Utgave 2

1.Juni 2018

DISTRIBUERTE NYHETER

NOEN SENTRALBANKER MED BLOCKCHAIN/DLT PROSJEKTER

Dette dokumentet er skrevet av Lasse Meholm og representerer mine private meninger, og analyser og ikke nødvendigvis de selskaper jeg arbeider i eller for.

Det meste av det som står her finnes også på bloggen min www.finansit.no/blogg men her finne noe mer tekst og flere bilder.

DISTRIBUERTE NYHETER

NOEN SENTRALBANKER MED BLOCKCHAIN/DLT PROSJEKTER

INNHOLD

Noen DLT prosjekter gjort av sentralbanker. 2
Prosjekt Stella (ECB og BOJ) 2
Banco Central do Brasil 3
Project Ubin – Singapore 4
Prosjekt Jasper (Canada) 6
Bank of England (BoE) 8
BIS (Bank for International Settlements) 13

SENTRAL-BANKER OG DLT

Her følger noe korte oppsummering av noe få prosjekter gjennomført av ulike sentralbanker. Jeg har lest tilgjengelig offentlig informasjon om disse prosjektene, anslagsvis 300 sider dokumenter.

NOEN DLT PROSJEKTER GJORT AV SENTRALBANKER.

Her følger noe korte oppsummering av noe få prosjekter gjennomført av ulike sentralbanker. Jeg har lest tilgjengelig offentlig informasjon om disse prosjektene, anslagsvis 300 sider dokumenter.

PROSJEKT STELLA (ECB OG BOJ)

Prosjekt Stella ble startet desember 2016 i fellesskap av ECB (European Central Bank) og BOJ (Bank of Japan, Japans sentralbank). Mens ECB benyttet lokalt installert hardware, benyttet BOJ skybasert hardware. I testen ble det benyttet transaksjonsvolumer fra virkeligheten for disse to markedet, mellom 10 og 70 transaksjoner i sekundet (RPS- Requests Per Second). Basis var også straks betalinger basert på Real-Time Gross Settlement (RTGS). Dette var i stor grad en teknisk test av stabilitet og betalingshastighet, og i mindre grad en test av makroøkonomi og utstedelse av krypto valuta.

Det ble testet transaksjonsvolumer opp mot 250 transaksjoner i sekundet, noe som medførte utfordringer som ikke ble løst i testen. Det ble også oppdaget at antall noder reduserte betalingshastigheten, opp mot 65 noder reduserer hastigheten med 0,2 sekund i forhold til 4 noder. Også den fysiske avstanden mellom nodene har betydning for betalingshastigheten, for eksempel innenfor Japan rundt 0,6 sekunder i snitt, mens en betaling fra Frankfurt i Europa til Osaka i Japan tok 1,5 sekunder.

Både ECB og BOJ er ansvarlig for RTGS oppgjør i sine markeder. ECB benytter TARGET2 systemet som opereres av Eurosystem, og behandler daglig rundt 350 000 transaksjoner for 1,8 milliarder Euro. TARGET2 kjører i tandem på to separate datasentre i Europe for redundans og backup, som skifter hver 6. måned. BOJ kjører BOJ-NET systemet selv og behandler daglig 70 000 transaksjoner for 1,1 milliarder Euro. BOJ-NET systemer kjøres lokalt av BOJ, men de har en back-up fasilitet utenfor Japan. Begge har Liquidity Saving Mechanisme (LSM) funksjonalitet.

Testen ble gjennomført med Hyperledger Fabric 0.6.1 som benytter Practical Byzantine Fault Totelance (PBFT) konsensus mekanisme. Hele transaksjons historikk er desentral hvor hver node har hele historikken. Det ble benyttet smart kontrakter i gjennomføring av hver betaling.

Det ble test hva som skjer dersom en node får avbrudd (faller ut). Det har ingen virkning på stabiliteten i nettverket selv om mange noder faller ut, og når nodene igjen er i operasjon tar det opp mot 30 sekunder før de har synkronisert databasen og er operative igjen, noe Hyperledger Fabric sørger for.

Fabric har en sentral CA (Certificate Authority), noe som introduserer en Single Point of Failure (SPOF). Det som skjedde når CA var satt ut av drift var at alle transaksjoner ble avviste. Når CA igjen kom i drift var systemet opp igjen, uten at andre funksjoner måtte omstarte.

Det ble også testet hva som skjer dersom inputdata inneholder feil i formatet. Smart kontraktene løser dette glimrende, selv om opp mot 80 % av alle transaksjoner har feil i formatet. Smart kontraktene var programmert med en feil-oppdagelse-mekanisme som automatisk rettet feil. En erfaring var at dersom andelen input transaksjoner med feil var stor, krevde nettverket mer prosessorkapasitet for å beholde hastigheten.

Konklusjonen er at DLT kan benyttes til betalinger og det planlegges nye prosjekter.

BANCO CENTRAL DO BRASIL

Prosjektet ble gjennomført siste halvdel av 2016 og første halvår 2017. FEBRABN (Brazilian Federation of banks) deltok i prosjektet. Prosjektet hentet lærdom fra andre prosjekter ved starten, som prosjekt Ubin (Singapore), Emerald (Skotland) og Jasper (Canada). Sentralbanken vurderte flere user cases, og valgte til slutt SALT systemet som prosjekt for å teste DLT. SALT (System for Transaction Settlement) er et backup system basert på RTGS (straks betaling) dersom hovedsystemet for oppgjør svikter. Brasil har tett teknisk integrasjon med straks betalinger til noen av sine naboland.

