengig av problemstilling og kontekst. Hackathon ble brukt til å engasjere deltakere i en teknisk løsning, mens konferanse og workshops ble brukt til å tiltrekke akademikere og andre målgrupper, i tillegg til å gi Norges Bank verdifull informasjon. Idemyldring var mest praktisk rettet.

DSP-prosjekt i detaljhandelen
De største dagligvareaktørene i Norge har høsten og vinteren 2022-23 vært eiere av og deltakere i prosjektet «Central Bank Digital Currencies – Use cases in retail". Nordic Initiative var koordinator for prosessen. Norges Bank var observatør.

I prosjektets sluttrapport[33] heter det om motivasjon for prosjektet:

[32] Rangert kronologisk etter aktivitetsstart.
[33] https://www.nordicinitiative.com/theinitiative

"Being able to buy food is a critical function in society. If CBDCs are to be a true alternative to other forms of payment, they must at least be able to be used to buy food. CBDCs may become legal tender, but even if they are not, grocery merchants may have to accept them. The retail actors should familiarize themselves with the potential implications. But CBDCs may also bring benefits, depending on the features they are equipped with. It is at this point, early in the process, that the opportunities to influence the development of future money are the greatest".

Prosjektets formål var å beskrive og visualisere noen eksempler på bruk av DSP i dagligvarehandelen, og beskrive muligheter og utfordringer. Dette skulle gjøres på en måte som kunne gjenbrukes/videreutvikles for annen handel og øvrig næringsliv.

Prosjektet pekte på noen potensielle fordeler med DSP:

- Forsterket betalingsberedskap.
- Reduserte kostnader knyttet til kontanthåndtering.
- Muligheter for innovasjon, bl.a. gjennom bruk av smartkontrakter.

Prosjektet pekte også på noen forutsetninger for en vellykket innføring:

- DSP må være tilstrekkelig uavhengig av dagens betalingsløsninger.
- DSP må inkludere offline-funksjonalitet:
    - Mulighet for P2P-betalinger, for eksempel innenfor en beløpsgrense.
    - Mulighet for å "laste ned" penger til en fysisk enhet.
- Løsningen bør bygge på prinsipper fra blokkjede/DLT som åpner for smarte kontrakter.
- DSP må fungere godt over landegrenser. Det er avgjørende at sentralbankene samarbeider for å sikre interoperabilitet.
- Kostnadene knyttet til å innføre og drifte DSP må holdes nede. Det er viktig at DSP ikke belaster brukersteder og kunder unødvendig. I stedet bør løsningen føre til økt konkurranse i betalingsmarkedet.

I prosjektrapporten heter det:

"Through the exploration of central bank digital currencies, the participants have come to the conclusion that the introduction of CBDCs may bring a number of advantages, as long as important prerequisites are met. At the same time, the retail actors could play a decisive role for a successful introduction. (…)".

For Norges Bank har dette vært en viktig aktivitet for å bedre forstå behovet som brukersteder i detaljhandelen har til betalingsinfrastrukturen og som innspill til videre arbeid med DSP.

Konferanse & hackathon i Bergen 21. oktober 2022 i samarbeid med Simula/UiB

Den første DSP-konferansen ble arrangert i Bergen i oktober 2022[34]. Konferansen var forskningsrettet med ca. 50 deltakere fra akademia, FinTech-miljøet og sentralbanker. Det var også deltakelse fra samarbeidspartnere internasjonalt, som for eksempel BISIH Nordic Centre, Digital Euro Association (DEA) og OpenCBDC[35].

[34] Dedikert nettside for konferansen finnes her: https://simula-uib.com/cbdc-event-2022/
[35] Program for konferansen finnes her: https://simula-uib.com/wp-content/uploads/2022/11/Bergen-CBDC-Conference-programme-v2.pdf

Temaer diskutert i konferansen var blant annet: arbeidet med DSP i Norges Bank, DeFi og juridiske problemstillinger, AML og DSP, personvern og DSP, kvanteteknologi og OpenCBDC.

Konferansen ble en kick-off for en hackathon[36] med fokus på å overføre DSP-tokens gjennom broer mellom openCBDC og EVM-kompatible nettverk. Det ble ikke delt ut pris for beste bidrag i denne hackathon.

Idemyldring og hackathon i samarbeid med Digdir
Sommeren 2022 startet arbeidet med å planlegge en idemyldring sammen med Digdir. Tema var "Hvilke eksisterende problemer kan DSP løse, og hvilke nye muligheter kan DSP gi samfunnet?" Arrangementet ble holdt i lokalene til Digdir 22. november 2022, hvor anslagsvis 100 påmeldte personer møtte opp og ble delt inn i grupper for idemyldring. På slutten av dagen ble gruppenes forslag presentert i plenum. Denne dagen var også starten på en teknisk hackathon. Hackathon ble utført i grupper på opptil 5 personer som programmerte tekniske løsninger i prototypen/sandkassen til Norges Bank. 11 grupper presenterte sine verdifulle forslag til hva DSP kan bidra med i et arrangement i Norges Bank 19. januar 2023.

Workshop på UiO
10. januar 2023 gjennomførte vi workshop med Blockchain Lab på UiO. Universitetet deltok med forelesere fra det akademiske miljøet med omfattende kunnskap om ulike forhold knyttet til blokkjedeteknologi, som for eksempel IT-sikkerhet, miljøvern og prosessorkapasitet. Mye tid ble også viet til tingenes internett (IoT) og maskin til maskin (M2M)-kommunikasjon og betalinger.

Møter, arrangementer og hackathon i samarbeid med Fintech Norway
Hackathon var rettet mot medlemmer i Fintech Norway og Virke. Hackathon varte i tre dager og var dermed det mest kompakte hackathon-arrangementet i denne fasen. To grupper ble med i sluttpresentasjonene som ble begrenset til visualisering via PowerPoint-presentasjoner. Aktiviteten var vellykket idet den engasjerte private aktører til å bli mer kjent med vår prototype. I tillegg ga det brede spektrumet av deltakerne mulighet til å utvikle konseptene, med fokus på både kundesentrisk perspektiv og underliggende teknologi som kan tas i bruk. Det ble bl.a. vist til muligheten for semi-offline DSP muliggjort via DAG-teknologi (samme teknologi i bruk som for IOTA), mulighet for peer-to-peer transaksjoner via «escrow vault» (som bruker til dels HTLC-mekanismer), mulige løsninger for personvern og bedre brukeropplevelser. Med den begrensede tiden som var til rådighet fikk ikke gruppene utviklet tekniske løsninger.

