E-kronapiloten etapp 1

april 2021

Innehållsförteckning

1 Varför e-krona?

Sedlar och mynt används alltmer sällan i Sverige. Det beror bland annat på den tekniska utvecklingen som gett oss olika typer av digitala betaltjänster. Riksbanken ser att problem kan uppstå på grund av kontantminskningen och driver därför ett projekt där vi undersöker möjligheten att ta fram ett digitalt komplement till kontanterna, så kallade e-kronor. Denna rapport beskriver kortfattat den tekniska lösning som testats under etapp 1 av e-kronapiloten och de legala utredningar som gjorts av lösningen. Även övergripande lärdomar från projektet och nästa steg i arbetet redovisas. Än så länge finns dock inget beslut om att ge ut e-kronor eller hur e-kronorna i så fall skulle designas och fungera och vilken teknik som skulle användas.

Riksbanken har i uppdrag att främja ett säkert och effektivt betalningsväsende och har sedan 1904 monopol på att ge ut svenska sedlar. Kontanterna är idag de enda centralbanksutgivna pengar som är tillgängliga för allmänheten.[1] Den tekniska utvecklingen har dock inneburit att fysiska kontanter används alltmer sällan medan de digitala betaltjänsterna blir alltmer populära. När kontanterna får stå tillbaka till förmån för de privata aktörernas digitala tjänster innebär det att Riksbankens direkta roll på betalningsmarknaden minskar. Riksbanken kan därmed få svårare att fullfölja sitt uppdrag att främja ett säkert och effektivt betalningsväsende tillgängligt för alla grupper i samhället. Riksbanken har därför sedan 2017 arbetat med att utreda vilken roll Riksbanken bör ha i en allt mer digitaliserad värld och om det kan finnas skäl för Riksbanken att ta fram ett digitalt komplement till de fysiska kontanterna, en så kallad e-krona.

Riksbankens e-kronapilot

Riksbanken bildade 2019 enheten för e-kronapilot vars syfte är att öka Riksbankens kunskaper om hur en eventuell e-krona skulle kunna utformas genom att ta fram förslag på en teknisk lösning samt undersöka regelverksfrågorna för en e-krona. I februari 2020 tecknades efter en offentlig upphandling ett avtal med Accenture i rollen som leverantör av den tekniska lösning som e-kronapiloten testar. Den tekniska pilotlösning som utvecklats i en sluten testmiljö ska inte tolkas som den lösning som Riksbanken har valt för en eventuell e-krona, utan som den metod vi valt för att utifrån en konkret, möjlig, teknisk lösning kunna analysera policyfrågor, tekniska frågor, säkerhetsfrågor och juridiska frågor kring en eventuell e-krona.

[1] Se riksbankslagen (1988:1385) kap.5 § 1 samt 6 kap. 7 §. Det finns idag digitala centralbankspengar i Riksbankens avvecklingssystem, RIX, men dessa är endast tillgängliga för deltagare i systemet, som exempelvis banker.

2 Testad teknisk lösning under etapp 1 av e-kronapiloten

E-kronan i den tekniska lösning som testas i etapp 1 av e-kronapiloten är tokenbaserad i ett distribuerat nätverk baserat på en typ av blockkedjeteknik. Att e-kronan, som endast kan skapas av Riksbanken, är tokenbaserad ger den vissa egenskaper som liknar de fysiska kontanterna. En sådan likhet är möjligheten att lagra tokens lokalt hos slutanvändaren, vilket skiljer mot de digitala pengar vi lagrar på konto idag, som skapar alternativ för hur lösningen skulle kunna implementeras. E-kronanätverket som utvecklats under etapp 1 och som beskrivs nedan har byggts i en avgränsad testmiljö där viktiga delar som deltagare, likviditetsförsörjning och slutanvändare har simulerats.

2.1 E-kronan utformas som en token

Svenska kronor kan utformas på olika sätt. Kronan kan ha fysisk form och utgöras av de sedlar och mynt som innehavaren kan bruka genom att rent fysiskt ha dem i sin ägo. Kronan kan också vara i elektronisk form som pengarna vi har på konton, där innehavaren genom att identifiera sig bevisar sin rätt att använda pengarna på kontot. E-kronan i den tekniska lösning som e-kronapiloten testar är utformad som en s.k. *token* vilket innebär att det är en unikt identifierbar digital värdeenhet med egenskapen att den kan bära värdet av kronor. Detta har dock ingen större betydelse för hur e-kronan ser ut för slutanvändaren; e-kronorna framstår som dagens digitala pengar där man ser saldot av sitt innehav av e-kronor och inte en eller flera unika digitala värdeenheter. E-kronans tekniska egenskaper skapar dock nya möjligheter som är värda att nämna och förklara närmre.

Att e-kronan har formen av en token innebär att den delar en del egenskaper med de fysiska sedlarna men också att den är annorlunda i några viktiga avseenden. Precis som med sedlarna är det endast Riksbanken som kan skapa och ge ut e-kronorna. Rent tekniskt styrs detta av ett certifikat som bevisar att Riksbanken är utgivare av e-kronan, och precis som med sedlarna står staten som garant för e-kronans värde. Varje token bär också ett specifikt värde, men medan sedlarna har givna valörer kan värdet en token innehåller variera. Likt sedlarna är varje token också unikt identifierbar och de e-kronor den innehåller går att spåra till Riksbanken som enda utgivare.

Att e-kronan genom tokens är digital innebär också skillnader mot de fysiska kontanterna. För att få tillgång till och genomföra betalningar med e-kronorna krävs att man har en digital plånbok kopplad till ett betalningsinstrument i form av exempelvis ett kort eller en app. Till skillnad från kontanter som kan användas mellan personer utan tekniska hjälpmedel och utan någon tredje part inblandad så kräver betalningar med

e-kronor att betalaren kan kommunicera med e-kronanätverket. Kommunikationen sker via deltagare i nätverket, exempelvis banker och betaltjänstleverantörer.