Det var en del forutsetninger ved starten:

- Ingen wallet kunne ha negativ balanse
- Ingen deltager kan se andre deltageres balanse i wallet
- Sentralbanken skal kunne se alle transaksjoner og få informasjon om alle sin balanse
- Nettverket skal kunne fungere både med og uten sentralbank som aktiv deltager
- Når dagen starter skaper sentralbanken en mengde kryptopenger, det kan ikke skaper mer kryptopenger i løpet av dagen, og alle kryptopenger skal veksles tilbake til sentralbank penger på slutten av dagen
- Private (permissioned) nettverk

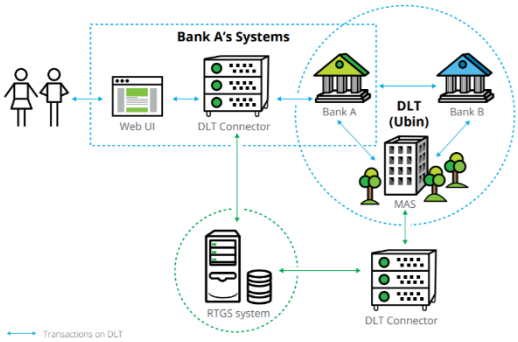
Det ble besluttet å basere seg i fase 1 en på Ethereum teknologien, og bruk av «BlockApps» en utvikler plattform i Ethereum. BlockApps har noen gode API'er som teamet fant veldig brukervennlige. De bygget smartkontraktene i Solidity. Sentralbanken bygget også en monitor panel, slik at de enkelt kunne holde oversikt over balansen til hver enkelt deltager.

En utfordring med BlockApps er privat informasjon, ettersom alt er tilgjengelig for alle i Ethereum. Det ble testet ulike løsninger fra ulike leverandører, men en god løsning ble ikke funnet i løpet av testen.

Det ble besluttet å starte fase to med Hyperledger Fabric 0.6.1 og Corda. Fabric 0.6.1 fungerte bedre men kom helle ikke helt i mål angående privat informasjon. Det er opplyst at Fabric versjon 1 er forbedret med hensyn på dette, noe teamet ikke fikk tid til å teste. Corda viste seg å være umodent og ikke tilpasset betalinger, i henhold til hva dette teamet opplevde. Corda sporet ble fort lagt bort av utviklingsteamet. I tillegg innfører Corda flere «single point of failure» og økt risiko. En faktor er at bare de nodene som er deltager i transaksjoner har sin egen hele transaksjonsrisiko, noe som medfører at back-up og disaster recovery er en utfordring (ikke distribuert databaser). Det må innføres en notarius for å få konsensus, som er en «singe point of failure». I tillegg ble det reist tvil om Corda hadde god nok støtte for «double spending» problemet. Den siste teknologien som ble testet var Quorum, som er en Ethereum plattform. Denne siste teknologien ga det beste resultatet, med unntak at det ble reist spørsmål rundt double spending. Private informasjon var løst, delvis som en off-chain registrering av ID kryptert. Zerocoin Electric Coin Company og JP Morgan videreutvikler Quorum plattformen for å løse disse siste delene.

PROJECT UBIN – SINGAPORE

Figure 10: High-level architecture of Project Ubin



Prosjekt Ubin startet november 2016 med sentralbanken i Singapore, MAS (finanstilsynet i Singapore), Bank of America Merrill Lynch, BCS Information system, Credit Suisse, DNB Bank ltd, HSBC, J.P.Morgan, Mitchibushi UFJ Financial Group, OCBC Bank, R3, Singapore bank, Overseas bank og Deloitte. Hensikten var å test hvordan tokens (kryptovaluta) kan forbedre det finansielle systemet i Singapore. Dagens system for oppgjør kjøres av MAS og er basert på straks betalinger, brutto bilateralt oppgjør (RTGS) og heter MEPS+ (MAS Electronic Payment System og er basert på SWIFT protokoller. Utgangspunktet var å bevise følgende karakteristika ved DLT som 1) oprasjonell forenkling 2)bedre effektivitet for reguleringsmyndigheter 3)redusering av motpartsrisiko 4)redusere tid ved oppgjør 5)likviditet og kapital forbedringer 6)redusere sannsynlighet for bedrageri. På generell basis har Singapore ønske om å ta en ledende posisjon i verden på DLT. Prosjektet ble delt i to spor, et for teknisk gjennomføring og et for makroøkonomisk gjennomføring. Hver deltagende bank har to konti, en for Singapore dollar (CA) og en annen for krypto dollar (BCA). Testen ble gjennomført i Ethereum.

Prosessen var som følger:

Dagen starter med at alle tre bankene A, B og C har 100 dollar i sin konto i sentralbanken. Bank A konverterer 10 dollar til kryptodollar, Bank B konverterer 20 dollar til kryptodollar og bank C konverterer 30 dollar til Kryptodollar i sentralbanken, til sammen 60 kryptodollar. Dette gjøres i smart kontrakter. Kryptovalutaen ble kalt «digital SGD»

Start of day – Pledge (batch process)

Before				Step 1				Step 2			
MEPS+		DL		MEPS+		DL		MEPS+		DL	
Bank A RTGS	100	Bank A	0	Bank A RTGS	**90**	Bank A	0	Bank A RTGS	90	Bank A	**10**
Bank B RTGS	100	Bank B	0	Bank B RTGS	**80**	Bank B	0	Bank B RTGS	80	Bank B	**20**
Bank C RTGS	100	Bank C	0	Bank C RTGS	**70**	Bank C	0	Bank C RTGS	70	Bank C	**30**
Omnibus collateral	0	Central Bank	0	Omnibus collateral	**60**	Central Bank	**60**	Omnibus collateral	60	Central Bank	**0**

Bank A betaler 5 kryptodollar til Bank B, og bank B betaler 15 kryptodollar til bank C i løpet av dagen. Da ender vi opp i en situasjon hvor bank A har 5 kryptodollar, bank B 15 kryptodollar og bank C 40 kryptodollar. På slutten av dagen (når testen for i dag avsluttes) veksler bank A inn sine 5, bank B inn sine 15 og bank C inn sine 40 kryptodollar til Singapore dollar. Sentralbanken betaler ut de 60 Singapore dollar som ble hentet inn ved starten av dagen og holdt som garanti for utstedelse av kryptodollar. Sentralbanken kan ikke dele ut mer kryptodollar enn hver bank har på karantikonto i sentralbanken.

