Blockkedjeinspirerade tekniklösningar för redovisning, revision och skatt

Ett samverkansprojekt med FAR, Skatteverket, Kairos Future, Visma, SEB, Fortnox och FAR:s medlemmar PwC, Deloitte, Grant Thornton och KPMG.
Januari 2019

Sammanfattning

Denna rapport sammanfattar resultatet av ett projekt där FAR, Skatteverket, Kairos Future, Visma, SEB, Fortnox och FARs medlemmar Deloitte, PwC, Grant Thornton och KPMG medverkat.

Syftet med projektet är att identifiera utmaningar i dagens verksamheter kopplade till redovisning, revision och skatt. Därefter att beskriva dessa utmaningar samt beskriva möjligheter att lösa dessa med hjälp av digitala informationskedjor, exempelvis blockkedjan.

Vi vill avmystifiera blockkedjan, göra den teknik och de principer som blockkedjan bidragit till att tydliggöra, göra tillgänglig och begriplig för fler. Det stimulerar till att lära sig mer och utveckla nya tankar, processer, system och i slutändan ett roligare och mer värdeskapande arbete i branschen för redovisning, revision och skatt samt bland företagen.

Den övergripande utmaningen är att skapa förtroende för digitala processer, handlingar, identiteter m.m. hos alla inblandade parter. Vi vill öka effektiviteten, minska risker och försvåra medvetna och omedvetna fel hos företagen. Vi vill också göra detta utan att kompromissa med anonymitet.

Det vanligaste sättet att försöka lösa dessa utmaningar idag är att samla in mer data i centrala databaser. Att göra det innebär emellertid ofta säkerhetsrisker och utmanar såväl integritet som anonymitet.

Blockkedjan har i The Economist beskrivits som en förtroendemaskin, ”trust machine”. Ett resultat av projektet är att vi betraktar tekniken som en uppsättning verktyg som kan kombineras på olika sätt för att skapa förtroende. Dvs, det är inte en teknik och i synnerhet inte en blockkedja som föreslås i lösningarna.

Resultatet av projektet är fem förslag på lösningar inom följande områden:
1. Digital kvittohantering
2. Personalliggare
3. Realtid/SINK (Särskild inkomstskatt för personer som inte bor i Sverige)
4. Fullmakter
5. Företagsuppgiftstjänst

För tre av de ovanstående lösningarna (Digital kvittohantering, Personalliggare och Fullmakter) bedömer vi att förslagen som beskrivs i rapporten är mycket bra lösningar för att skapa samhällsnytta. När det gäller SINK finns det ett par beroenden av andra processer som behöver utredas och eventuellt lösas innan lösningen kan realiseras. För den femte lösningen, Företagsuppgifter, finns det ett par länder som har intressanta lösningar för några olika typer av data. Det finns ett behov av att se vilka olika grupper av data som bör vara i fokus samt en bättre kunskap om de lösningar som idag finns i andra länder och deras för- och nackdelar.

Sammanfattningsvis är resultatet mycket lovande. Vi bedömer det som mycket troligt att det går att skapa samhällsnytta på en bra bit över tio miljarder per år enbart i Sverige i ett fem till tio års perspektiv. Det bedöms angeläget att man fortsätter att utreda och arbeta vidare med processer, juridik och teknik på samtliga fem identifierade områden.

Innehåll

Inledning

Detta är en rapport som sammanfattar ett projekt som fokuserat på att undersöka möjligheterna med blockkedjeteknik och även annan teknik som kan sägas inspireras av blockkedjetekniken. Utgångspunkten har varit att identifiera lösningar inom områdena redovisning, revision och skatt. Hypotesen är att vi kan effektivisera och underlätta arbetet bland företagen och skapa samhällsnytta.