[36] Dedikert nettside for hackathon finnes her: https://www.cbdc-hack.no/

5. Eksterne tester som har belyst valideringsarbeidet

5.1 Tester gjennomført av andre sentralbanker/BIS

De aller fleste sentralbanker gjør en eller annen form for arbeid med DSP.[37] Mesteparten vurderer DSP som er tilgjengelig for allmenheten (såkalt "retail" DSP). Det er også mange sentralbanker som ser på "wholesale" DSP for oppgjør mellom banker og store aktører i finansmarkedet. Dette er å betrakte som sentralbankreserver i tokenisert form og kan potensielt styrke oppgjøret av handel og betalinger med tokeniserte aktiva. Utredninger av "wholesale" DSP kan også gi nyttig kunnskap om hvordan "retail" DSP kan utformes. Teksten under omhandler "retail" DSP.

Foreløpig er det kun noen få sentralbanker i utviklingsland og fremvoksende økonomier som har innført DSP. Mange sentralbanker utreder DSP, uten å ha tatt stilling til innføring. Flere av dem har utviklet ulike former for prototyper for å få mer kunnskap om ulike teknologiske løsninger og designvalg.

Noen generelle trekk ved utredninger fra sentralbanker i industriland er:

- Det er fokus på DSP brukt ved betalinger, og ikke til verdioppbevaring. Mange sentralbanker vurderer beløpsgrenser og andre friksjoner for å understøtte dette og unngå uheldige konsekvenser knyttet til store og raske flyttinger fra innskudd i private banker til DSP.
- Teknologisk plattform: Sentralbanken står for kjerneinfrastruktur og noen grunnleggende betalingsløsninger. Private (regulerte) aktører utvikler og tilbyr tjenester på toppen.
- Mange ser på ulike tokenbaserte løsninger, men noen ser også på elementer av mer tradisjonell betalingsteknologi.
- Det er fokus på programmerbarhet, eksempelvis at en på forhånd definert hendelse skal utløse betaling. Samtidig ønsker de at alle DSP skal være identiske for mottakere og like fritt kunne gjenbrukes.
- Personvern er et sentralt tema: Betalinger med DSP bør ikke være anonyme, i hvert fall ikke betalinger over et visst beløp, men sentralbank og andre myndigheter skal ikke se persondata.
- Utvikling av «scheme» med regelverk blant annet for hva sentralbanken ønsker at ulike aktører skal og ikke skal gjøre (ansvars- og rolledeling).
- Distribusjonsmodeller og hvordan DSP skal fungere sammen med det øvrige betalingsøkosystemet.
- Hva "basisbetalinger" med DSP skal koste for brukerne og hvordan tilbydere av betalingstjenester skal kunne ta seg betalt og ha insentiver til innovasjon.

Blant sentralbankene i industriland som utreder DSP, kan det synes som Eurosystemet er langt framme. I oktober 2023 besluttet Governing Council i ECB at arbeidet føres videre i en «digital euro preparation phase».

[37] Ifølge en undersøkelse fra BIS i 2022 arbeidet 93 prosent av sentralbankene i et bredt utvalg med DSP på ulike måter. Se Kosse og Mattei (2023). Making headway - Results of the 2022 BIS survey on central bank digital currencies and crypto, BIS Papers No 136. Tilgjengelig her: https://www.bis.org/publ/bppdf/bispap136.htm.

Sentralbankene i Sverige, Storbritannia, USA, Canada, Japan, India, Singapore og Australia er andre sentralbanker som utreder DSP og utvikler "proof of concept", prototyper og/eller piloter for DSP-løsninger. Flere at disse sentralbankene har invitert finansinstitusjoner og andre interessenter i betalingssystemet til referansegrupper for drøfting av ulike forhold ved DSP av betydning for dem. Sentralbankene kan på denne måten få innspill som kan ha betydning for en vellykket innføring av eventuelle DSP-løsninger.

Også internasjonale organisasjoner som IMF og BIS bruker mye ressurser på å analysere ulike problemstillinger knyttet til DSP. Flere BISIH-sentre er etablert for å utrede og eksperimentere med hvordan ny teknologi kan styrke det finansielle systemet. BISIH har flere prosjekter som berører DSP og kan gi nyttig informasjon til vår utredning. Prosjektene *Polaris*, som utreder funksjonalitet for offline-betalinger, og *Icebreaker*, som testet grensekryssende betalinger, er beskrevet over. Videre er Norges Bank observatør i Project *mBridge*[38], og har blant annet fulgt med på Project *Rosalind*.[39] *mBridge* undersøker en felles DSP-infrastruktur og grensekryssende betalinger for flere sentralbanker, mens i *Rosalind* utvikles prototyper for API-er[40] for distribusjon av DSP og "testcaser" for dette drøftes.

5.2 Tester gjennomført av ulike organisasjoner

I tillegg til testingen gjennomført i regi av sentralbanker og BIS skjer det også mye testing i privat regi. Dette gjennomføres både av private aktører med kommersielle interesser i DSP og av organisasjoner som ikke har et rent kommersielt formål. Nedenfor er noen av testene som gjennomføres i privat regi kort beskrevet. Oversikten er ikke uttømmende.

