Riksbankens E-krona

Svar på förfrågan 2017-09-20 ”Hjälp Riksbanken att ta fram en teknisk lösning för en eventuell e-krona

Cashbutler AB (”CB”) startades utifrån en vision om att alla framtida betalningar kommer att ske digitalt och med användande av digitala valutor. Projektet startades för över 10 år sedan, alltså i tiden innan smartphones och ”appar” existerade. Resultatet är den plattform för hantering av elektronisk valuta som vi nu önskar presentera för Riksbanken.

Vår lösning kommer givetvis att behöva utvecklas i dialog med er och utvalda samarbetspartners. Detta gäller särskilt frågor om säkerhet, spårbarhet och om hur man bör kombinera en registerbaserad valuta med en värdebaserad. Den tekniska lösningen är dock heltäckande då det definierar ett säkert sätt att utfärda, bära och hantera e-kronan i alla led från utgivande till avveckling.

CBs lösning innebär liksom t ex Bitcoin att blockkedjor används. Skillnaden ligger främst i att CBs lösning är en värdeneutral metod för att hantera valuta elektroniskt, dvs. den är inte en valuta i sig. I CB:s system är det en central aktör företrädesvis utgivaren som säkerställer äkthet och äganderätt hos utgivna DC. Vår bedömning är att systemet är utbyggbart med ”distributed ledger” tekniken.

CB: s system innebär att den underliggande tekniken är densamma oavsett hur e-kronan lagras. Det innebär att en värdebaserad e-krona skulle kunna vara identisk med en registerbaserad, det enda som skiljer dem åt är om de lagras lokalt eller centralt. I besvarandet av nedanstående frågor har vi därför slagit samman fråga ett och två.

Svar på Riksbankens frågor

1) & 2) Hur skulle en teknisk lösning för *en registerbaserad e-krona/värdebaserad e-krona* kunna se ut?

Grundläggande systemuppbyggnad
CB:s system bygger på en universell bärare av elektronisk valuta. Vi kallar denna bärare ”Dynamisk Check” eller ”DC”. Dynamiska checkar består i princip av dataobjekt som kopplas ihop i kedjor vid en överföring. Vid lagring kan en DC liknas vid en rad i en databas. Databasen kan ligga lokalt t.ex. i en mobiltelefon eller centralt i ett eller flera register förvaltade av t.ex. Riksbanken, utgivare eller en specialiserad plånboks-aktör. Oavsett var en dynamisk check ligger lagrad har den samma format. CBs system medger därför samexistens av både värdebaserade och registerbaserade kontanter i valutan e-SEK.

DC hanteras av en programvaruenhet vars tre huvudkomponenter är databas, logikmodul och säkerhetsmodul. Säkerhetsmodulen hanterar autentisering och kryptering och verifierar motparten i en kommunikation. Logikmodulen utför ett begränsat antal operationer på databasen, t.ex. aggregera checkar, skapa dottercheckar, skapa DC blockkedjor och beräkna saldo på befintliga valutor. Programvaruenheten kan t.ex. installeras i en mobiltelefon i form av en app eller i en kassaapparat.

Databasen kan ligga lokalt i t.ex. en mobiltelefon och har då tydliga likheter med Riksbankens ”värdebaserade” e-krona, eller i en central databas och liknar då den ”registerbaserade” e-kronan. I det fall databasen hanteras centralt utförs även logik och säkerhetsoperationer centralt. CB:s system medger ett obegränsat antal utgivare och valutor. Riksbanken kan därför välja att samarbeta med flera aktörer för utgivning av e-SEK.

Transaktioner och överföringar
Grundprincipen med de dynamiska checkarna är att de i likhet med fysiska kontanter bär med sig all nödvändig information för att fungera i ett eko-system även om kontakt med en central server saknas. I uppsättningen med information som varje DC bär på finns en identifikationskod, valutakod och utgivarkod vilka säkerställer att den är unik i DC eko-systemet. Mot bakgrund av att systemet säkerställer att DCn är unik och att bär med sig all nödvändig information kan den flyttas direkt från en enhet till en annan utan hjälp av någon tredjepartsförmedlare förutsatt att enheterna kan autentisera varandra.

En DC har alltid täckning antingen eftersom den är präglad och garanterad av Riksbanken eller då utgivaren deponerat medel på ett depåkonto. När ett köp av e-valutan görs innebär det att en dynamisk check präglas och i samband med det ges den ett bestämt värde. Eftersom varje DC har ett bestämt värde är det inte säkert att värdet matchar priset på den vara eller tjänst som en användare önskar köpa med sin e-krona.

Nedan finns ett exempel på hur systemet fungerar vid en sådan transaktion.

Antag att en användare har följande dynamiska checkar i sin plånbok:
300 e-SEK
450 e-SEK
100 e-SEK

Antag vidare att användaren skall betala 600 e-SEK. Ett alternativ är att aggregera 300 checken och 100 checken. Gapet blir då 600 – 300 – 100 = 200. En 200 e-SEK dotter-check genereras från 450 checken som då får ett kvarvarande värde på 250 e-SEK. Både moderchecken och dotterchecken får i samband med denna transaktion nya unika identiteter som fortfarande kan kännas igen och verifieras av utgivaren.