Blockkedjetekniken har sagts innebära några av de mest samhällsomvälvande möjligheterna de senaste decennierna. Dollarn ska ersättas som betalningsvaluta för världen, guldet ska ersättas som reservvaluta för centralbanker, världshandelns flöden ska kontrolleras säkert och virtuella företag ska agera på marknaderna styrda av teknik utom räckhåll för nationer och lagstiftare. Nu har det emellertid gått tio år sedan Bitcoin lanserades och hittills har endast värdet på krypovalutor kommit i närheten av de visioner som utlovats.

Men hade The Economist fel när de kallade blockkedjan The trust machine? Kanske inte, men tolkningen av förtroendemaskinen har troligtvis fokuserat för mycket på en världsomspännande teknik, rent av en enda blockkedja. I detta projekt har vi försökt titta på möjligheterna med den nya tekniken men fokuserat på att se nya möjligheter snarare än att använda blockkedjetekniken i sin helhet. Ett begrepp som används i rapporten är ”digitaliserade informationskedjor”, ett begrepp som kan tolkas som ”en teknik som gör att data inte kan manipuleras utan följas så som i en kedja”. Eftersom teknik ger möjligheter att skapa förtroende, är detta något som vi varit nyfikna på. Vi har i detta projekt även försökt att hålla

ambitionerna på en rimlig nivå, vilket kanske skiljer oss från inställningen från andra som arbetar med blockkedjeteknik. Vi är nöjda om vi lyckas spara ett par miljarder kronor per år i Sverige, något vi tror är fullt möjligt.

Grundhypotesen har varit att blockkedjan har synliggjort ett antal tekniska verktyg som kan användas för att lösa gamla problem på nya sätt. Genom att samla en grupp nyfikna personer från ett par nyckelaktörer som verkar inom redovisning, revision och skatt kan vi kanske identifiera nya möjligheter att öka förtroendet, minska risker, spara tid och pengar samt minska medvetna och omedvetna fel.

Syfte

Syftet är att identifiera utmaningar i dagens verksamheter kopplade till redovisning, revision och skatt. Därefter att beskriva dessa utmaningar samt beskriva möjligheter att lösa dessa med hjälp av digitala informationskedjor, exempelvis blockkedjan.

Målsättningen är att de deltagande organisationerna ska se fler möjligheter till lösningar på dagens problem och därigenom stimuleras till att ta fram nya tekniska lösningar i syfte att åstadkomma digitala informationskedjor som kan komma att få stor nytta.

Ambitionen är också att sprida kunskapen om dessa lösningar till flera organisationer och individer. Vi vill avmystifiera blockkedjan, göra den tillgänglig och begriplig för fler. Det stimulerar till att lära sig mer och utveckla nya tankar, processer, system och i slutändan ett roligare och mer värdeskapande arbete både i de aktuella branscherna och i näringslivet i övrigt.

Medverkande

Medverkande i projektet har varit FAR, Skatteverket, Visma, Kairos Future, Fortnox, SEB samt FARs medlemmar PwC, Deloitte, Grant Thornton och KPMG.

Från projektgruppen har följande medverkat:
Karin Apelman, FAR
Dan Brännström, FAR
Camilla Carlsson, FAR
Lena Henriksson, FAR
Bengt Skough, FAR
Göran Sundin, Skatteverket
Therése Allard, Skatteverket
Pablo Dias Taguatinga, Skatteverket
Björn Erling, Skatteverket
Patrik Lindmark, Skatteverket
Eric Thorén, Skatteverket
Patrik Cardell, Visma
Jennie-Ann Karlsson, Visma
Håkan Runquist, Visma
Henrik Olsson, PwC
Jonas Hagström, PwC
Lars Alm, Fortnox
Cesar Nilsson, Fortnox
Fredrik Nilsson, KPMG
Jens Gullfeldt, Deloitte
Magnus Folkesson, SEB
Johan Hörmark, SEB
Magnus Kempe, Kairos Future