Det er etablert flere organisasjoner som representerer ulike interesser knyttet til utviklingen av DSP. I USA har "The Digital Dollar Project"[41] utgitt en rekke publikasjoner. Tilsvarende finnes "The Digital Pound Foundation"[42] i UK. I EU er "The Digital Euro Association" - DEA[43] etablert som en privat tenketank rundt både offentlige og private (i form av stablecoins) varianter av en digital euro. Et fokusområde for DEA har vært personvernegenskaper knyttet til en digital euro[44] og dette arbeidet har blitt benyttet i Norges Banks testing. Gross et al (2021)[45], som vi har nyttiggjort i den eksperimentelle testingen, springer ut av miljøet rundt DEA. I tilknytning til Gross et al (2021) er det publisert en åpen kildekode[46] som blant kan

[38] https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm
[39] https://www.bis.org/publ/othp69.htm
[40] Application Interface Programming (API) er et grensesnitt for hvordan to eller flere computere/IT-løsninger kan kommunisere med hverandre. I Rosalind gjelder dette kommunikasjon mellom det sentrale DSP-registeret og private leverandører av betalingstjenester til publikum.
[41] https://digitaldollarproject.org/
[42] https://digitalpoundfoundation.com/
[43] https://home.digital-euro-association.de/en
[44] https://blog.digital-euro-association.de/privacy-and-cbdcs-dea-working-group?hsLang=en
[45] J. Gross, J. Sedlmeir, M. Babel, A. Bechtel and B. Schellinger. (2021). Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. Tilgjengelig her: http://dx.doi.org/10.2139/ssrn.3891121
[46] https://github.com/applied-crypto/cbdc

brukes til å teste og validere eksperimentene med anonyme betalinger gjort i Gross et al (2021). Dette ble gjennomført som en del av valideringsarbeidet.

Mange banker og finansinstitusjoner utforsker og gjennomfører tester.
Både Mastercard og Visa har gjennomført tester relatert til DSP. Mastercard har både gjort tester av hvordan DSP kan integreres i Mastercards betalingsnettverk og har utviklet et miljø der sentralbanker kan teste DSP.[47] Visa har blant annet i samarbeid med selskapet Consensys utviklet en løsning for å koble DSP til Visas betalingsnettverk.[48] Både Visa og Mastercard har også gjennomført tester knyttet å integrere blokkjedebaserte løsninger, herunder stablecoins, med sitt betalingsnettverk. Slike tester er også relevante for DSP basert på tilsvarende teknologi.

6. Oppsummering av validering av egenskapene

Nedenfor følger en oppsummering av valideringen av de egenskapene som skulle testes. I tabell 2 over er det også vist hvilke testcaser som dekker hvilke egenskaper.

6.1 Fordring på Norges Bank

DSP skal være en fordring på Norges Bank. Dette innebærer at det er Norges Bank som utsteder DSP, og at DSP står som en passivapost på sentralbankens balanse på linje med sedler og mynt og sentralbankreserver.

Egenskapen “fordring på Norges Bank” er primært av regnskapsrettslig art, og som sådan ikke egnet for teknisk testing. Denne egenskapen er likevel sentral for at DSP skal ha tillit hos publikum. All testing og validering i gruppens arbeid har lagt til grunn at det er Norges Bank som utsteder DSP, og at disse distribueres til bankene. Testingen har vist at denne egenskapen ikke reiser tekniske problemer, og lar seg gjennomføre uten vanskeligheter. Dette gjelder både Norges Banks egen prototype og de øvrige løsningene som arbeidsgruppen har sett på.

Dersom DSP flyttes over fra den blokkjeden som Norges Bank har utstedt DSP på, til en annen blokkjede som drives av andre enn Norges Bank, må det etableres en “bro”, slik det er beskrevet foran. En problemstilling ved bruk av slike broer, er at identifikatorene på den andre blokkjeden ikke er de samme som Norges Bank utstedte. Teknisk sett er det altså et annet token enn det Norges Bank utstedte. Dette tokenet kan kalles “syntetisk” DSP. Hvorvidt denne type syntetisk DSP rettslig sett skal bedømmes som “ekte” DSP, eller som privat utstedte penger, som i denne sammenheng må anses som stablecoins, er et spørsmål som må løses i lovgivning. Vi tar ikke standpunkt til hva som er den beste løsningen her. Vi nevner bare at hvis “syntetisk” DSP skal likestilles med ekte DSP, så må de fortsatt være en fordring på

[47] https://www.mastercard.us/en-us/business/issuers/grow-your-business/crypto/central-bank-digital-currencies.html
[48] https://usa.visa.com/visa-everywhere/blog/bdp/2022/01/13/envisioning-a-future-1642034573970.html

sentralbanken. Ved motsatt løsning vil "syntetisk" DSP være en fordring på det rettssubjektet som er ansvarlig for omveksling fra ekte DSP til det aktuelle tokenet.[49]

6.2 Par verdi mot kontanter og bankinnskudd

DSP skal ha par verdi (1:1) mot bankinnskudd og mot kontanter og andre sentralbankpenger (sentralbankreserver). Fri overføring mellom DSP og bankinnskudd, mellom DSP og reserver og mellom DSP og kontanter antas i de fleste tilfeller å være tilstrekkelig til å sikre paritet. Det kan i ekstreme tilfeller oppstå situasjoner der pariteten kan komme under press, for eksempel der innskyterne er usikre på soliditeten og likviditeten til hele den private banksektoren. Dette gjelder også for kontanter.

Paritetsegenskapen er ikke en egenskap egnet for direkte testing. Paritet forutsetter fri omveksling mellom ulike pengeformer, men omvekslingsfunksjonalitet har ikke vært del av testoppsettet i denne fasen.

6.3 Kunderettet fokus

DSP skal ha et kunderettet fokus. Dette betyr for det første at systemet bør være tilgjengelig for et bredt publikum. For det andre bør systemet være attraktivt nok til å sikre tilstrekkelig bruk.

For å være attraktivt bør DSP kunne brukes i flere ulike betalingssituasjoner, både i fysisk handel, til netthandel og ved overføring mellom privatpersoner. For å sikre tilstrekkelig bruk er det trolig nødvendig enten at tredjeparter utvikler attraktive løsninger eller at DSP-infrastrukturen knyttes opp mot allerede eksisterende betalingsløsninger eller betalingsinstrumenter.