Efter att de dynamiska checkarna cirkulerat kan exempelvis en handlare önska avveckla en mängd e-kronor. Systemet sorterar då upp de dynamiska checkarna efter utgivare och överför sedan varje uppsättning till ansvarig utgivare som krediterar användarens bankkonto genom att debitera sitt depå-konto. Utgivaren makulerar sedan samtliga avvecklade DC som då utgår ur DC ekosystemet.

Eftersom användaren deponerar medel för att införskaffa e-valuta tar mottagaren i en transaktion av en DC ingen kreditrisk.

Ytterligare säkerhetsaspekter som kryptering och autentisering som behöver byggas in i produkten. För att ta fram dessa funktioner behöver en dialog med lämpliga samarbetspartners initieras i samråd med Riksbanken.

Överföring mellan register- och värdebaserat system
I vårt system kan en användare som har tillgång till en registerlagrad e-krona ladda ner den till sin mobila enhet och därmed omvandla den till en värdebaserad e-krona. När detta sker minskar dock möjligheterna att i framtiden säkerställa äganderätten och äktheten hos denna e-krona (eller dess dotterenheter) eftersom den övergått till att bli värdebaserad. Ett centralt register bör därför inte ta emot en DC som kommer från en lokal lagring eftersom det innebär en högre risk än om överföringen görs centralt mellan två användares centrala register. Fördelen med det centrala registret blir därför att det kompletteras med information om hela kedjan av ägare och på så sätt inför en spårbarhet som en lokalt lagrad valuta svårt att erbjuda.

En ytterligare fördel som kommer med det registerbaserade systemet där valutan lagras centralt är att det finns väsentligt mindre möjligheter att införa falska dynamiska checkar, eftersom dessa omedelbart kommer att avvisas i den online check som då alltid sker mot utgivaren. Denna säkerhet kan komma att stärkas ytterligare i ett framtida scenario där en distribuerad liggare (eng. distributed ledger) kan ersätta det centrala registret.

Eftersom en värdebaserad respektive registerbaserad e-krona kan vara identisk innebär det i princip att utgivaren eventuellt mot en viss avgift skulle ha möjlighet att erbjuda växling från en värdebaserad till en registerbaserad. I en transaktion där en värdebaserad enhet växlas mot en registerbaserad

skulle den värdebaserade makuleras och en ny registerbaserad präglas och lagras i det centrala registret. I det omvända fallet behövs ingen växling eftersom en tillförlitlig registerbaserad e-krona kan överföras direkt till en lokal databas exempelvis i en mobiltelefon.

Utgivaren har möjlighet att erbjuda kringtjänster inom ramen för CBs system. Det kan beräkna och betala ut ränta baserad på det präglingsdatum som finns lagrat i DCns basnyckel. När räntan beräknats makulerar utgivaren samtliga DC som varit föremål för ränteberäkningen och en ny DC med ett värde av den som makulerades samt räntan präglas. I och med det återställs datumbeteckningen och den nya DCn får ränteberäkningsdagens datum i basnyckeln.

3) Vilka utmaningar och möjligheter ser ni med respektive e-kronalösning?

Riksbanken har en unik möjlighet att bli världsledande på området. Utmaningarna består i att finna en balans mellan registerbaserade och värdebaserade transaktioner och att bestämma en lämplig säkerhetsnivå. CBs system definierar värdebaserade digitala blockkedjor där varje block för med sig önskad information om utfärdare, tidpunkt, aktuellt värde mm. Inget hindrar dock att e-kronorna förs i ”depåer” och blir föremål för handel indirekt, dvs precis på samma sätt som transaktioner idag genomförs på konton via mellanmän, exempelvis Swish. Som Riksbanken är inne på måste man ha bägge lösningarna, dvs även tillåta värdebaserade transaktioner. I annat fall har man inte skapat förutsättningar för en digital valuta som kan ersätta kontanter.

En annan utmaning gäller spårbarheten. Ju mer spårbarhet som införs, desto svårare kan det vara att göra valutan attraktiv som ersättare i kontantledet. I och med att CB:s system medger flera valutor kan man tänka sig två olika e-kronor, en spårbar som tillåts avvecklas i större omfattning och en mindre ”light” variant som inte är spårbar men heller inte enkelt avvecklingsbar över en viss nivå.

4) Hur ser er vision för en e-krona ut, finns andra lösningar än register- och värdebaserad som ni bedömer är bättre lämpade?

I vår vision subventionerar Riksbanken tillhandahållandet av ”e-krone Appar” till allmänheten samt kostnaden för den datorkraft som vid var tidpunkt krävs för att utfärda och avveckla e-kronor. Kontoföring kan vara en del i Riksbankens uppdrag men då används befintlig infrastruktur.

Vi känner inte till några andra effektiva, snabbare och säkrare förslag till lösningar. CBs metod innebär ett driftssäkert och autonomt tillhandahållande av betalningsmedel, särskilt om den tillåts använda värdebaserade innehav och transaktioner som fungerar utanför web- och telefonnät. CB:s metod bygger på väl skyddad teknologi.

5) Vad saknas i Riksbankens koncept?

Riksbankens saknar hittills koncept för de tekniska lösningar som krävs, vilket också framhålls i rapporten. CB kan tillhandahålla en sådan teknisk lösning.

Med vänlig hälsning

Cashbutler AB
Box 5339
102 47 Stockholm

Org.nummer: 556708-6631