Intervjuer och inbjudna till workshops:
Amey Rajput, Tech Mahindra
Anna Eriksson, DIGG
Annika Follin, Bolagsverket
Christian Landgren, iTeam
Einar Persson, iTeam
Jesper Granlund, Deloitte
Johan Bergsten, Bolagsverket
Jürgen Sûvalov, Estonian Information System Authority
Lars Åke Lundberg, IT- och Telekomföretagen/Svenskt Näringsliv
Martin Runosson, Aspia
Olle Kinnman, Deloitte
Patrik Nilsson, Företagarna
Roger Fagerud, DIGG
Zizzi Marten, Tech Mahindra

Ansvarsbegränsning
Ingen organisation eller person tar ansvar för innehållet i rapporten. Rapporten är i huvudsak, men inte enbart, författad av Magnus Kempe.
I rapporten används ordet ”vi” och då avses projektgruppen, även om projektgruppen inte tar ansvar för eller är enig kring de formuleringar som finns i rapporten.

De legala hinder som finns för att få de möjliga lösningarna på plats har inte utretts. Rapporten gör inte anspråk på att de olika lösningarna ryms inom gällande lagstiftning. Rapporten ska vara en inspirationskälla till fortsatt arbete med de möjligheter som blockkedjeinspirerad teknik ger.

Blockkedjeinspirerad teknik

Ordet blockchain blev allmänt känt i och med publiceringen av det White Paper som beskrev uppbyggnaden av Bitcoin. Där beskrevs hur grupper av krypterad data, block, kopplas ihop i en kedja, chain. Eftersom kombinationen av några kända och mindre kända tekniker visade på ett antal revolutionerande möjligheter blev blockkedjan efter ett par år ett teknikbegrepp. I detta projekt vill vi inspireras av de möjligheter som blockkedjan synliggjort, men också se möjligheter där man inte använder tekniken blockkedjan i sin helhet. Vi är mer intresserade av samhällsnytta och möjligheter än att använda en teknik som kan beskrivas som blockkedjan.

Vad en blockkedja ska omfatta för teknik för att kallas blockkedja finns det också olika uppfattningar om. Ibland används t.ex. ordet Distributed ledger eller Distributed Ledger Technology (DLT). Det finns utomordentligt intressanta diskussioner kring juridik, teknik och filosofi som blockkedjan har bidragit till. I denna första del av rapporten finns några synsätt och perspektiv som blockkedjan inspirerar till. När det gäller lösningarna som beskrivs försöker vi emellertid ha en pragmatisk ansats. Vi använder en teknik som vi har ett starkt stöd för att påstå att den fungerar, oavsett vad den kallas.

En grundprincip i projektet är att vi försöker identifiera möjligheter med tekniker som skiljer sig från ytterligheterna. Den allmänna är uppfattningen är att det två ytterligheterna är blockkedjan och en central databas.

Dessa begrepp kan beskrivas på följande sätt:

1. Blockkedja: I extremfallet är blockkedjan en öppen, distribuerad databas, d.v.s alla databaser som deltar i nätverket har möjlighet att se och validera all registrerad information och informationen är densamma i alla databaser.
2. Central databas: I extremfallet central databas finns det i stället en enda databas som samlar in och kontrollerar all information.

Dessa två synsätt har också kopplingar till styrning, där den förra kan beskrivas som ”code is law”, d.v.s. det behövs ingen lagstiftare eftersom tekniken i sig själv reglerar vilka utfall som ges till olika maskiner, personer och organisationer. Ingen lagstiftare kan till exempel hindra pengar från att utbetalas i Bitcoin. Det är åtminstone ambitionen med systemet. I Sverige är synen på staten i huvudsak positiv och behovet av att upprätta en infrastruktur där lagstiftningen inte gäller eller kan försvaras är sannolikt mindre än på många andra platser, åtminstone under de kommande åren.