End of day – Redeem (batch process)											
Before				Step 1				Step 2			
MEPS+		DL		MEPS+		DL		MEPS+		DL	
Bank A RTGS	90	Bank A	5	Bank A RTGS	90	Bank A	0	Bank A RTGS	95	Bank A	0
Bank B RTGS	80	Bank B	15	Bank B RTGS	80	Bank B	0	Bank B RTGS	95	Bank B	0
Bank C RTGS	70	Bank C	40	Bank C RTGS	70	Bank C	0	Bank C RTGS	110	Bank C	0
Omnibus collateral	60	Central Bank	0	Omnibus collateral	60	Central Bank	60	Omnibus collateral	0	Central Bank	0

Prosjektet benyttet Ethereum, MQ Client, common payment gateway (CPG) som teknologi og utviklet interface mot RTGS systemet MEPS+ ved hjelp av smart kontrakter og tradisjonell teknologi. Ettersom det var sentralbanken som utsteder krypto pengene hadde bankene en fordring på sentralbanken for de kryptopenger som ble utstedt, bankene hadde dermed ingen kredit risiko – noe som krever en del advokat arbeide å gjennomføre i praksis. Ved en senere fase kan det vurderes at bankene låner kryptodollar av hverandre.

Ettersom betalingen ble gjort basert på atomic gross payment er det ingen likviditetsrisiko. Selv om en av bankene skulle gå konkurs vil det ikke berøre de andre og flyten av penger vil fortsette mellom restene av bankene, ettersom det distribuerte nettverket fortsatt fungerte. I DLT er det ingen penger «i bevegelse» slik som ved tradisjonell teknologi.

Figure 15: Observations

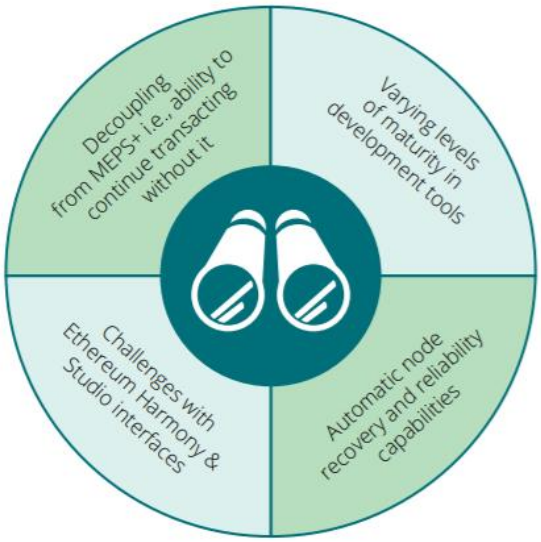


Figure 16: Lessons learnt

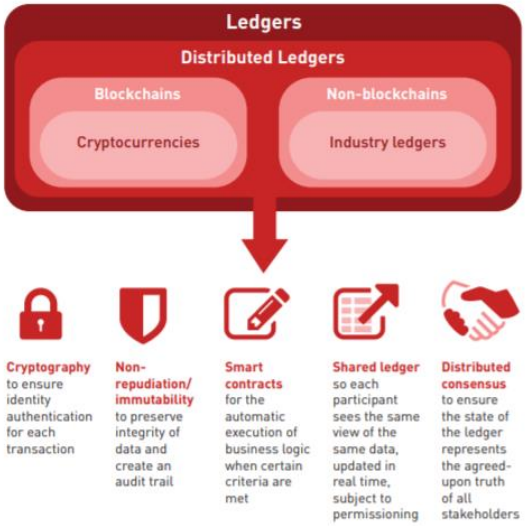
PROSJEKT JASPER (CANADA)

Prosjekt Jasper ble lansert mars 2016 med fase 1 med deltagelse fra sentralbanken og den sentrale oppgjørs organisasjon i Canada (Payment Canada), flere av bankene som er med i R3 samarbeide, R3 og andre deltagere i Canada som arbeider med betalinger og samtidig har kompetanse på DLT.

Innledningsvis satt de opp en rekke fordeler som DLT teknologien kan bety for bank næringen. Oppsummerings er det 1) behov for en sentral database forsvinner 2) enklere å bygge inn fleksibilitet (resilience) 3) kostnads effektiv 4) konfidensialitet er mulig å bygge inn 5)redusere feilsituasjoner og krav etter feil i betaling i forhold til dagens teknologi.

I tillegg kan det løse problemet med at det ikke finnes noen global sentral part, til tross for CLS (Continius Linked Settlement).

Figure 1: Benefits and Key Features of DLT



I fase 1 ble Ethereum benyttet som teknologi. Det ble opprettet en krypto canadiske dollar benevnt DDR, som sentralbanken kunne utstede mot at bankene deponerte tilsvarende antall canadiske dollar på en sikrings konto i sentralbanken. Hver morgen fikk hver bank tilført DDR og hver kveld måtte de konvertere tilbake til fiat penger (CAD). Hver bankkunde hadde en krypto wallet. Prosjektet oppdaget svakheten i Ethereum rundt skalering ettersom Ethereum benytter «proof of work» konsensus mekanisme. Et annet problem var at transaksjonene er transparente for alle deltagere, noe som er bra i en test fase, men uhensiktsmessig i produksjon. I fase 1 ble det utviklet noen få integrasjon mot tradisjonell infrastruktur for å teste om sentralbankens systemer kan benyttes.

Figure 3: High-Level Overview of Project Jasper Phases 1 and 2

	Phase 1	Phase 2
Purpose	Experimental review of DLT's applicability to wholesale interbank payments settlement	Further evaluation of the scalability and flexibility of DLT by building a Corda experiment. Accommodate multiple settlement options covering RTGS and LSM. Provide a data-driven simulation exercise with operational data sets to evaluate platform and LSM performance.
Platform	• Ethereum • Custom middleware • Solidity (3 contracts) • Angular JS front end	• Corda • Kotlin • Extended Phase 1's Angular JS front end
Innovations	• Atomic exchange (transfer without reconciliation) • Maintained knowledge of ecosystem distribution • Impacts on PFMI	• Netting options • Decentralized node authorities • Corda 1-N atomic flows • Operational impact
Notable output	• Ethereum prototype • Research in PFMI context	• Corda prototype • Platform comparison • 2 LSM comparisons • Research White Paper

[13]The legislated mandate and duties of Payments Canada are articulated in the *Canadian Payments Act*, which came into force in 2001 (succeeding the *Canadian Payments Association Act*). It is available for download on the Payments Canada website at **www.payments.ca.**

[14]The term "interbank" is synonymous with "wholesale" and "high-value."