En viktig teknisk skillnad är också att en token enbart kan användas en gång. Varje transaktion med e-kronor innebär att den token som använts noteras som förbrukad och de e-kronor som ingår i transaktionen får nya representationer i form av en ny token till mottagaren och i de fall det är aktuellt en ny token med växel tillbaka till betalaren. Mängden e-kronor i cirkulation som går att spåra till Riksbanken är densamma men kronorna är representerade av nya tokens.

En grundläggande princip är dock att en svensk krona alltid har samma värde oavsett om den kommer i form av fysiska kontanter utgivna av Riksbanken, kontotillgodohavanden hos en privat aktör eller en digital e-krona utgiven av Riksbanken. Växlandet mellan den ena till den andra ska alltid vara i ett-till-ett förhållande.

2.2 Distributionsmodellen liknar dagens modell för kontanter

Distributionsmodellen i e-kronapilotens lösning påminner om hur de fysiska kontanterna distribueras idag. De fysiska kontanterna kräver av naturliga skäl en logistikmodell som har längre ledtider än de digitala e-kronorna, men från ett roll- och ansvarsperspektiv så finns det tydliga likheter.

En sådan viktig likhet är att endast Riksbanken kan skapa och destruera e-kronorna. En annan likhet är att Riksbanken har en relation med distributörerna av e-kronor, i e-kronanätverket kallade deltagare, som i sin tur har en relation med allmänheten som slutanvändare. Deltagarna i e-kronanätverket driver sina egna noder från vilka de kan begära att e-kronor ges ut av Riksbanken mot att deras konton i Riksbankens avvecklingssystem, RIX, debiteras. E-kronorna skapas därefter av Riksbankens nod i nätverket och distribueras till deltagarens nod i nätverket. Deltagarna kan sedan lagra e-kronorna digitalt i så kallade deltagarvalv för vidare distribution till slutanvändarna. Deltagarna erbjuder slutanvändarna möjligheten att via en digital plånbok kopplad till ett betalningsinstrument, som en mobilapp eller ett kort, växla till sig e-kronor mot kontotillgodohavanden. Processen påminner om hur man växlar till sig kontanter mot kontotillgodohavanden vid ett bankomatuttag, men istället för att växla till sig fysiska kontanter så växlar man till sig e-kronor som lagras digitalt. E-kronorna kan sedan användas för transaktioner och om så önskas kan användaren växla tillbaka dem till kontotillgodohavanden igen via sin deltagare, exempelvis sin bank. Deltagaren kan i sin tur lösa in e-kronorna hos Riksbanken som destruerar dem och krediterar deltagarens konto i RIX.

E-kronanätverket där e-kronorna cirkulerar är baserat på företaget R3:s Cordaplattform som är en sorts blockkedjeplattform. Nätverket är ett decentraliserat privat nätverk (tekniken brukar kallas för DLT *Distributed Ledger Technology*) där Riksbanken som ägare bestämmer vilka som får ansluta som deltagare. Att nätverket är decentraliserat innebär att transaktionerna med e-kronorna registerförs hos de för transaktionen inblandade deltagarna i nätverket, istället för i en central databas. Deltagarna,

exempelvis banker och betaltjänstleverantörer, driver sina egna noder i nätverket och har därmed möjlighet att begära utgivning av och att växla in e-kronor, distribuera e-kronor samt utföra och ta emot transaktioner åt anslutna slutanvändare. Nätverket är parallellt och använder därmed inte dagens befintliga infrastrukturer för betalningar med digitala pengar, som exempelvis kortnätverken och bankgirot. Detta innebär att betalningar inom nätverket fungerar vid problem med befintlig betalinfrastruktur. Det skapas inte några nya pengar i e-kronanätverket. Istället försörjs nätverket med likviditet från Riksbankens avvecklingssystem, RIX. I detta avseende finns alltså ett beroende till ett externt system för att skapa nya e-kronor eller ta ut e-kronor ur nätverket.

Diagram 1. Så distribueras e-kronan
Transaktioner inom nätverket sker genom noder som drivs av Riksbanken och utvalda deltagare.