Det andra alternativet är i stället centralisering av informationen, d.v.s. en myndighet eller ett företag samlar in all information och gör sedan sin bedömning av hur t.ex. en lag ska tolkas när den (allt mer fullständiga) informationen samlats in. Nackdelen med detta system är att om staten, eller företag och individer, ges möjlighet att samla in fullständig information förlorar människor stora delar av sin integritet och sitt privatliv. Stora mängder data som samlas in och analyseras är en grund för makt som kan missbrukas både av innehavaren och av den som på ett eller annat sätt kommer över informationen. Ett steg för att reglera denna fara är The General Data Protection Regulation (GDPR) och USA:s motsvarighet The California Consumer Privacy Act of 2018. I praktiken är dessa regleringar emellertid omständliga och otillräckliga för att uppnå sitt syfte. För närvarande är dessutom tolkningen av dessa lagar inte tydlig eftersom

det saknas rättsfall. Ett exempel på detta är att det finns olika tolkningar av vad som ska betraktas som en personuppgift och vad som inte ska betraktas som en personuppgift. En indikation är att pseudonymisering inte är tillåten men anonymisering är tillåten. Regleringarna bromsar vissa problem med personuppgifter i delar av världen, men de hindrar den inte. Det finns också en risk att mindre nogräknade nationer med sämre skydd för personer och företags data kan utveckla bättre tjänster, till exempel bättre AI, med bättre tillgång till data. En alltför strikt tolkning av GDPR kommer att försvåra konkurrens med nationer och företag som har lättare att utveckla bättre teknik. Blockkedjetekniken, den krypteringsteknik och de möjligheter som tekniken synliggjort innebär att det finns stora möjligheter att kombinera den bästa av två världar, d.v.s. säker data, anonymisering och samtidigt kontroll och avancerade analystjänster t.ex. AI.

I efterdyningarna av de stora prisfall som skett på kryptovalutor under 2018 kan det vara lockande att vifta bort tekniken och tro att vi nog inte behöver lära oss något om blockkedjan. Vi hoppas att denna rapport vidgar perspektivet och stimulerar till att lära mer om de olika teknikerna och synsättet som blockkedjan bygger på. Många av dessa tekniker är sannolikt en förutsättning för att bygga en värld där demokrati, privatliv m.m. kan fortsätta existera så som vi ser på dem idag.

Det växande beroendet av Internet som infrastruktur i samhället är ytterligare ett skäl till att det är angeläget att hitta möjligheter att säkra upp denna infrastruktur med krypteringsteknik, där blockkedjan är ett exempel. Det finns ett växande hot mot Internet i form av uppkopplade datorer och inte minst andra saker än datorer, det som brukar kallas Internet of Things (IoT). Det är idag svårt att kontrollera om de uppkopplade enheterna är manipulerade. Alla dessa uppkopplade enheter riskerar därför att bli hackade och kan då angripa Internet, t.ex. genom överbelastningsattacker.

Grundtesen är att det finns ett ökat behov av att samla in delar av data och att dela med sig av delar av data, men att vi behöver använda den nya tekniken som finns för att göra detta på ett klokare sätt. Blockkedjetekniken har banat väg för en rad nya innovationer och idéer som inte kan vänta längre på att bli verklighet. Hypotesen i inledningen av detta projekt har varit att det finns flera olika användarfall som enbart i Sverige kan spara många miljarder varje år, och att det i flera fall kan vara relativt enkelt att realisera dessa.

Dela kontroll och bygg förtroende

”We must move beyond transactions and to more meaningful relationships. Must achieve right balance of being in touch and in control. The paradox is that the more we are in control, the more out of touch we are. The more we give up control, the more we become in touch.”
AG Lafley Chairman, President, CEO of P&G at ANA conference Masters of Marketing 2006

Om AG Lafley hade hållit motsvarande tal idag skulle han kanske ha sagt:”The more we give up control, the more we build trust”. Blockkedjetekniken och den breda grupp av andra tekniker vi identifierat som intressanta i projektet bygger på samma princip. Genom att frånhända oss kontroll bygger vi förtroende. Ett konkret exempel på detta är offentlighetsprincipen. Genom att möjliggöra för medborgare att begära ut mötesprotokoll, beslut, handlingar etc. från offentliga aktörer fråntas de offentliga aktörerna viss kontroll. De kan i normalfallet inte vägra att lämna ut materialet som efterfrågas. Det minskar deras kontroll. Det ökar samtidigt förtroendet för offentlig sektor. Misskötsel kan förhållandevis