I testfasen er det utviklet et enkelt brukergrensesnitt som gir tilgang mot prototypen. Videreutvikling eller nyutvikling av ulike typer brukergrensesnitt er både mulig og gjennomførbar. I testfasen har vi ikke testet tilknytning mot eksisterende betalingsløsninger eller betalingsinstrumenter og dermed heller ikke mot ulike betalingssituasjoner.

Mange av testcasene som er gjennomført hadde et kunderettet fokus. Dette ettersom det var fokus på økt funksjonalitet og økt effektivitet i betalingssystemet. Eksempler på testcaser som kan sies å ha hatt et kunderettet fokus er prosjekt *Icebreaker* og testene av masseutbetalinger. I tillegg har kontakten med ulike sluttbrukermiljøer gjennom flere hackathons hatt fokus på kunderettede løsninger.

Testene har vist at det er mulig å gjøre DSP tilgjengelig for et bredt publikum. Det er i prinsippet mulig for tredjeparter å utvikle løsninger rettet mot publikum som er attraktive nok til å sikre tilstrekkelig bruk. Men om en eventuell norsk DSP faktisk får tilstrekkelig bruk er avhengig av at banker og andre tredjeparter utvikler effektive og attraktive tjenester basert på DSP.

[49] Problemstillingen er drøftet nærmere i Norges Bank Staff Memo 4/2023.

6.4 Tilstrekkelig friksjon mot bankpenger

Det er fornuftig at et DSP-system designes slik at friksjoner for å begrense uønsket mengde flytting fra bankinnskudd til DSP er mulig. Dette kan blant annet bidra til å redusere virkningene av eventuelle «løp» mot banker og bidra til finansiell stabilitet.

Bruk av volumgrenser og (lav eller negativ) rente er eksempler på friksjoner. Bruk av renter på DSP har vært gjenstand for testing, se testcase G over. Bruk av volumgrenser er også testet i denne fasen, se testcase I over.

Testingen har vist at det er mulig å lage løsninger som kan sørge for tilstrekkelig og ønsket friksjon mot uønsket flytting mellom bankinnskudd og DSP.

6.5 Kontrollert av Norges Bank

Et DSP-system må være kontrollert av Norges Bank. Dette innebærer som et minimum at Norges Bank må ha kontroll på utstedelse og destruksjon av DSP og de grunnleggende egenskapene til DSP-systemet.

I den eksperimentelle testingen validerte vi at det kan utstedes DSP-token innenfor prototypen der Norges Bank har kontroll på utstedelse og destruksjon. Bare Norges Bank kan utstede og destruere DSP. Gjennom å teste ut såkalte “swaps” og “broer” fikk vi testet ut om det var mulig å flytte DSP mellom ulike registre uten at det ga andre aktører mulighet til å utstede og destruere DSP. Det kan likevel tenkes at denne flyttingen av DSP kan være en sårbarhet, som kan åpne for uautorisert utstedelse av DSP. I verste fall kan det eksponere sentralbanken for store økonomiske tap. I tillegg kan slik uautorisert utstedelse og destruksjon true tilliten til systemet, samt reise en rekke rettslige problemstillinger knyttet til ansvar.

Dersom det skal være renter på DSP, vil utbetaling av renter kunne innebære at det må utstedes nye DSP. Eventuell beregning og utbetaling av renter på DSP vil måtte fullautomatiseres. Det vil kunne innebære at DSP utstedes av en smartkontrakt uten direkte involvering av Norges Bank, slik at de rutinene som følges ved ordinær utstedelse av DSP ikke følges. I vårt testcase om renter ble DSP utstedt på denne måten. Konsekvensene for kontroll, herunder sikkerhetsutfordringer ved denne måten å gi renter på, må eventuelt vurderes nærmere.

I prototypen hadde vi kontroll over de grunnleggende egenskapene ved systemet. De grunnleggende egenskapene i DSP-tokens ble programmert inn i kontrakten når DSP ble utstedt og bare Norges Bank kunne utstede DSP-token. Ved å velge et lukket (privat) nettverk hadde vi kontroll med de som hadde tilgang i tillegg til koden som ble brukt og valideringen av transaksjoner.

Bruk av åpen kildekode reiser samtidig spørsmål knyttet til kontroll. Koden og avhengigheter i koden utvikles fortløpende av et “community”. Selv om Norges Bank ikke behøver å benytte modifikasjoner (siste versjon) av koden, kan dette være nødvendig, blant annet på grunn av sikkerhet og interoperabilitet. Slik utvikling kan påvirke egenskapene til systemet og dermed innebære at Norges Bank mister noe av kontrollen over egenskapene. Avhengighet av kode utviklet av tredjeparter og

egenskaper bestemt av tredjeparter blir enda klarere dersom en tillater at DSP flyttes til andre registre gjennom broer, særlig om en tillater at DSP flyttes til registre drevet av private. En vil i slike tilfeller også være avhengig av utviklingsplaner bestemt av andre. Som et eksempel var vi i en av testcasene avhengig av utvikling av en tredjepart for å gjennomføre testcaset.

Overordnet er derfor konklusjonen at bruk av åpen kildekode reiser noen utfordringer når det gjelder kontroll. Videre testing og analyser gjøres for å vurdere om bruk av åpen kildekode gir tilstrekkelig kontroll.

Utgangspunktet for et norsk DSP er at tredjeparter utvikler applikasjoner for bruk av DSP, og slik sett kan oppfylle egenskapen om å være en plattform for innovasjon. Dette kan komme i konflikt med behovet for kontroll. Norges Bank kan legge både teknologiske og regulatoriske føringer for hvilke applikasjoner tredjeparter kan utvikle og kravene til de som utvikler disse. I prototypen var det i utgangspunktet ingen begrensninger i hvordan brukere kunne opprette digitale lommebøker og sende penger mellom disse. Vi har ikke direkte testet hvordan man kan legge begrensninger på å opprette digitale lommebøker, men testcasene knyttet til digital identitet/VC og KYC gjør det mulig å hindre illegitime transaksjoner. Tekniske og regulatoriske virkemidler for å opprettholde kontroll over hvem som kan tilby betalingstjenester i et DSP-system bør utredes videre i en neste fase for å finne riktige avveininger og mekanismer mellom kontroll og innovasjon av tredjeparter.