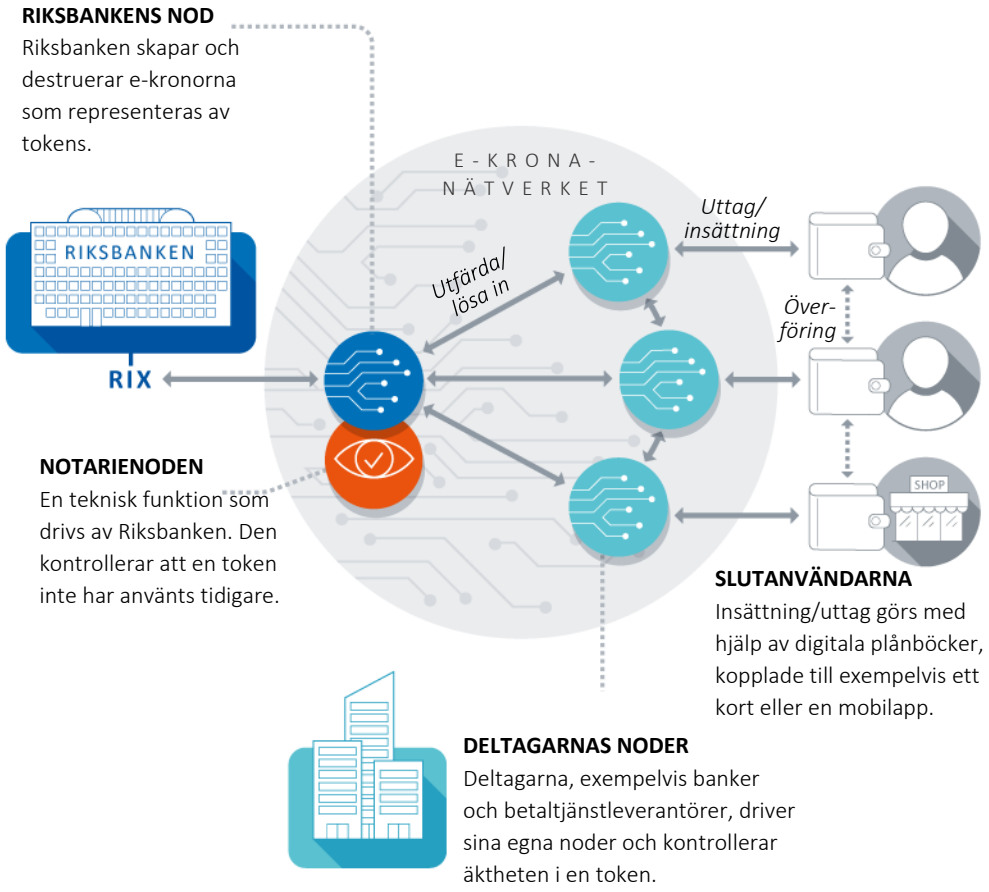


Diagram 1 visar en förenklad bild av hur e-kronanätverket och dess aktörer är integrerade och kan kommunicera med varandra och slutanvändarna, hur e-kronanätverket förses med likviditet och hur transaktioner utförs. Transaktionerna i nätverket sker i realtid och ska vara tillgängliga dygnet runt årets alla dagar.

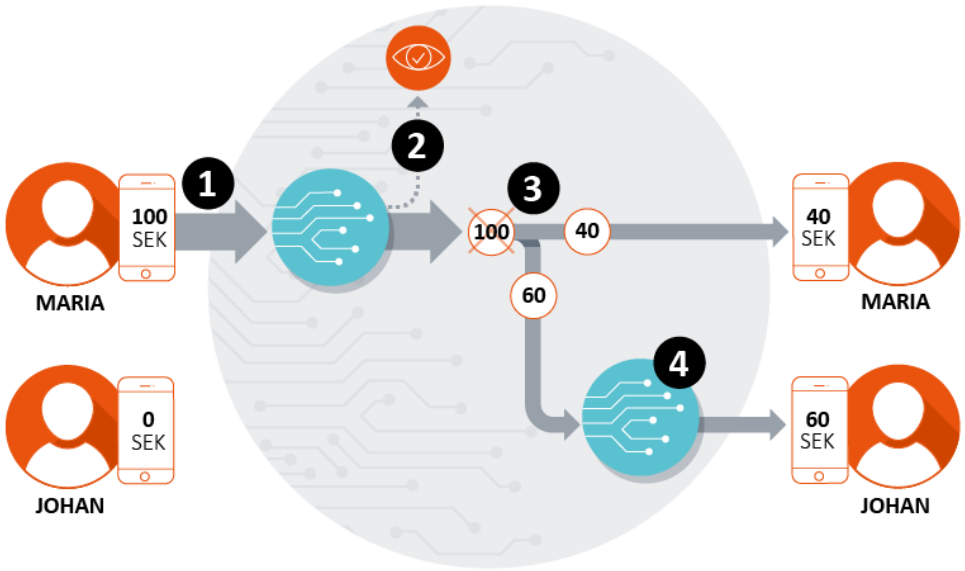
2.3 Äktheten av e-kronor kontrolleras i en transaktion

När man har elektroniska pengarna på ett konto är saldot på ens konto resultatet av ingående och utgående transaktioner i ett kontrollerat system (till exempel en banks interna system). Kontot innehåller information om vem som är innehavare till saldot på kontot men pengarna håller ingen mer information än just saldot på kontot. Hos de tokenbaserade e-kronorna ligger däremot trovärdigheten i själva e-kronorna i sig och i informationen som kan bevisa att de är unikt identifierbara med en spårbarhet till Riksbanken som utgivare, precis som kontanterna. E-kronanätverket behöver därför kunna validera och verifiera att e-kronorna som används i en transaktion är äkta.

För att skapa trygghet och tillit till betalmedlet kontanter är sedlar och mynt designade så att de ska vara lätta att känna igen för mottagaren samt svåra att förfalska. För e-kronorna måste äktheten styrkas digitalt inom e-kronanätverket. Som nämnts ovan så får också varje token som representerar en viss mängd e-kronor endast användas en gång. Uppgiften att säkerställa äktheten av e-kronorna utförs av deltagarens noder genom att verifiera att e-kronornas transaktionshistorik har en spårbarhet till Riksbanken som utgivare. Kontrollen att den specifika token som används i en transaktion är oanvänd, utförs av en speciell kontrollfunktion i nätverket som kallas notarienoden. I bilden nedan illustreras hur en transaktion i nätverket går till och vilka kontroller som görs av vilka parter för den implementering som gjorts under etapp 1 av e-kronapiloten.

Diagram 2. Så går en transaktion till

Maria ska överföra 60 e-kronor till Johan. Hon har en token på 100 e-kronor i ett digitalt värdefack hos sin deltagare.



1. Maria skickar en begäran till sin deltagare. Deltagaren kontrollerar att täckning finns. Maria signerar transaktionen.
2. Notarienoden kontrollerar att Marias token på 100 e-kronor inte använts tidigare. Den noteras som förbrukad och transaktionen signeras.