lätt upptäckas. I ett slutet system med full kontroll kan medborgarna och journalister få betydligt svårare att hitta bevis för felaktigheter och brottslighet. Den förlorade kontrollen har samtidigt ett pris. Det kan därför vara olämpligt att dela med sig av fullständig data. Digitaliseringen har gjort att offentlighetsprincipen fungerar sämre än tidigare i vissa situationer. Känsliga personuppgifter kan exempelvis säljas i större skala till lägre kostnad jämfört med tidigare. Privata företags uppgifter omfattas inte heller av samma krav på öppenhet som myndigheter. Exempelvis kan privata företag hemlighålla styrelseprotokoll. I det fallet gör samhället bedömningen att inhämtning av fullständig data är konkurrenskänsligt, riskabelt och en inskränkning i privatlivet. I stället begär olika myndigheter in kontrolluppgifter. Med dessa som stöd blir det svårare för företaget att missköta sig. Ytterligare en kontroll är revisorernas granskningar. Genom att tvinga företag att låta en tredje part granska företagets finansiella rapportering blir företaget därmed tvunget att avhända sig kontroll. På detta sätt får vi mer förtroende för företagen som granskas. Även ett traditionellt avtal är ett exempel på hur vi avhänder oss kontroll genom att signera ett avtal och låta ett exemplar av detta finnas hos någon annan part. Det blir då lättare för den andra parten att bevisa vad som är överenskommet i avtalet och förtroendet ökar.

Digital information kan manipuleras

I den digitala världen har vi problem med att bevisa händelseförlopp. Om en enskild aktör har full kontroll över data kan denna data manipuleras. Av det skälet godkänner vi oftast inte namnteckningar som är skrivna med digitala bokstäver. Den som har ett digitalt kontrakt kan manipulera innehållet, t.ex. byta ut namnet eller ändra i villkor, belopp, datum eller liknande. Offentlighetsprincipen räcker med andra ord inte för att vi ska

få förtroende för digitala handlingar och processer. Modern krypteringsteknik, där blockkedjan är ett exempel, har dock olika lösningar för att vi ska uppnå detta förtroende.

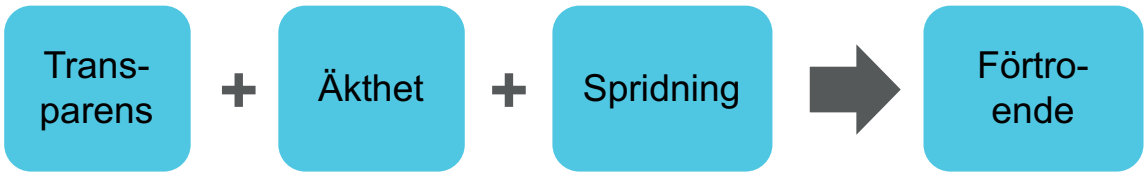
I praktiken behöver vi komplettera och reglera transparensen. Vi vill inte göra alla handlingar och händelser i vår omgivning transparenta för alla och vi vill säkerställa äkthet. Det innebär att om vi får ut en offentlig handling eller ett avtal som är digitalt behöver vi kunna säkerställa att detta är äkta. Om t.ex. ett protokoll från ett möte på en myndighet är möjligt att manipulera ger transparensen kring detta protokoll i efterhand inte samma förtroende. Kan vi däremot säkerställa äktheten och dessutom enkelt få tillgång till protokollet skapas förtroende och möjlighet att utkräva ansvar.