6.6 Kan fungere som tvungent betalingsmiddel

At DSP skal kunne fungere som tvungent betalingsmiddel, er primært en rettslig egenskap i den forstand at DSP i lov må likestilles med sedler og mynter utstedt av sentralbanken. Denne siden av egenskapen er ikke gjenstand for teknisk testing.

Dersom DSP skal kunne fungere som tvungent betalingsmiddel i praksis, må det likevel stilles krav om at DSP dels er lett tilgjengelig, og dels er lett å betale med for sluttbruker i praktiske situasjoner. Den tekniske testingen har vist at DSP enkelt lar seg distribuere fra Norges Bank til bankene. Testingen har videre vist at DSP lar seg distribuere videre fra bankene til sluttbrukeres elektroniske lommebok, se testcase B foran, også i form av massebetalinger, se testcase D foran. Testingen har derfor vist at DSP kan være lett tilgjengelig for sluttbrukere (som har egnet lommebok). Testingen av prototypen har imidlertid ikke tatt hensyn til at betalinger med DSP skal være brukervennlige for alle grupper av sluttbrukere. I det hele tatt har brukervennlighet og “kundereisen” vært en mindre del av testingen. Testingen har derfor ikke fullt ut verifisert at DSP som tvungent betalingsmiddel vil fungere i praksis som et brukervennlig betalingsmiddel. Brukervennlighet vil derfor være en sentral egenskap å utvikle i neste fase av prosjektet.

6.7 Samsvar med EØS-forpliktelser

Denne egenskapen sikter først og fremst til to regelsett: hvitvaskingsreglene og GDPR. Testingen av Norges Banks egen prototype har vist at identiteten til en bruker av DSP kan verifiseres av betalingsmottaker. Dels har dette blitt gjort gjennom egen identifikasjonsløsning som legges i tokenet, dels gjennom VC-løsningen i samarbeid med Digdir. Det er fortsatt mange utestående spørsmål som

gjelder regulatorisk ansvar for transaksjonskontroll, men det kan legges til grunn at det kan etableres tilfredsstillende løsninger for identitetskontroll.

Det er ennå ikke bestemt hvilke personopplysninger som blir lagret ved bruk av DSP, hvor disse opplysningene skal lagres, eller hvilke sikkerhetsløsninger som vil være tilfredsstillende. Testingen av aliasbasen har vist at opplysninger om eier av lommebok med navn, personnummer og mobiltelefonnummer kan lagres på en sikker måte, og at feilbetalinger kan unngås. Løsningen med en database (MYSQL) på en server utenfor blokkjeden, innebærer dessuten at kundens bankforbindelse kan gjennomføre kundekontrolltiltak etter hvitvaskingslovgivningen.

Dersom borgere i andre EØS-land utenfor Norge ikke får tilgang til betalingsløsninger for DSP, kan det potensielt utfordre bestemmelsene om de fire friheter i EØS-avtalen del II og del III. Slike problemstillinger er verken testet eller vurdert. Vi vil likevel vise til at vi gjennom Prosjekt *Icebreaker* har testet at grensekryssende DSP-betalinger lar seg gjennomføre.

6.8 Betalinger umiddelbare og endelige

Egenskapen knyttet til at betalinger skal være umiddelbare og endelige er godt testet gjennom protypen. Brukerne av løsningen vil umiddelbart motta pengene når transaksjonen er gjennomført, og det er ikke noe mellomledd når samme register benyttes. Slik sett vil også betalingen være endelig når den er validert og oppdatering av registeret er gjennomført. Kryptografien som benyttes for å sikre registeret vil hindre uautorisert endring og dermed sørge for at integritet ivaretas.

Overføring av penger fra en valuta til en annen er validert gjennom bruk av tredjeparter som sørger for veksling. Ved betaling vil midlene først låses i avsenders valuta. Tredjeparten som foretar veksling vil deretter automatisk overføre et beløp til sluttmottaker basert på avtalt vekslingskurs. Når mottaker mottar beløpet, vil samtidig pengene fra avsender frigjøres til tredjeparten ansvarlig for veksling. Også her benyttes kryptografi i de ulike registrene for å sikre integritet (endelighet). Testene i prosjekt *Icebreaker* som omtalt foran er et eksempel som forklarer dette i detalj.

6.9 Samsvar med gode IT-arkitekturprinsipper

Samsvar med gode IT-arkitekturprinsipper er en egenskap som favner bredt. Arbeidet med prototypen har vært drevet av behov knyttet til den eksperimentelle testingen og det er gjort en rekke forenklinger med hensyn til en helhetlig og sikker arkitektur. Likevel har arbeidet adressert flere områder som er relevante og i samsvar med gode arkitekturprinsipper.

Interoperabilitet er et viktig aspekt som har blitt adressert gjennom test av ulike type broer for å utveksle DSP mot register og løsninger som benytter en annen teknologi enn Norges Banks prototype. Det har blitt gjennomført vellykkede tester for grensekryssende betalinger og mot et nettverk for tingenes internett for simulert kjøp og salg av strøm. I tillegg har det blitt gjennomført vellykkede tester mot sentrale register for identitet (Id-porten). En forutsetning for interoperabilitet er bruk av standarder og at standardene har et tilstrekkelig gjennomslag i markedet. I valideringsarbeidet er det benyttet standarder som eksempelvis ERC-20, som for

tiden har et godt gjennomslag i markedet. Det er imidlertid viktig å følge med på utviklingen og spesielt hvilke eventuelle valg store aktører som eksempelvis store sentralbanker tar.