3. Marias deltagare skapar en transaktion med två nya tokens (en med 40 och en med 60 e-kronor) och fördelar dem i Marias värdefack och till Johans deltagare.
4. Johans deltagare kontrollerar äktheten på token värd 60 kr och lagrar den i hans digitala värdefack.

Som bilden visar är det den avsändande deltagaren som, redan när transaktionen inleds gör den första kontrollen av att betalaren faktiskt har e-kronorna som avses skickas. Den mottagande deltagaren validerar att e-kronorna som skickats är äkta genom en transaktionskedja som går att spara tillbaka till Riksbanken som utgivare. Notarienoden som är en teknisk funktion i nätverket som drivs av Riksbanken har endast en uppgift vilken är att kontrollera att tokens som används i en transaktion inte har använts tidigare. I nätverket sker alltså de nödvändiga kontrollerna som säkerställer att e-kronorna är äkta och att en transaktion kan genomföras. Processen skulle kunna likställas som en digital version av de kontroller vi själva gör när vi tar emot kontanter. Kontrollerna i det digitala nätverket görs dock av deltagarna och Riksbanken och inte av slutanvändaren själv som med de fysiska kontanterna.

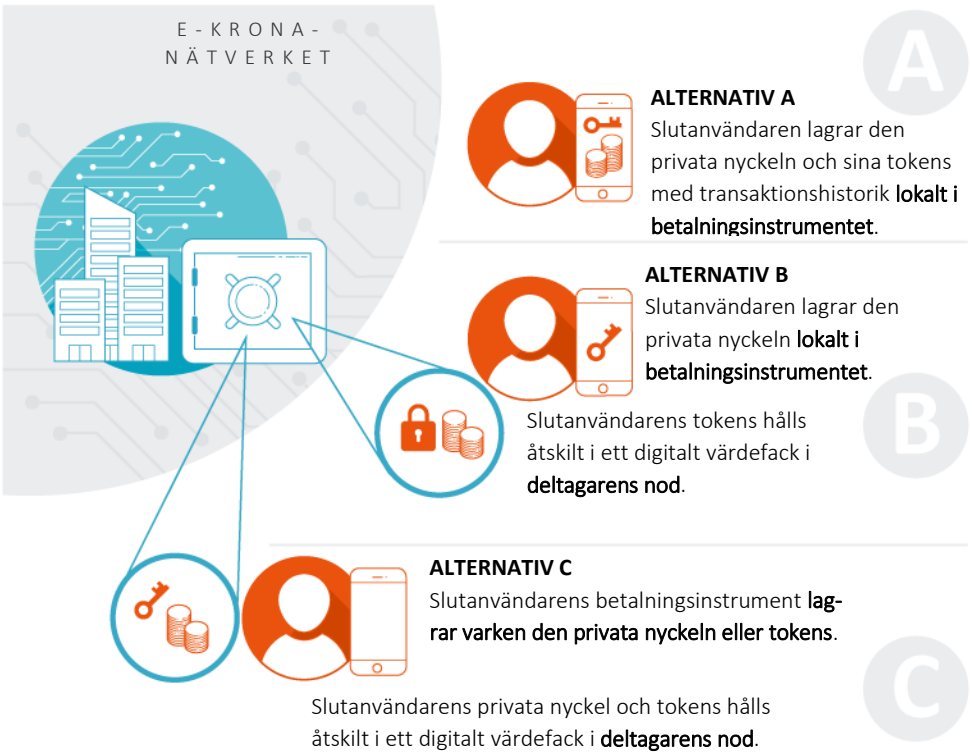
2.4 E-kronor kan förvaras på olika sätt

Olika betalningsinstrument som en app eller kort gör det möjligt att använda pengarna vi har på bankkonto under förutsättning att vi har tillgång till uppkoppling till internet eller en betalterminal. Men pengarna är inte lokalt lagrade och strikt knutna till det specifika betalningsinstrumentet, utan är fjärrlagrade i kontosystem hos de som tillhandahåller kontona, exempelvis banker.

Precis som med sedlar som lagras i en fysisk plånbok är det möjligt att lagra tokens och dess tillhörande information lokalt i ett betalningsinstrument. På så sätt så kan pengarna endast användas via det specifika instrumentet där pengarna lagras. I etapp 1 av e-kronapiloten är tokens med e-kronor inte lagrade på själva betalningsinstrumentet utan i digitala värdefack i noden hos den deltagare som slutanvändaren är ansluten till. Den privata nyckeln som ger rätt att använda e-kronorna är dock lagrad lokalt i den digitala plånboken som är kopplad till betalningsinstrumentet. Detta innebär att det endast går att styra pengarna från det specifika instrumentet. Den tekniska lösningen för e-kronapiloten erbjuder möjligheter att göra lagringen av e-kronorna och nyckeln till dessa mer eller mindre lik de fysiska kontanterna eller kontotillgodohavanden enligt alternativen nedan:

Diagram 3. Så förvaras e-kronorna

Tre alternativ för lagring av nycklar och tokens. I alla tre lagras deltagarens egna e-kronor i dess nod i ett digitalt valv.



A. Tokens med tillhörande information om e-kronorna och transaktionshistoriken lagras lokalt i ett specifikt betalningsinstrument tillsammans med den privata nyckeln som behövs för att använda e-kronorna. Detta är det mest kontantlika alternativet. Lagringen ger användaren en exklusiv kontroll över e-kronorna som är knutna till betalningsinstrumentet. Det ställs höga krav på den tekniska kapaciteten i betalningsinstrumentet, exempelvis ett kort eller en mobiltelefon, avseende lagring och hantering av information för att betalningsinstrumentet ska kunna lagra transaktionshistorik och validera äktheten lokalt som beskrivs i diagram 2. Lagringen innebär också, i likhet med kontanterna, att ett borttappat/trasigt betalningsinstrument där pengarna och nycklarna finns är svårare att få tillbaka, till skillnad från pengar som lagras i ett kontosystem. Den exklusiva kontrollen över e-kronorna innebär också att lösningen är svår att kombinera med vissa vardagliga tjänster för privatekonomin som exempelvis autogiro eftersom ingen annan än slutanvändaren via sitt betalningsinstrument har möjlighet att komma åt e-kronorna.