Fase 2 startet september 2016, og Corda fra R3 ble valgt som teknologi. Her ble det ikke utviklet noen form for integrasjon med tradisjonell infrastruktur. Corda introduserte konseptet med Notarius node. De to betalingstypene i fase 2 var «Atomic» (dette betyr null operasjonell motpartsrisiko) og LSM (Liqidity Saving Mechanism). Med LSM ble det også innført et sentralt køsystem og med det netto oppgjør. Dersom betalinger med lav prioritet kan vente litt når det er stort antall transaksjoner, blir belastninger på prosessor kapasiteten jevnere gjennom dagen. Fokus for begge fasene var betalinger mellom store kunder (wholesale).

Fase 3 ble presentert senhøsten 2017 og jeg har ingen informasjon om det nå.

Oppsummering

Alt i alt var testene vellykkede og gir grunnlag for videre faser.

Det faktum av Corda nodene bare lagrer de transaksjoner de selv deltar i medfører et større behov for back-up og data recovery enn Ethereum, selv om man bør gjøre back ut i Ethereum også. Testen viste at hver node (bank) må ha omfattende data recovery sikkerhets tjenester. Ettersom bare notarius har alle transaksjoner er det innført en «single point of failure». Det er mulig å sette opp med enn en notarius node i et nettverk.

Corda har bedre løsninger for privat informasjon enn Ethereum.

Corda har bedre skalering (antall transaksjoner i sekundet) enn Ethereum.

Innføringen av LSM og en sentral køordninger introduserte en ny «single point of failure» selv om de fleste i testen mente et køsystem en nødvendig.

Canada har et veldig effektivt og lav kost betalingssystem i dag (LVTS) og det skal mye til å gjøre det bedre med DLT, men DLT gir mange andre fordeler som bedre back office støtte.

Table 2: Future Opportunities for Exploration

Opportunity	Description
Connect domestic settlement capability with another domestic DLT/blockchain use case	• What advantages would a DLT solution based on central bank-issued digital cash equivalents provide for related processes, such as securities settlement? What experiments could be conducted to join the Jasper settlement platform with DLT initiatives in capital markets?
Central bank to central bank digital cross-border currency exchange	• How might a single-currency DLT zone best be connected with other currencies? What are the optimal models for addressing friction in the current cross-border payment ecosystem?
Define the operational (non-technical) considerations that need to be addressed to support a DLT settlement solution	• What policy considerations and changes need to be addressed? What new or reformed legal constructs are required? • How would a production system be governed, maintained and supported? • Explore non-cash collateral, including high-quality liquid assets (HQLA) and other asset holdings in addition to cash?

BANK OF ENGLAND (BOE)

Bank of England har publisert en rekke rapporter og analyser fra 2014 frem til slutten av 2017. BoE har tatt teknologien mer som selvfølge og vært fokusert på makro økonomiske konsekvenser av å innføre en krypto engelske pund.

«Digital future for sterling», Juli 2017.

Dette dokumentet omhandler potensiale for CDBC (Central Bank Digital Currency) og hvordan CDBC kan fungere som en ekvivalent for kontanter. I dag utgjør bruk av kontanter omtrent halvparten av all betaling «over disk» i England. Dokumentet konkluderer med at mens andre bransjer har opplevd disrupsjon (Uber, AirBnB og Netflix) har bank og betaling ikke opplevd samme transformasjon. Stor sett bare forbedringer på kundeflaten. Men BoE regner med at transformasjonen i bank og finans kommer nå. BoE har et RTGS system som gjennomfører oppgjør for 500 milliarder pund hver dag. Med utviklingen av Bitcoin, Litecoin, Dogecoin, etc. nevnes at BoE kan utstede CDBC hvor selskaper og privatpersoner har ha konto med CDBC rett i sentralbanken, og gjennomføre betalinger til hverandre real time P2P. Dokumentet konkluderer med at mange spørsmål er ubesvart med hensyn på politiske forhold, finansiell stabilitet, endringer for de kommersielle bankene og finanstilsyn.

"The economics of digital currencies», høsten 2014.

De kryptovalutaene som finnes nå har en ferdig pengemengde (Bitcoin har 21 millioner Bitcoin). Dette er en mekanisme som sannsynligvis ikke kan brukes av en sentralbank for en lands økonomi. Pengemengden må sannsynligvis kunne endres over tid.

Betalinger har gjennomgått endringer fra gullmynter hvor verdien var vekten av gull, til papirpenger og nå elektroniske penger. Betaling mellom to kunder av samme bank gjøres opp internt i samme bank, men mellom kunder av to banker via BoE sentraliserte oppgjørs system. Bitcoin representerer både et betalingssystem og en pengeenhet. Pengene skapes uten en sentralbank og kunder kan betale direkte til hverandre uten en mellommann. I tradisjonell betaling garanterer banken for at betaler har penger på konto (saldo basert), mens i Bitcoin sørger teknologien for at samme Bitcoin ikke brukes to ganger av betaler. Tillit er flyttet fra en finansiell institusjon til selve teknologien. Nøkkelen er felles regnskapssystem (distributed ledger), gjennomsiktig for alle.

Penger skal ha tre funksjoner 1)betalingsmiddel 2)en måte å oppbevare verdi på og 3)en regnskapsenhet. Radford (1945) kunne dokumentere at sigaretter hadde alle disse tre definisjonene blant krigsfanger under sist verdenskrig. Bitcoin og kryptovaluta kan ansees som penger for de som har tilgang til internett, i parallell med tradisjonelle penger. Forutsetningen er at Bitcoin må ha verdi i fremtiden, og samtidig at volatiliteten gjør verdifastsettelsen usikker. I forhold til å være betalingsmiddel er antall børser man kan veksle og butikker som aksepterer Bitcoin avgjørende. Om ingen eller veldig få aksepterer kryptovalutaen er den uegnet som betalingsmiddel.