Et annet viktig arkitekturprinsipp er at løsningene skal ha høy sikkerhet. Dette oppnås gjennom sikkerhet i dybden, hvor flere lag med sikkerhet sørger for økt motstandskraft mot uautorisert tilgang og cyberangrep. I arbeidet med prototypen er det gjort forenklinger på dette området, og det er en rekke tiltak og forbedringer som må gjennomføres før en løsning er produksjonsklar. Dette går blant annet på tiltak for å forhindre kompromittering og tiltak for å oppdage og håndtere forsøk på kompromittering. Vurderingen er likevel at grunnteknologien som benyttes har et potensiale for å oppnå tilstrekkelig motstandsdyktighet og sikkerhetsnivå ved rett implementering. Teknologien er i aktiv bruk i markedet og det er gjennomført sikkerhetsvurderinger av denne.

Personvern er et annet aspekt knyttet til sikkerhet. I prototypen er registeret tilgjengelig for alle deltakere og alle kan se alt. Dette innebærer at registeret viser alle transaksjoner som er gjennomført med beløp. Transaksjonene skjer mellom digitale lommebøker som identifiseres med lange tekststrenger. Slik sett vil det ikke være en direkte kobling til personen som eier lommebøkene, men dette vil kunne utledes etter hvert som betalinger gjennomføres. Som nevnt vil det også være en balanse mellom personvern og bankenes behov for å oppfylle krav til KYC og AML/CFT.

Brukervennlighet og «kundereisen» er viktig for at et DSP-system skal være attraktivt, men som nevnt tidligere har dette av kapasitetsgrunner blitt nedprioritert i arbeidet med prototypen. Ved eventuell innføring av DSP er det viktig at også krav til universell utforming ivaretas for å blant annet sikre tilgjengelighet for personer med funksjonshemminger. En kan for eksempel teste om betalinger med wallets i prototypen er gjennomførbare med tilgjengelige løsninger for personer med funksjonshemminger.

Det er en rekke andre aspekter knyttet til arkitekturprinsipper som er adressert gjennom arbeidet i fase 4. Bruk av åpen kildekode og offentlig tilgjengeliggjøring av Norges Banks kildekode har vært et virkemiddel for å forenkle arbeidet med innovasjon. På denne måten er det lagt til rette for at flere kan bidra i arbeidet og bygge videre på prototypen, eksempelvis gjennom hackathons. Tilnærmingen valgt for arbeidet med prototypen har også avdekket noen svakheter med hensyn til drift og forvaltning av løsningen, blant annet ved at registeret ved enkelte endringer burde nullstilles. Drift og forvaltning er aspekter som må få et større fokus i arbeid med en eventuell løsning som kan settes i produksjon.

Modularitet er viktig for fremtidens IT-løsninger, også for DSP. Muligheten til å bytte ut komponenter som fungerer dårlig med nye som fungerer bedre er ikke testet. Det kan være gjenstand for tester i det videre arbeidet med DSP.

6.10 Teknisk uavhengighet og mulighet for offline-betalinger

DSP-systemet bør kunne fungere tilstrekkelig uavhengig av bankenes betalingssystemer for å sikre betalingsberedskap.

I testprototypen legges det til rette for at transaksjoner skjer direkte mellom sluttbrukerne, uten å gå via banker. Prototypen legger også til rette for at myndighetene eller Norges Bank kan overføre DSP direkte til husholdninger eller foretak (med digitale lommebøker for DSP) i beredskapssituasjoner der bankenes systemer er nede.

I en fullverdig løsning vil det imidlertid måtte være en sterkere tilknytning til andre systemer, både ved at omvekslingen og overføring mellom bankinnskudd og DSP ikke er mulig å gjøre uavhengig av bankenes systemer og ved at bruken av DSP skjer gjennom andre aktørers løsninger. En løsning der flere uavhengige tredjeparter tilbyr løsninger for sluttbrukere på toppen av Norges Banks kjerneinfrastruktur, vil kunne sikre beredskap selv om ikke kravet om teknisk uavhengighet innfris i bokstavelig forstand. Det kan også tenkes at Norges Bank selv utvikler og drifter en teknisk uavhengig minimumsløsning for sluttbrukerne til bruk i spesielle situasjoner. Det er ikke utviklet eller testet en slik løsning i denne fasen.

Det er mange aspekter ved teknisk uavhengighet som ikke er spesielt velegnet for direkte testing. Uavhengighet vil i større grad være et resultat av hvordan systemet designes og konstrueres.

Offline-funksjonalitet
En offline-betaling kan defineres som en betaling direkte mellom sluttbrukere og deres betalingsinstrumenter i situasjoner der det ikke er kontakt mellom registeret eller kontosystemet og brukergrensesnittet. Midlene må da lagres lokalt og overføringen mellom brukerne vil skje på nær avstand. Offline-betalinger er ikke omfattende testet og problemstillingene knyttet til egenskapen er derfor ikke tilstrekkelig verifisert gjennom testing. Deltagere fra VG deltok på workshops med BISIH Nordic Centre i forbindelse med prosjekt *Polaris* i Stockholm hvor ulike leverandører av offline-løsninger fikk mulighet til å presentere sine løsninger. Dette ga Norges Bank verdifulle innspill om offline-funksjonalitet. Ikke minst ga det informasjon om utredning av mange ulike løsninger basert på helt ulik teknologi. Utviklingen av en felles standard for slike offline-betalinger er ennå ikke nådd.

6.11 Kundekommunikasjon og -kontroll foretas av tredjeparter

Prosjektet har lagt til grunn at det også i fremtiden vil være bankene som vil være ansvarlige for KYC og “onboarding” av nye kunder, på samme måte som de i dag er ansvarlige for KYC/AML/CFT-funksjonene. Utføring av slike funksjoner kan medføre merarbeider og merkostnader for bankene, noe det bør finnes en god forretningsmodell for. De som i fremtiden eventuelt tilbyr digitale lommebøker og betalingstjenester basert på DSP, kan inkludere andre typer aktører enn banker, forutsatt tilstrekkelig autorisasjon, regulering og tilsyn.

Både vår egen prototype og andre sentralbankers test av DSP har vist at det er mulig å designe en DSP-arkitektur som gir tilfredsstillende KYC.