B. Tokens med tillhörande information om e-kronorna och transaktionshistoriken lagras i nätverket i deltagarens nod i ett digitalt värdefack åtskilt från deltagarens och övriga slutanvändares e-kronor. Nyckeln till dessa tokens lagras dock lokalt i betalningsinstrumentet vilket ger innehavaren exklusiv behörighet att utföra transaktioner med pengarna från det betalningsinstrument där

nyckeln finns lagrad. Som nämnts ovan är detta den variant som testats i etapp 1 av e-kronapiloten. Även denna lösning med den lokalt lagrade nyckeln som ger slutanvändaren exklusiv behörighet till e-kronorna är svår att kombinera med vissa vardagliga tjänster för privatekonomin som exempelvis autogiro.

C. Tokens med tillhörande information om e-kronorna och transaktionshistoriken tillsammans med nyckeln att bruka dessa lagras i nätverket i deltagarens nod åtskilt från deltagarens och övriga slutanvändares e-kronor. Alternativet har stora likheter med kontotillgodohavanden med kopplade betalningsinstrument. Lagringen hos deltagaren ger möjlighet för deltagaren att genomföra betalningar på begäran av slutanvändarna. Denna typ av lösning möjliggör därför finansiella tjänster som vi är vana vid idag, som exempelvis flera betalningsinstrument kopplade till samma konto och autogiro. Denna modell ställer därför också minst krav på det lokala betalningsinstrumentet vad gäller möjligheter att lagra och validera information.

3 Juridisk analys av testad lösning

Den juridiska analysen har utgått ifrån den tekniska lösningen för etapp 1 av e-kronapiloten. En analys har gjorts av de betalningsmedel som finns på betalningsmarknaden idag för att se om den testade lösningen skulle passa in under något av de tillgångsslag som finns i dag eller om det krävs ett nytt tillgångsslag. Vidare har vi tittat på hur aktuell teknisk lösning skulle förhålla sig till penningtvättsregelverken.

3.1 E-kronan som betalningsmedel

I den juridiska analysen av e-kronan som betalningsmedel har vi jämfört lösningen i etapp 1 av e-kronapiloten med de betalningsmedel vi har idag i form av kontanter, kontotillgodohavanden och elektroniska pengar. Vi har även jämfört den med kryptotillgångar. Den typ av blockkedje- och DLT-teknik som används i e-kronapiloten förknippas ofta med kryptotillgångar eftersom tekniken fick sitt stora genombrott med denna typ av tillgångar. Digitala centralbankspengar kategoriseras dock inte som en kryptotillgång. Anledningen är att centralbankspengar har en stat, en betrodd aktör, som utgivare och att staten garanterar betalningsmedlets värde.

Frågan om digitala centralbankspengar tillgängliga för allmänheten är relativt ny och har blivit aktuell först de senaste åren såväl i Sverige som internationellt. Därför saknas lagstiftning och även rådgivande exempel. En utgivning av en e-krona skulle med största sannolikhet kräva viss ny lagstiftning, oavsett dess modell, design och teknisk lösning.

På 1980-talet dematerialiserades finansiella instrument i Sverige. Innan denna utveckling hade aktiebrev i fysisk form representerat ägande i aktiebolag men nu var det inte längre nödvändigt att något fysiskt objekt var bärare av den ekonomiska rättigheten. Denna utveckling skapade ett snabbare och säkrare system för handel med finansiella instrument. Att ersätta eller komplettera fysiska pappersdokument med en digital tillgång är således ingen ny företeelse.

E-kronan jämförd med kontotillgodohavanden

Som den tekniska beskrivningen av etapp 1 ovan visat så finns det tydliga skillnader mellan de unikt identifierbara e-kronorna som distribueras av deltagare i e-kronanätverket och kontotillgodohavanden hos privata aktörer. Kontotillgodohavanden utgör en fordran på den privata aktören. I den aktuella lösningen förvaras e-kronan åtskilt i ett digitalt värdefack hos den deltagare som slutanvändaren har som distributör och ska inte ses som kontotillgodohavanden.

E-kronan jämförd med elektroniska pengar

Vissa institut har rätt att ge ut elektroniska pengar i enlighet med lagen om elektroniska pengar. I korthet kan elektroniska pengar beskrivas som ett betalningsmedel som kan vara utgivet av institut som inte har rätt att ta emot inlåning och där medlen är *förbetalda* vilket innebär att institutet inte får använda de mottagna medlen. Elektroniska pengar får inte heller uppbära ränta. Då utgivning av e-kronan bör ses som ett led i Riksbankens myndighetsutövning och utgivningen av e-kronan då sannolikt faller utanför lagen om elektroniska pengars tillämpningsområde så ger denna lagstiftning inte någon ytterligare vägledning för e-kronans utformning.