Transaksjonsavgiften er lav i kryptovaluta (LM: Bitcoin transaksjoner kostet noen få øre i 2014) noe som er avgjørende for Bitcoin sin utbredelse, uansett om betalingen krysser landegrenser eller størrelsen på betalingen. Kostnadene er knyttet til å prosessere betalingen. I tradisjonell teknologi hos en sentral part, i kryptovaluta distribuert hos en rekke «minere». I prinsippet vil det alltid være billigere å prosessere betalingen ett sted i stede for mange steder (distribuert). Men i Bitcoin får

minere 12,5 (LM: i 2014 25) nye bitcoin for hver blokk de miner, dermed subsidierer generering av nye Bitcoin transaksjons kostnad. Transaksjons kostnader ventes ¨stige med redusert subsidiering over tid (i Bitcoin halveres beløpet hver 4. år). En risiko er at antall minere blir færre over tid og man får et monopol.

Den faste pengemengden er et problem i kryptovaluta. Ved resesjon og høy arbeidsledighet vil en konstant pengemengde sannsynligvis øke problemene for landet. Det er ingen teknisk grunn til at kryptovaluta har en fast pengemengde. Pengemengden er i dag variabel som resultat av sesong (julehandel), syklisk (resesjon) og strukturell (f.eks. ny teknologi). Dersom pengemengden ikke kan respondere på slike begivenheter vil prisene på varer være volatile og dermed ødelegge husholdningenes levestandard. Dette kan løses i en kryptovaluta ved for eksempel øke pengemengden når antall transaksjoner øker, eller ved automatisk avstemming.

BoE er ansvarlig for økonomisk og finansiell stabilitet i henhold til Financial Service Act 2012. Dagens volum i kryptovaluta er for liten til å true den finansielle stabiliteten, selv om kursen krasjer. Men dersom volumet i kryptovaluta blir signifikant i fremtiden, kan en krasj føre til problemer for den finansielle stabiliteten. Men det vil oppstå et stort problem dersom prinsippet om fractional reserve banking blir fragmentert. (at andre enn bankene «trykker» penger). Rapporten diskuterer muligheten for at kommersielle banker utsteder kryptopenger i likhet med dagens kontopenger. Dersom vi får en «bank run» i en for fragmentert pengetrykking, vil ikke sentralbanken i en slik situasjon kunne bidra. En annen trussel er at MPC (Monetary Policy Committee) mister kontrollen på inflasjon og økonomisk politikk. I dag gjøres det blant annet gjennom rentesetting, som igjen påvirker forbruk og investeringer i samfunnet.

286 Quarterly Bulletin 2014 Q3

Conclusion

Both digital currencies' status as money and the distributed ledger technology used by them have potential to develop over time. Most digital currencies, at present, deploy fixed eventual money supplies, although this is not strictly an essential feature. Usage of digital currencies is presently very low and, as currently designed, there are a variety of incentive problems that are likely to prevent their widespread adoption in the long run.

Digital currencies do not, at present, play a substantial role as money in society. But they may have the potential to come to exhibit at least some of the functions of money over time. There is little incentive for the pricing of goods and services to change from traditional currencies, however, unless these currencies were to suffer from a wholesale collapse in confidence.

Digital currencies do not currently pose a material risk to monetary or financial stability in the United Kingdom. Should they achieve limited adoption as a payment system, they are unlikely to undermine the Bank's ability to achieve monetary stability. While that could, in theory, change if sterling were abandoned in favour of an alternative currency for a significant fraction of the economy, such a scenario is considered extremely unlikely at present. A variety of potential risks to financial stability could emerge if a digital currency attained systemic status as a payment system, most of which could be addressed through regulatory supervision of relevant parties.

Staff working paper No 605, juli 2016.

Fokus for dette 90 sider lange dokumentet er hvordan makroøkonomien kan fungere med en digital pengeenhet utstedt av sentralbanken. Teknologien som er nevnt i dokumentet er basert på DLT,

uten at det er gjort noen teknisk analyse slik andre sentralbanker har gjort. Avslutningsvis er det utarbeidet en rekke interessante matematiske modeller for gjennomføring av CBDC (Central Bank Digital Currencies).

> We study the macroeconomic consequences of issuing central bank digital currency (CBDC) — a universally accessible and interest-bearing central bank liability, implemented via distributed ledgers, that competes with bank deposits as medium of exchange. In a DSGE model calibrated to match the pre-crisis United States, we find that CBDC issuance of 30% of GDP, against government bonds, could permanently raise GDP by as much as 3%, due to reductions in real interest rates, distortionary taxes, and monetary transaction costs. Countercyclical CBDC price or quantity rules, as a second monetary policy instrument, could substantially improve the central bank's ability to stabilise the business cycle.

Kort oppsummert: 30 % av BNP bør være i CBDC, som vil øke BNP med 3 %. Publikum bør få sette inn innskudd i sentralbanken på rentebærende konto (som i tillegg er risikofritt) og i konkurranse med bankenes kontopenger som betalingsmiddel.

Ettersom det ikke finnes noe empiri å undersøke har denne studien benyttet DSGE modellen med parametere fra USA før finanskrisen før 2007. Det er benyttet 30 % av BNP i CBDC ettersom det tilsvarer de kvantitative lettelsene flere sentralbanker har benyttet de sist 10 årene. Resultat viser at å benytte CBDC vil øke BNP med 3 % på grunn av bedre betalings infrastruktur og tilpassing av skatt. Ettersom innovasjonen både vedrørende kontanter og elektroniske penger (lønnskonto, bedriftskonto, lån og innskudd) ikke har funnet sted på mange ti-år, representerer private penger, slik som Bitcoin innovasjon både som betalingsmiddel og regnskapsenhet. Det er spesielt den desentrale hovedboken (distributed ledger) som medfører innovasjon ved at sentralbankens uunnværlighet bortfaller.

Dagens betalings systemer er basert på en sentral enhet med sentralbanken i sentrum. Bankene gis adgang gjennom innskudd i sentralbanken, og med det en fordring på sentralbanken. Betaling mellom kunder i en bank medfører bokføring i denne bankens hovedbok. Betalinger mellom flere banker gjøres ved bokføring i disse's hovedbøker og via bokføring i sentralbanken, alternativt en oppgjørsbank i utlandet. For å sørge for tillit er banker regulert og gjenstand for kapitaldekningskrav og andre krav. Regulering av finansmarkedet skaper inngangsbarrierer og gir bankene prismakt og makt til å prise gjeld.