6.12 Fleksibilitet for ulike personvernløsninger

Det er et mål at DSP skal være robust for ulike krav til personvern og samtidig kunne oppfylle regulatoriske krav som skal oppfylle etterlevelse og kontroll. Personvern er et overgripende samfunnshensyn og DSP må være i samsvar med de avveiningene som gjøres av myndigheter, herunder i samsvar med EU-regelverk slik som GDPR.

Flere av testene vi har gjennomført har belyst mulighetsrommet for å gjennomføre betalinger med høy grad av personvern (opp til full anonymitet) og samtidig sørge for regulatorisk etterlevelse. Vi har testet en åpen kildekode fra den akademiske litteraturen for å gjennomføre anonyme betalinger[50]. Vi har også, som et testcase, undersøkt hvordan eksisterende tjenester for anonymisering av betalinger kan benyttes i vår prototype, herunder hvordan dette kan kombineres med regulatorisk etterlevelse. Personvern og etterlevelse har også blitt belyst i hackathons/ideathons vi har vært med på å arrangere. Vi har også testet VC som kan være en viktig komponent for personvernløsninger.

Testingen har vist at teknologien vi har benyttet i prototypen gir høy grad av robusthet for ulike grader av personvern og ulike opplegg for regulatorisk etterlevelse.

Uansett utgangspunkt er det viktig å finne tekniske løsninger som er fleksible for ulike krav og ønsker både nå og i fremtiden. Samfunnets behov endres, og nye teknologier gir nye muligheter.

Gjennom testene som er gjort har vi vist at det er mulig å finne fleksibilitet for ulike personvernløsninger.

6.13 Plattform for tredjepartstilbydere

I flere rapporter (Norges Bank Memo 2/2019 og 1/2021) har denne egenskapen blitt diskutert som en viktig innovasjonsforutsetning for DSP. Flere øvelser i denne fasen har indikert at prototypen/sandkassen kan benyttes som en plattform for tredjepartstilbydere.

Dette ble synliggjort i hackathon med Digdir (del 2). Det var påmeldt 11 grupper som hadde utviklet innovative løsninger (testcaser) i vår sandkasse/prototype. Testcasene ble presentert av et bredt spektrum av private og offentlige aktører. Testcasene viste i forskjellige dimensjoner hvordan tredjepartstilbydere kan tilby tjenester og produkter til samfunnet ved å integrere tilbudet med DSP- prototypen. I et testcase ble offline-kapabiliteten av DSP testet. I andre testcaser fungerte DSP som oppgjørsmiddel (noen eksempler: eierskapshåndtering i sanntid via smartkontrakter, utbetaling til midlertidige arbeidere i Norge, bruk av digitale lommebøker til utbetalinger i flere andre testcaser og oppgjør i egenutviklet spill). I tillegg var det eksempler på løsninger på toppen av DSP som personalisering av DSP, bruk av M2M-teknologi og klimabevisstgjøring.

[50] Gross et al. (2021).

Interoperabilitet er en viktig forutsetning for å kunne tilrettelegge for innovasjon. Interoperabilitet ble testet i flere spor i denne fasen. Et eksempel er testen av bro i testcase C. Et annet eksempel er *Icebreaker*-prosjektet.

I testarbeidet i denne fasen ble det lagt vekt på å teste ut mulighetsrommet for hvordan DSP kan være en plattform for tredjepartstilbydere. I det fremtidige arbeidet med testing bør det også legges vekt på forretningsmodeller og regulatoriske rammebetingelser som gir tredjeparter insentiver til slik utvikling.

6.14 Ivareta gjennomslaget av pengepolitikken

I tillegg til den eksperimentelle testingen som beskrives her, ble det også gjennomført et eget analytisk arbeid i delprosjektet «DSP - konsekvenser for likviditetsstyringen og pengepolitikken», se Bernhardsen og Kloster (2023).

I den eksperimentelle testingen har vi gjennom programmerbarhet testet renter og beløpsgrenser som kan bidra til at DSP ikke får et så stort omfang at det kan true gjennomslaget av pengepolitikken.

6.15 Relevant informasjon i NBs makroøkonomiske overvåking

I de nåværende DSP-prototypene er det mulig å spore transaksjoner i sanntid, samtidig som det er mulig å få tilgang til historikken av transaksjonene. Likevel er det til nå ikke definert flere roller i de forskjellige brukere (dvs. alle brukere har de samme rettighetene, unntatt Norges Bank). Dersom aktører får ulike roller i systemet, slik at det er mulig å analysere brukermønstre, vil DSP kunne gi ytterligere makroøkonomisk informasjon. Dette kan eventuelt inngå i ytterligere testarbeid.

Med makroøkonomisk overvåkning i denne sammenheng er det en forutsetning at personvernet er ivaretatt. Det har blitt testet en egen database «off-chain» med privat informasjon som viser muligheten til knytning av nåværende register (med alias) med et offentlig register (med ID som knyttes til alias). Slik «dekobling» av informasjon kan muliggjøre personvern i makroøkonomisk overvåking. Ulike kryptografiteknikker kan også benyttes for å hindre at DSP-bruk i den makroøkonomiske overvåkingen avslører personopplysninger. Dette kan eventuelt testes videre.

6.16 DLT-kompatibelt

Prototypen vi har testet er basert på DLT-teknologi og er dermed i seg selv DLT-kompatibel. Bruk av ulike elementer av DLT-teknologi er et kjennetegn for testing av DSP-systemer rundt om i verden.

Bruk av DLT-teknologi i prototypen gjør den også delvis kompatibel med andre DLT-baserte systemer. Dette muliggjøres blant annet ved at DSP i prototypen kan låses i såkalte HTLC slik at det bare kan låses opp igjen dersom visse vilkår er oppfylt. Dette har vært brukt i såkalte broer for å flytte DSP mellom ulike registre og var

også sentralt i gjennomføringen av testen for betalinger på tvers av nasjonale DSP-systemer (prosjekt *Icebreaker*).

Bruk av DLT-teknologi bør også stå sentralt i det videre testarbeidet, blant annet fordi dette er sentralt for såkalt tokenisering. For Norges Banks prosjektfase 4 var DLT-kapabilitet en forutsetning for å kunne delta i *Icebreaker*-prosjektet nevnt tidligere. Det kan også tenkes at DLT-kompabilitet blir en forutsetning for at eventuelle norske DSP skal være interoperable med andre lands DSP.