E-kronan jämförd med kontanter

De enda centralbankspengarna som finns tillgängliga för allmänheten idag är kontanter i form av sedlar och mynt. Det finns som nämnts en del likheter med den testade typen av lösning för e-kronan som gör att jämförelsen med kontanter och idén om e-kronan som en digital version av kontanter blir relevant. Exempelvis är e-kronorna likt sedlarna unikt identifierbara och kan endast skapas av Riksbanken. Att slutanvändaren, i den tekniska lösning som testats under etapp 1, har en exklusiv rätt att via sin privata nyckel bruka e-kronorna liknar också vårt sätt att använda fysiska kontanter. Likheterna gör att man kan argumentera för att e-kronan tillhör samma tillgångsslag som kontanter men i en digital form i stället för en fysisk. Om en e-krona till övervägande del ska likna kontanter så blir det dock svårt att tillämpa ränta på e-kronan då uttag av ränta kräver att en penningfordran finns.

En e-krona som representeras av tokens skiljer sig dock i viss mån från kontanter eftersom den är digital och förutsätter tekniska hjälpmedel, kommunikation och deltagare för att det ska gå att göra transaktioner. Detta medför att e-kronan möjligen inte bör anses tillhöra samma tillgångsslag som kontanter utan snarare bör ses som en ny typ av betalningsmedel. Med ett sådant synsätt skulle det sannolikt krävas större ändringar i lagstiftningen än om man skulle se e-kronan som samma tillgångsslag som kontanter men fördelen är att lagstiftningen skulle kunna utformas på ett sätt som passar e-kronan och dess specifika behov på ett mer ändamålsenligt sätt.

3.2 Penningtvätt

Verksamhetsutövare som tillhandahåller digitala pengar och betaltjänster omfattas av lagen om åtgärder mot penningtvätt och finansiering av terrorism. Detta innebär att aktörerna är skyldiga att ha kännedom om de kunder som använder deras tjänster och även möjlighet att spåra deras transaktioner. En e-krona skulle förmodligen även den omfattas av dessa lagar och regler. Distributionsmodellen i den testade lösningen distanserar Riksbanken från avtalsrelationer med slutanvändarna. Det ansvaret ligger i stället på deltagarna i nätverket som i rollen som distributörer erbjuder möjligheten att hålla e-kronor och utför transaktioner på uppdrag av slutanvändarna. På det här sättet skulle Riksbanken bibehålla sin nuvarande roll som utgivare av pengar och tillhandahållare av betalningsinfrastruktur medan känn-din-kund-kontroller och övervakning av transaktioner liksom idag skulle utföras av distributören.

Anonyma betalningar är tillåtna endast i mycket begränsad omfattning enligt dagens penningtvättslagstiftning och endast mindre belopp kan idag överföras anonymt. Konton får inte vara anonyma enligt gällande lagstiftning vilket man bör ha i åtanke när man fortsättningsvis diskuterar eventuella anonyma e-kronor. Det är möjligt att det kommer att kunna finnas anonyma e-kronor men de kommer att ha ett mycket begränsat användningsområde.

4 Lärdomar

Den tekniska lösning som har testats i e-kronapiloten har resulterat i ett nätverk där tokenbaserade e-kronor kan användas för transaktioner enligt den ovan beskrivna distributionsmodellen. Lösningen baserad på DLT och tokens är dock en ny teknik som är oprövad och vars förutsättningar att hantera massbetalningar i den magnitud och med de krav som en digital centralbankspeng kräver behöver utredas mer. Teknikens eventuella fördelar när det gäller att bygga upp ett nytt parallellt system för betalningar för ökad robusthet och den lokala lagringens alternativa möjligheter för offlinebetalningar är också områden som behöver undersökas närmre.

4.1 Ny teknik som måste utredas mer

Den tekniska lösning som testas i e-kronapiloten är en oprövad teknik för att ge ut digitala värdeenheter och hantera massbetalningar i den skala och med den säkerhet som en centralbanksutgiven digital krona kräver. Tekniken innebär att e-kronorna liknar de fysiska kontanterna på så sätt att det går att spåra utgivningen till Riksbanken och även i det att de är unikt identifierbara. Denna spårbarhet kräver dock att nätverket kan följa hur en utgiven e-krona har använts i transaktionerna som lett fram till den senaste transaktionen. Detta reser en del frågor, exempelvis hur tekniken ska kunna leva upp till banksekretessen vid digitala betalningar samtidigt som lösningen förutsätter att en kedja av tidigare transaktioner behöver verifieras för att säkerställa betalningsmedlets äkthet.

Det finns också utmaningar att prestandamässigt hantera massbetalningar med en teknik som bygger på DLT och tokens. Varje transaktion i den testade lösningen förutsätter att historiken tillbaka till Riksbanken som utgivare av e-kronor kan valideras samt att notarienoden kontrollerar att de tokens som ska användas inte har använts tidigare. Nya tokens innehållandes e-kronor skapas också i transaktionen. Detta är en informationsrik och prestandakrävande process. Det måste exempelvis gå att hantera långa kedjor av bakomliggande transaktioner och situationer där flera aktörer eller användare samtidigt begär att en token som innehåller en stor mängd e-kronor ska delas upp i flera tokens med mindre summor. Lösningen har under etapp 1 av e-kronapiloten levt upp till de prestandakrav som ställts i upphandlingen. Men detta har skett i en begränsad testmiljö och den nya teknikens möjligheter att hantera massbetalningar i stor skala behöver utredas och testas ytterligare.

4.2 Lokal lagring av nycklar och tokens samt betalningar offline

Hur lagring av nycklar och pengar ska se ut i en e-krona bör i slutändan avgöras av vilka funktioner som ska prioriteras hos en e-krona. En fråga som lyfts som viktig för en e-krona är möjligheten att betala offline och där ger olika sätt att lagra nycklar och tokens olika möjligheter[2]. Under etapp 1 av e-kronapiloten har inte offlinefunktionalitet testats men nedan förklaras hur den testade lösningen är tänkt att fungera vid betalningar offline.