Digitale penger har en rekke fordeler slik som økt konkurranse, økt tilgjengelighet og økt fleksibilitet. Men digitale penger medfører også ulemper, som kostnaden ved å ha mer en enn hovedbok (LM: mer enn en valuta) som skal synkroniseres med eksisterende og kostnadene ved at aktørene ikke har tillit til hverandre. Dersom nye aktører skal ha muligheten til å delta må det finnes en mekanisme for å velge dem inn.

Kryptovaluta har mye av de mekanismene som behøves og Bitcoin er den fremste av disse. Aktører (minere) som ønsker å legge transaksjoner til hovedboken må også bevise at de aksepterte en stor kostnad ved å få det gjort, noe som kalles «Proof of Work» (PoW). Ettersom minere konkurrer er det den som legger ned mest arbeid som har størst sannsynlighet for å vinne. Fordelen med PoW er at den tillater nye aktører bare dersom de er villige til å betale prisen for å delta, uten at den nye aktøren har noen kontrakt eller avtale med de andre aktørene, noe som sikrer et komplett desentralt system.

For å sikre at en blokk mines omtrent hvert 10 minutt, tilpasser vanskelighets-graden i algoritmen seg kontinuerlig etter tiden mellom hver blokk. Blir tiden mye mindre enn 10 minutter blir algoritmen vanskeligere å løse og omvendt om det tar lenger tid. Som kompensasjon for å mine en blokk får aktøren/den som miner transaksjons avgiftene + utstedelse av nye kryptovaluta. Dette siste subsidierer kostnaden ved å godkjenne transaksjonene og holde nettverket i drift.

Ulempen med PoW er at hver miner har fokus på egen kompetansekraft og sub-optimerer investeringene for å vinne i konkurransen slik at øko systemets samlede investering i datakraft er alt for stor og den sosiale faktor reduseres. Dermed forbrukes langt mer elektrisk kraft enn hva som behøves. BoE sin konklusjon er at dersom et land skal benytte kryptovaluta, må det finnes andre mekanismer enn PoW.

Sentralbank utstedelse av digitale penger (CBDC) er en universal, 24/7, elektronisk, nasjonal valuta som er rentebærende. De forutsetter at mesteparten av pengene er fordring på bankene og del av innskuddsgaranti. I prinsippet at bankene, og ikke sentralbanken, utsteder mesteparten av pengene i henhold til Tobin's forslag (1987). Distribuert hovedbok er i helt nødvendig, men vil gjøre det enklere å administrere to pengeenheter, enten ved at sentralbanken vedlikeholder hovedboken, eller at noen privat sektor gjør det. Rentesetting på CBDC kan enten settes av sentralbanken, eller at bankene byr på renten på en «markedsplass», noe som vil regulere pengemengden i CBDC. Sentralbanken har alltid gitt bankene mulighet til å aksessere sentralbankens balanse gjennom kjøp av sedler og mynt. Kontanter er fordring på sentralbanken, rentefritt. Det er flere ganger vurdert kompensasjon i form av skatt på kontanter, eller at kursen mellom kontanter og digitale penger er ulik 1:1, men ingen sentralbank i verden har frem til nå innført slikt. Rente effekten er ikke en del av denne analysen.

A - Strukturelle forhold.

Når sentralbanken utsteder kontanter som leveres til banken reduseres rentebærende gjeld for sentralbanken. Det utgjør økt inntekter for staten. Denne rentenetto må forbli positiv. Derfor medfører CBDC kjøp av statens gjeld redusert renteforpliktelse for staten og øker sikkerheten til gjenstående gjeld og dermed redusere kredittrisikoen til private. Dette vil igjen føre til lavere renter til publikum og med det større økonomisk sparing.

Ulempen med at transaksjonsvolumet flyttes til CBDC er at innskudd i bankene reduseres til fordel for innskudd i sentralbanken, dermed vil en større del av bankenes innskudd komme fra privatpersoner til en høyere rente, noe som vil redusere bankenes rentemargin.

Utstedelse av CBDC bør utelukkende skje mot statsgjeld/obligasjoner, noe som kan bidra til mot syklisk politikk (repro transaksjoner). På den måten kan sentralbanken trekke inn CBDC fra sirkulasjon. Det kan finnes alternativer som for eksempel noen form av utbytte eller utlån av CBDC til bankene.

Når beholdningen av CBDC ble skapt initialt og senere mot syklisk endret vil årlige inn og utbetalinger fra staten kunne bli påvirket av reduserte renteutgifter, noe som igjen kan lede til lavere skatt til befolkningen. Dette dokumentet skraper bare i overflaten av dette spennende tema, og bør studeres nøyere senere.

Kostnadene i forbindelse med betalinger vil bli redusert, selv om rapporten ikke klarer å kvantifisere det. Også likviditets kostnader blir redusert.

Ettersom inngangsbarrierer for nye betaling-leverandører reduseres med en desentral modell, øker konkurransen og kostnadene for publikum reduseres. Dette vil også medføre en større konkurranse om publikum og selskapers innskudd, som igjen vil medføre mer innovasjon.

I dagens betalings system har bankene motparts risiko (kreditt risiko i fall en bank går konkurs) og i tillegg likviditets risiko ved at en bank ikke har satt av tilstrekkelig innskudd i sentralbanken som sikkerhet for oppgjør. Som et resultat benyttes tilnærmet risikofri statspapirer, og særlig for mindre banker som benytter større banker for oppgjør, noe de normalt hadde ønsket å beholde i egne bøker. CBDC på den annen side medfører oppgjør direkte mellom partene på tvers av sentralbankens balanse. Motpartsrisiko er dermed fjernet fullstendig, og deponering av statspapirer behøves ikke, noe som frigjøre enorme mengder likviditet knytet til ikke-transaksjons beholdning. I tider med finansielle kriser og mangel på finansiell sikkerhet vil dette medføre en betydelig finansiell stabilisering.