6.17 Attraktiv nisjeløsning

DSP skal også kunne fungere som en nisjeløsning, dvs. oppfylle særskilte betalingsbehov for brukerne.

I denne fasen ble funksjonalitet for masseutbetalinger utviklet og testet ut. Aktuelle testcaser for en slik massutbetaling kan være betalinger fra offentlige aktører som for eksempel skattemyndigheter og NAV.

Et annet testcase som kan sies å være en nisje, var *Icebreaker*-prosjektet som dokumenterte grensekryssende betalinger som kan være raskere, billigere og bedre enn dagens løsninger.

Andre nisjeløsninger, som ikke ble testet, kan være “atomiske” transaksjoner slik som betaling ved levering (såkalt «delivery versus payment», DvP), i form av en betaling som gjennomføres automatisk når en avtalt hendelse inntreffer.

7. Oppsummering og veien videre

Oppsummering
Prosjektgruppens overordnede vurdering er at den eksperimentelle testingen har vært vellykket, gitt tiden og ressursene som var til rådighet i denne prosjektfasen. Gjennom den eksperimentelle testingen har vi fått belyst hvordan tekniske løsninger kan oppfylle egenskapene DSP må ha. Testarbeidet har også belyst nødvendige avveininger. For eksempel kan Norges Banks behov for kontroll legge begrensninger på private aktørers muligheter til å utvikle innovative løsninger. Den eksperimentelle testingen har i tillegg belyst juridiske, økonomiske og regulatoriske sider. Blant annet har ulike måter å organisere såkalte broer på betydning for hvordan DSP fortsatt kan være en fordring på Norges Bank. Gjennom mange av testcasene har vi bare delvis fått validert hvordan teknologiene kan oppfylle egenskapene. Fortsatt testing er derfor nødvendig for å kunne gi et bedre faktabasert beslutningsgrunnlag for en endelig anbefaling.

Begrensinger i testingen
Tema for den eksperimentelle testingen har vært å teste ut mulighetsrommet til teknologi. Det innebærer at testene har vært gjennomført i begrenset skala på “forenklede” infrastrukturer. Det innebærer at det blant annet ikke er gjennomført såkalt ytelsestesting på for eksempel kapasitetsgrenser. Videre er det lagt til grunn en “happy path” der det er ikke lagt vekt på ha gode løsninger som tar høyde for at brukerne tilsiktet eller utilsiktet bruker teknologien feil. Prototypene er heller ikke

utviklet med tanke på å kunne oppfylle sikkerhetskrav som et DSP-system må oppfylle.

Integrasjon med eksisterende infrastruktur
Ved oppstart av fase 4 ble det valgt å la prototypen/sandkassen være en "stand alone"-løsning. Det medførte at det ikke ble testet at bankene får tilført DSP i en to-lags arkitektur ved trekk på sentralbankreserver, slik det muligens ville være i produksjon. Det ble heller ikke stilt noe ønske til deltagende banker om at bankkunder fikk DSP ved trekk på innskuddskonto.

Det er heller ikke utviklet regelverk, insentivstrukturer og forretningsmodeller for tredjeparters deltakelse i systemet, og tester i denne sammenheng. For eksempel er det ikke testet om banker eller andre aktører kan insentiveres til deltakelse ved å få en andel av gebyrer eller liknende. Det kan gjøres i neste fase. Det innebærer at det i neste fase bør utvikles testcaser som belyser ulike insentivstrukturer.

Den eksperimentelle testingen omfattet ikke testing av en helhetlig infrastruktur som kan benyttes for DSP i Norge. Den eksperimentelle testingen har likevel ytterligere belyst hvordan en helhetlig arkitektur potensielt kan se ut.

En lærdom fra testingen er at ulike registre har ulike egenskaper som i ulik grad er egnet til å oppfylle egenskapene en DSP må ha. For eksempel har en kontobasert løsning, slik som i Hyperledger Besu og ERC-20 token, gode forutsetninger for å tilby programmerbarhet. Programmerbarhet har vært sentralt for å kunne gjennomføre flere av testcasene og har også vært sentralt for mange caser som ble utviklet i forbindelse med idemyldring/hackathon. For bruksområder som ikke krever programmerbare penger eller bare krever begrensede programmeringsfunksjoner, kan såkalt UTXO token-løsninger være mer effektive.

En annen lærdom var at en Ethereum-teknologi som Hyperledger Besu gjør det enklere å tiltrekke seg innovasjon og nye løsninger, spesielt i en eksperimentell test, ettersom det i Norge og internasjonalt finnes et stort antall programmerere med god erfaring og kompetanse.

Ulike registerløsninger kan derfor ha ulike fordeler og ulemper i flere dimensjoner:

- Representasjon av penger.
- Programmerbarhet.
- Rollefordeling og desentralisering.

Broer innebærer at DSP flyttes fra et register til et annet separat register. Dette kan omfattes som en "side-chain". Et alternativ til "side-chains" er å benytte L2 som innebærer at det legges et nytt register på "toppen" av DSP-kjerneregisteret. En mulighet med en L2 er at denne kan knyttes tettere til kjerneregisteret og det kan være lettere å gjenbruke noe av den sikkerheten som allerede ligger i kjerneregisteret. L2 og "side-chains" utelukker ikke hverandre og det kan av og til være en flytende grense mellom dem. Både "broer" og L2 kan potensielt testes nærmere i neste fase.

Veien videre
Forslag til formål og plan for fase 5 er nærmere beskrevet i Norges Bank Memo 2/2023 med sluttrapporten fra fase 4.

Norges Bank
Norges Bank Memo

Oslo 2023

Adresse: Bankplassen 2
Post: Postboks 1179 Sentrum, 0107 Oslo
Telefon: 22 31 60 00
E-post: post@norges-bank.no
www.norges-bank.no

ISSN 1894-0277 (online)
ISBN 978-82-8379-292-8 (online)