Om nycklar och tokens lagras lokalt, i enlighet med alternativ A ovan, ska det enligt lösningen gå att betala i offlineläge: betalaren och mottagaren ska kunna genomföra en transaktion och även validera att de lokalt lagrade e-kronorna är äkta när mottagaren tar emot transaktionen. Det innebär att den validering som görs av deltagaren i diagram 2 görs lokalt i slutanvändarens betalningsinstrument istället. Men det skulle inte gå att avveckla transaktionen, det vill säga slutgiltigt reglera den, i offlineläget eftersom notarienoden i nätverket först måste kontrollera att tokens inte har använts tidigare. Slutlig kontroll och avveckling kan alltså göras först när någon av parterna är online igen. En sådan lösning skulle ändå kunna erbjuda ett alternativ för betalningar i offlineläge där token faktiskt flyttas, mellan betalaren och mottagaren, jämfört med dagens offlinebetalningar som endast är möjliga via krediter hos vissa kortutgivare.

Riksbanken har ännu inte testat offlinelösningen och ännu inte utrett hur ett digitalt betalningsmedel ska kunna fungera säkert såväl online som offline. Riksbanken avser därför att fortsatt undersöka frågan. Det faktum att nycklar och tokens lagras lokalt i betalningsinstrumentet innebär dock att sårbarheten ökar då båda delarna kan förloras på samma sätt som kontanter som förvaras i en fysisk plånbok. Det är ännu osäkert i vilken utsträckning det skulle vara möjligt att få tillbaka de lokalt lagrade pengarna och hur komplicerad processen skulle vara om betalningsinstrumentet går sönder eller förloras. En annan utmaning är de nämnda kraven på teknisk kapacitet som offlinebetalningar ställer på betalningsinstrumentet. Även det ska undersökas vidare.

Som nämnts ovan så behöver dock inte en lösning baserad på tokens innebära att man lagrar nycklar och tokens lokalt. Det är möjligt att hantera nycklar och tokens på ett sätt som påminner mer eller mindre om hur vi lagrar våra digitala pengar på konton idag.

4.3 Tokensmodell med saldotak och ränta

En digital centralbankspengs potentiella effekter på den finansiella stabiliteten är en fråga som ofta lyfts i debatten om CBDC:s (*Central Bank Digital Currencies*). Möjligheten att kontrollera utbudet och efterfrågan genom saldotak på plånböcker och ränta på e-kronan är något som också testats under etapp 1. Den tekniska lösningen med tokens som bärare av e-kronor är förenlig med såväl saldotak som positiv och negativ ränta. En positiv ränta skulle innebära att Riksbanken betalar ut ränta i form av nya tokens med e-kronor till innehavare av e-kronor (deltagare och slutanvändare) via

[2] Offline definieras här som avsaknad av internetuppkoppling men tillgång till elektricitet.

deltagarna, likt distributionsmodellen ovan. En förutsättning för att det ska vara möjligt med negativ ränta inom den tekniska lösningen är dock att nycklarna till tokens inte lagras lokalt i betalningsinstrumentet (som i A och B i förklaringarna ovan). Detta eftersom att lokal lagring innebär att endast det specifika betalningsinstrumentet har tillgång till och kan utföra transaktioner med e-kronorna. En negativ ränta skulle innebära att det på begäran av Riksbanken genomförs en transaktion av e-kronor motsvarande räntan från betalningsinstrumentet till Riksbanken som mottagare. Då det inte kan förutsättas att slutanvändaren alltid är online, tillgänglig, har tillgång till sitt betalningsinstrument och utför transaktionen är inte negativ ränta förenligt med en lokal lagring av e-kronor med exklusiv kontroll hos slutanvändaren kopplat till betalningsinstrumentet. Vid lagring av nycklar och tokens hos deltagaren är det däremot förenligt tekniskt. Hur förenlig en räntebärande e-krona, positiv som negativ, är med en distributionsmodell som testats under etapp 1 är dock en bredare fråga än de rent tekniska möjligheterna och begränsningarna.

4.4 Ett parallellt nätverk gör betalsystemet mer robust

Ett mål för e-kronan skulle kunna vara att öka motståndskraften i infrastrukturen för digitala betalningar. Den tekniska lösningen baserad på DLT och tokens innebär att man etablerar en infrastruktur som till stora delar skulle kunna fungera parallellt med dagens infrastruktur för betalningar. Det är därför intressant att jämföra de båda infrastrukturerna med utgångspunkten att e-kronasystemet ska vara så fristående och parallellt som möjligt.

Sådant som bör studeras vid en jämförelse är bland annat robusthet, prestanda, kommunikation och adressering och om det är möjligt att avveckla betalningar. En djupare utredning är nödvändig för att ta reda på om den nya tekniken når upp till de krav som ställs på infrastruktur för betalningar idag och om den är mer eller mindre lämplig än redan etablerade lösningar för massbetalningar när det gäller att ansluta deltagare till systemet, hålla hög effektivitet och låg resursförbrukning.

4.5 Legala frågor

Vid den legala analysen av den lösning som testats i etapp 1 av e-kronapiloten har följande lärdomar kunnat dras.

E-kronan och ränta

Om en token legalt sett anses utgöra ett *betalningsmedel med fristående värde,* det vill säga *kontantliknande*, så skulle man eventuellt kunna använda sig av de rättsliga principer som gäller för kontanter och applicera dem på e-kronan.

Om ränta ska kunna utgå på e-kronan bör man istället överväga att e-kronan blir ett tillgångsslag som innebär att e-kronan har en fordranskonstruktion. En *token* skulle då kunna klassificeras som *ett löpande skuldebrev i digital form*. Att samtidigt prata om *ränta på e-krona* och *kontantliknande* e-krona som beskrivits i stycket ovan bör undvi-

kas eftersom kontanter enligt svensk rätt sannolikt utgör ett betalningsmedel med fristående värde. En *token* borde i sig inte hindra att ränta (positiv och negativ) utgår så länge denna token klassificeras som någon typ av penningfordran.