Avslutningsvis under strukturelle forhold betyr den desentrale arkitekturen at systemene aldri trenger å stoppe på grunn av vedlikehold, slik som i dagens systemer. De kan opererer 24 / 7 / 365.

B - Pris og stabilitet forhold

Sentralbanken kan bidra til å stabilisere økonomien gjennom renten. CBDC gir enda bedre mulighet til å stabilisere økonomien ved at pengemengden veldig raskt kan endres, både ved å utstede mer eller inndra mer. Det er å anta at renten på CBDC blir lavere enn renten i sentralbankpenger, men ikke null. Når renten går mot null, og endatil blir negativ reduseres sentralbankens mulighet til å bidra til stabilisering. Kvantitative lettelser ved å øke sentralbankens balanse er en mulighet. Ettersom CBDC har funksjoner utover «bare» det å være penger, kan CBDC utgjøre et bedre instrument for stabilitet.

Ettersom kommersielle banker i dag utgjør storparten av sentralbankens gjeld, kan det hende at kvantitative lettelser ikke medfører den effekten sentralbanken ønsker, ettersom bankene muligens kan ha andre interesser. CBDC derimot som medfører privat innskudd i sentralbanken kan i slike tilfelle bli mer effektivt.

CBDC kan også medføre at finans og pengepolotikken kan bli mer separat enn i dag. Blant annet kan det faktum at staten redusere sine rentekostnader medføre redusert beskatning av befolkningen. I tillegg vil det faktum at alle transaksjoner i utgangspunktet er synlig for alle gjør at tilsynsmyndighetene får bedre informasjon og i sanntid, og med det nye verktøy for å styre i spesielt vanskelige situasjoner og når økonomien gjennomgår sjokk.

C – Finansiell stabilitet forhold

Det er en risiko ved introduksjon av en ny teknologi som har til hensikt å være basis for landets økonomi. Først og fremst å være sikker på at teknologien ikke kan hackes og at den fungerer slik at befolkningen har nødvendig tillit til den. En annen risiko er at dagens finansielle system er komplekst og globalt. Det må tas hensyn til både alle mulige komplekse instrumenter og andre lands sentralbanker og finansielle system.

En annen risiko er faren for at private og bedrifter vil ta penger ut av bankene for å sette dem i sentralbanken for å konvertere til CBDC. Dette kan muligens skape en ubalanse hos de kommersielle bankene, noe som ikke er videre studert i dette dokumentet. Slik ubalanse kan

muligens avhjelpes ved at private kan by på renten til CBDC, blir renten negativ kan det hende private heller ønsker innskudd i bankene.

Utgangspunktet for CBDC er at man trenger statsobligasjoner for å veksle til seg CBDC i sentralbanken. Man kan i dette dokumentet ikke veksle til seg CBDC gjennom direkte innskudd i sentralbanken. Ettersom det stort sett er bankene som selger statsobligasjoner til det private markedet, vil balansen til bankene forbli tilstrekkelig. Det kan likevel hende bankene får utfordringer ettersom komposisjonen til balansen til bankene endrer og reguleringsmyndigheten har satt krav til vektet risikonivå i bankenes balanse.

CBDC må være tilstrekkelig stor og gjennomgripende og ikke være avhengig av en eller få aktører, som kan utgjøre fare dersom de går konkurs. Arkitekturen må ta hensyn til sannsynligheten for at en eller flere banker kan gå konkurs. Dersom dette tas hensyn til vil CBDC utgjøre en bedre løsning for kundene enn dagens løsning med innskuddsgaranti. Bare den effekten at betalingene skjer i sanntid og ikke timer eller dager, reduserer konsekvensene av en mulig hypotetisk bank konkurs. CBDC er en fordring på sentralbanken og ikke den kommersielle banken.

CBDC kan introduseres i tillegg til og parallelt med dagens sentralbankpenger. Det betyr at vi får to økosystemer. Dermed blir stabiliteten større og dersom en av systemene skulle få et avbrudd kan det andre benyttes. Det faktum at DLT er basert på distribuert arkitektur og dermed fungerer uavhengig av om sentralbanken eller en av bankene får databrudd, gjør at stabiliteten øker.

Det er også mulig at politikere får større forståelse av hele det økonomiske system, blant annet fordi smart kontrakter kan introduseres i forbindelse med komplekse finansielle transaksjoner.

For å oppsummere er det både positive og negative sider ved CBDC som gjør at myndighetene må vurdere nøye om fordelene er større enn ulempene.

BIS (BANK FOR INTERNATIONAL SETTLEMENTS)

«Central Bank Crypto Currencies" September 2017.
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Det kommer nesten daglig nye kryptovalutaer og det kan være interessant å se på hvordan sentralbankene kan posisjonere seg for CBCC (Central Bank Crypto Currencies). Det er i prinsippet to typer CBCC, en for detaljleddet og en for grossistleddet, som kommer i tillegg til sentralbankens kontanter og kontopenger (M1 pengemengden).

I løpet av mindre enn ti år har Bitcoin gått fra å være en obskur kuriositet til å bli et mye brukt begrep. Venture kapitaliser investerer tungt, sentralbanken og bloggere skriver om det og mantra er at den underliggende teknologien Blockchain og DLT kommer til å forandre verden. Mange av de store sentralbankene i verden har gjennomført prosjekter med kryptovaluta, hva har kommet ut av det så langt?

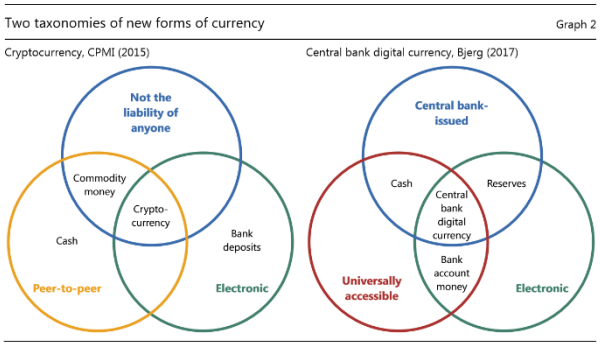
Det er fire parameter i en slik prosess 1-utsteder (sentralbank eller annen) 2-form (elektronisk eller fysisk) 3-tilgjengelighet (global eller begrenset) 4-overføringsmekanisme (sentral eller desentral). En CBCC er i elektronisk form for sentralbank penger som overføres desentralt, dvs. person til person

(P2P) uten mellomledd. Dette skiller CBCC fra andre sentralbank penger slik som kontopenger som distribueres på en sentral måte via bankenes innskudd i sentralbanken.