Förtroende från heder, kontroll eller spridning

I sin utmärkta och prisbelönta avhandling och bok Ordens Kraft: Politiska eder i Sverige 1520-1718 beskriver författaren Sari Nauman hur eder använts för att skapa förtroende mellan regenter och undersåtar. Nauman beskriver hur stor vikt man la vid eder, deras muntliga uttalande, sammanhanget och vittnen till ederna. Situationen liknar den som beskrivs i Game of Thrones. Eder är inget människor tar lätt på. Personer som bryter sina eder har förlorat sitt förtroende och det är mycket allvarligt. Nauman beskriver också hur sämre tillit och regentens frånvaro, bland annat på grund av krig, bidrog till att öka betydelsen av de skriftliga dokument som regenterna undertecknade. Kontroll ersatte tilliten. Medan heder var avgörande för tillit på 1500-talet har samhället allt sedan dess förlitat sig allt mer på skriftlig dokumentation snarare än personers heder, ära och goda vilja. Än idag ska vittnen närvara fysiskt i domstolar och ofta vittna under ed, men betydelsen av de skriftliga handlingarna och deras formuleringar har otvetydigt ökat de senaste århundradena.

Det pågår en tilltagande diskussion kring falska nyheter, källkritik m.m. som kan hänföras till digitaliseringen. Begreppet ”post-truth” utsågs 2016 till årets internationella ord av Oxford Dictionary. Data sprids idag i snabb takt och att kontrollerabåde innehållet och avsändaren är ofta svårt, inte minst eftersom information sprids över större geografiska områden. I den digitala världen har spridning och kännedom fått en större betydelse för tillit. Det har emellertid skett på bekostnad av kontroll och äkthet. Vi ser därför ett kraftigt ökat behov av att säkerställa just kontroll och äkthet.

Blockkedjetekniken bygger på krypteringsteknik och omfattar möjligheten att säkerställa just detta. Blockkedjetekniken kan till exempel svara på frågor som ”vad är äkta och enligt vem?”. Dagens allt kraftfullare teknik för AI och genmanipulering har gjort frågor om etik kring exempelvis AI mycket aktuella. Kanske innebär det att vi i framtiden behöver arbeta mer kring frågor om heder, etik och moral. Det är emellertid inte okomplicerat. Kanske är samhället redan på väg i en riktning där människor fäster större vikt vid avsändarens karaktär och åsikter än budskapets äkthet.

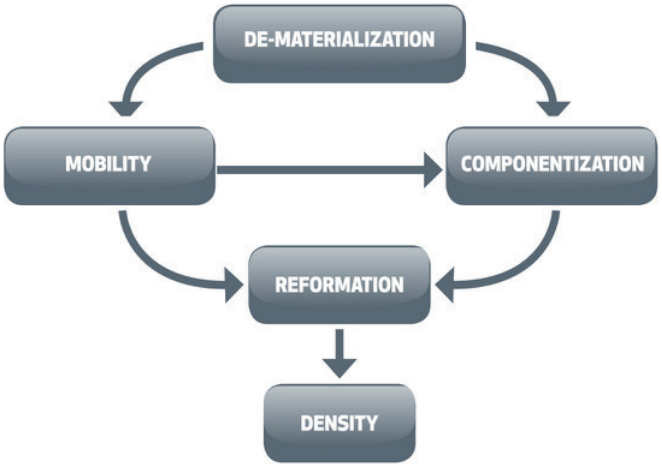


Sammantaget tycks transparens, äkthet och spridning bidra till ökat förtroende. Förtroende minskar transaktionskostnader. Enligt vissa forskare består moderna ekonomier av närmare 70 procent transaktionskostnader.[1] Den potentiella samhällsnyttan av att öka förtroende hos aktörer, processer, data med mera är med andra ord mycket stor. Blockkedjan kan förstärka förtroendet främst genom att bidra till kontroll och äkthet, vilket är något som den digitala världen har problem med idag.