Staten som garant för e-kronans värde

Riksbanken/staten bör kunna ses som garant för e-kronan även när det finns intermediärer i e-kronasystemet eftersom Riksbanken ska vara ensam utgivare av e-kronan. Det återstår att utreda om Riksbanken även när det kommer till testad lösning för e-kronan i vissa specifika fall bör åta sig att lösa in e-kronor direkt från allmänheten.

E-kronan, banksekretess och personuppgifter

Den tekniska lösning som testats innebär att äkthetskontroll av tokens görs genom att transaktionshistorik som innehåller information om tidigare transaktioner följer med till mottagaren. Information i transaktioner med e-kronor om andra kunder och andra deltagare än de kunder och deltagare som är involverade i en transaktion måste därför skyddas på ett sådant sätt att banksekretess upprätthålls och personuppgifter inte röjs. Riksbanken analyserar för närvarande i vilken utsträckning den information som lagras i transaktionshistoriken är att betrakta som information som omfattas av banksekretess samt om den utgör personuppgifter.

5 Nästa steg

Riksbanken har beslutat att förlänga avtalet med Accenture som teknisk leverantör för att fortsätta testa den tekniska lösningens möjligheter ytterligare. Fokus för etapp 2 kommer vara att inkludera potentiella distributörer av e-kronor som deltagare i nätverket för att testa hur en integration med deras interna system kan fungera med e-kronanätverket. Lösningens möjligheter till olika sätt att lagra tokens och dess nycklar samt dess möjligheter till offlinebetalningar kommer också att utredas närmare. Även fortsatta tester av lösningens prestanda för massbetalningar kommer att prioriteras under etapp 2.

Etapp 1 av e-kronapiloten har resulterat i ett e-kronanätverk byggt på R3:s Corda blockkedjeplattform i en isolerad testmiljö. Centrala delar av systemet har simulerats under första året, som exempelvis likviditetsförsörjning via Riksbankens avvecklingssystem, RIX, och deltagare i nätverket med rollen som distributörer av e-kronor. De simulerade aktörerna, slutanvändarna och betalningsinstrumenten (app, kort och smartklocka) och dessas funktioner har testats av Riksbanken.

Riksbanken har beslutat att förlänga avtalet med Accenture ett år till. Syftet med förlängningen är att ytterligare bredda och fördjupa kunskapen hos Riksbanken om hur en utgivning av en e-krona skulle kunna förverkligas, både tekniskt och verksamhetsmässigt. Genom att fortsätta arbetet med den testade tekniska lösningen kan Riksbanken fortsätta att utreda och verifiera såväl de tekniska som de regulatoriska frågorna som hör till en digital centralbankspeng tillgänglig för allmänheten. Arbetet med den specifika lösning som testas i e-kronapiloten ger kunskaper om just den lösningen, men är också en utgångspunkt för jämförelser med andra typer av lösningar för en potentiell e-krona. Nedan följer några fokusområden som Riksbanken beslutat att arbeta vidare med i det tekniska arbetet under etapp 2:

Integrera med potentiella deltagares interna system

Deltagarna i nätverket spelar i denna tekniska lösning en avgörande roll för såväl distributionen av e-kronor till slutanvändarna som transaktionerna i nätverket. Under etapp 2 avser Riksbanken därför att låta riktiga aktörer på marknaden, som skulle kunna vara potentiella deltagare i ett e-kronanätverk, testa denna tekniska lösning.

Utveckla offline-funktionen

Möjligheterna att betala offline är som nämnts en prioriterad funktion som ska utredas närmare. Under etapp 1 har vi endast gjort en teoretisk analys av lösningens möjligheter. Under etapp 2 ska en offlinelösning med lokal lagring av nycklar och tokens implementeras och användas i vidare tester som kan ge kunskaper om lösningens möjligheter och begränsningar.

Möjligheten att lagra nycklar och tokens på olika sätt

Den tekniska lösningen erbjuder olika sätt att lagra både den privata nyckeln till tokens och tokens med e-kronor. De olika alternativen som nämnts ovan har olika för- och nackdelar vilket gör att det är intressant att utvärdera möjligheten att kunna kombinera de olika alternativen och använda dem för olika ändamål.

Utveckla adresseringsfunktionen

Att det är enkelt att göra betalningar inom nätverket är en förutsättning för att en e-krona ska bli användarvänlig. Hur adresseringsfunktionen kan designas ska utredas vidare under etapp 2.

Utvärdera och förbättra prestanda och skalbarhet i e-kronanätverket

Vilka möjligheter som finns för att uppnå tillräcklig prestanda och skalbarhet för massbetalningar är frågor som ofta diskuteras när det gäller DLT- och tokenbaserade lösningar. Under etapp 2 ska detta utredas och testas än mer.

Integration mot en befintlig POS-terminal

E-kronan behöver kunna användas för betalningar i den dagliga handeln vid det fysiska inköpsstället. För att detta ska fungera så är det viktigt att e-kronan stöds av de betalterminaler som hanterar övriga digitala betalningar. Under etapp 2 ska en sådan integration testas.

Utredning av e-kronanätverkets infrastruktur

Syftet med detta fokusområde är att utvärdera infrastruktur, säkerhetsaspekter, kommunikation inom nätverket och ut ur nätverket, ansvarsfördelningen mellan deltagare samt att identifiera potentiell nätverksinfrastruktur.

SVERIGES RIKSBANK
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUKTION SVERIGES RIKSBANK
ISSN ISSN. (online)