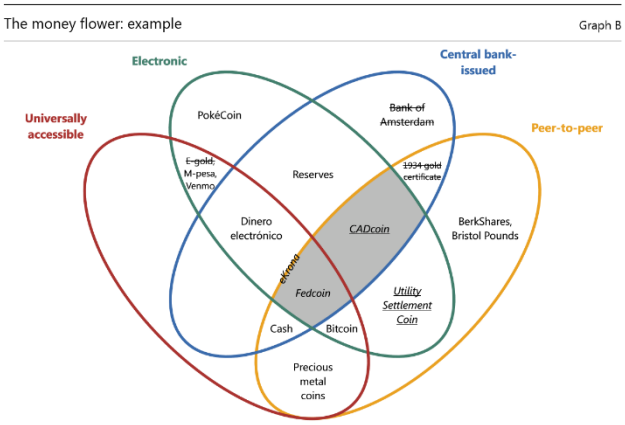
CBCC for detalj leddet (privatpersoner og bedrifter): For å kunne erstatte kontanter må anonymitet beholdes. Dersom anonymitet ikke er viktig kan sentralbanken tillate private innskudd i sentralbanken mot utstedelse av CBCC, noe som teknisk har vært mulig i lang tid, men som sentralbankene har holdt seg unna.
Grossist leddet (banker): Banker har ikke noe behov for anonymitet og alle transaksjoner er alt elektroniske og sporbare. Flere sentralbanker har annonsert forsøk med grossist ledd CBCC (Singapore, Canada, Den Europeiske sentralbanken, Japan med flere) men ingen har helt lykkes enda.

En ny form for sentralbank penger

CPMI (Committee on Payments and Market Infrastructure) laserte i 2015 en rapport som definerte en ny klasse valutaer som Bitcoin og altcoin (alternativ til Bitcoin). Denne klassen med valuta inneholder tre elementer 1) elektronisk 2) er ikke fordring på noen 3) person til person (P2P). Slike valutaer basert på DLT representer at ingen har tillit til noen, i motsetning til sentralbank penger hvor det finnes en mellommann med tillit. Kontanter er P2P men ikke elektronisk og det er en fordring på sentralbanken. Man kan muligens se CBCC som elektroniske kontanter som er en fordring på sentralbanken. Bedriftenes innskudd i kommersielle banker er en fordring på banken og ikke sentralbanken, er digitale og transporteres fra en kunde til neste via bankens regnskap, eventuelt til kunder i andre banker via sentralbanken. Det er i prinsippet bare banker som har fordring på sentralbanken i form av innskudd digitalt. Den største delen av dette er innskudd bankene har gjort for å sikre betaling, såkalt foliokonto i sentralbanken.



CBCC inkluderes i de fleste delene for hva som kan kalles tilgjengelige penger. Det finnes også penger med begrenset tilgjengelighet slik som mobile penger (M-Pesa og Dinero), virtuelle penger i spill (PokemonGo(Pokecoin), og lokale fysiske penger (Berkshare og Bristol Pound).



CBCC for detalj leddet.

Så langt er det ingen som har gjort forsøk på en CBCC for detalj leddet. Det er diskutert hyppig og Konigs forslag og Fedcoin er muligens det mest kjente. Fedcoin er en kopi av Bitcoin, men det er sentralbanken som «miner» og destruerer og kursen er en til en mot dollar. En enhet Fedcoin skapes ved at en enhet dollar elimineres, og omvendt når en enhet Fedcoin elimineres skapes en enhet dollar. Fedcoin vil bli desentral ved transaksjon (betaling) men sentral ved utstedelse. Fedcoin vil eliminere volatiliteten i valutaen og bedre den finansielle stabiliteten. I tillegg er det teknisk mulig å beregne renter i CBCC, også negative renter, noe som vil være uunngåelig dersom CBCC skal erstatte kontanter. Det er en risiko for at privat kapital vil søke å plassere sine

innskudd i risikofri rentebærende innskudd i sentralbanken i form av CBCC, og dermed søke seg bort fra tradisjonelle former for penger. Dette vil igjen sette bankenes forretningsmodeller under press. Fordeler må veies opp mot ulemper.

Anonymitet

Bitcoin er designet for å erstatte kontanter og ettersom elektroniske penger kan spores var løsningen at sender og mottaker er anonyme for andre enn de to involvert i transaksjonen. Senderen kan også holde seg anonym for mottakeren om han ønsker det. McAndrews (2017) hevdet at noe av grunnen for anonymisering er å forhindre ID tyveri, fysiske innbrudd og uønsket oppmerksomhet (spam). Motparts anonymitet er mindre viktig enn tredje parts anonymitet. Med bruk av Facebook og sosiale medier er det også usikkert hvor viktig anonymitet er. Det ble gjort en studie på universitet i Santa Barbara med 699 studenter om betalings tjenesten Venmo. 44 % synes det var helt greit at alle andre kunne se deres betalinger og 21 % tillot alle sine Facebook venner å se sine transaksjoner.

Andre forhold

Det kan virke underlig at en sentralbank ønsker å utstede penger som gjør det mulig å betale anonymt, men det er nettopp det sentralbanken gjør med sine mynter og sedler.

Det er ingen tvil om at den tekniske livssyklusen til dagens digitale kontopenger er i ferd med å nå sin slutt. Mange av de datasystemene som får infrastrukturen til å fungere er programmert i koder som ikke lenger kan vedlikeholdes, er kostbare og ikke tilpasset dagens behov.

Det faktum at DLT representerer umiddelbart oppgjør vil også bidra til redusert kapitalbinding i for eksempel handel av verdipapirer. Deutsche Bundesbank og Deutsche Börse har utviklet et system for levering-mot-betaling handel og oppgjør med bruk av «smart assets» og CBCC.