[1]Institutions and Economic Theory: The Contribution of the New Institutional Economics, Eirik G. Furubotn, Rudolf Richter

Dematerialiseringen av värde

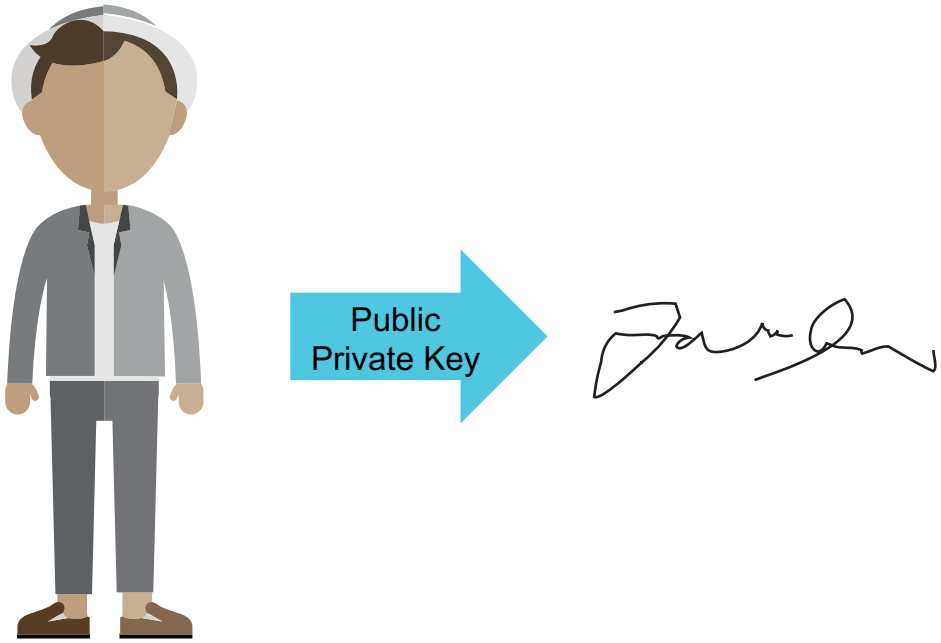
Richard Normann, en känd svensk managementforskare och författare, beskrev i sin bok ”När kartan förändrar affärslandskapet” att de viktigaste bärarna av värden i samhället och företagen är på väg att bli avmaterialiserade. Några exempel på vad som allt oftare är värdefullt idag är symboler, varumärken, algoritmer, information, data, kunskap och relationer. Alla dessa är viktlösa. Två stora konsekvenser av denna utveckling är enligt Normann komponentisering och rörlighet. Komponentisering innebär exempelvis att priset kan separeras från en produkt, något som har banat vägen för nya tjänster avseende prisjämförelser. Ett varumärke kan separeras från en produkt. Ett känt bilmärke kan därför sälja licenser för att använda sitt varumärke till andra produkter i olika geografiska områden. Detta var inte möjligt i en värld där bilens värde var enbart produkten och inte varumärket, vilket var fallet då bilen inte kunde köras i flera delar av världen samtidigt. När programvara är den viktigaste delen av motorn kan tillfälliga uppgraderingar säljas på distans, vilket är mycket enklare än att ta in bilen på en verkstad och ändra fysiska komponenter i motorn. För att inte tala om att byta ut hela motorn.



Dekonstruktion av data

Blockkedjan och modern kryptografi har gjort dematerialiseringen än mer sofistikerad och samhället har börjat bli medvetet om värdet av dekonstruktion av data i sig.

Ett uppenbart exempel är separeringen av identiteten från identifieringen. I den analoga världen måste en person som gör ett uttalande eller underteckna ett kontrakt befinna sig fysiskt på en viss plats. När telegrafen kom kunde vi kommunicera över avstånd, men vi kunde inte vara säkra på vem som befann sig på andra sidan. Med kryptografi kan vi numera göra det möjligt för en individ att identifiera sig utan att vara närvarande. En prestation som är extremt värdefull och något som blir alltmer vanligt förekommande på Internet.



Blockkedjan har som teknik visat sitt värde inom dekonstruktion av data men också delning av olika delar av den dekonstruerade datan.

Istället för att dela med oss av all data kan vi dela med oss av när data skapades. Det kan exempelvis vara praktiskt att kunna bevisa när i tiden data skapades och det är värdefullt att kunna göra det utan att behöva dela med sig av all data till en central databas.

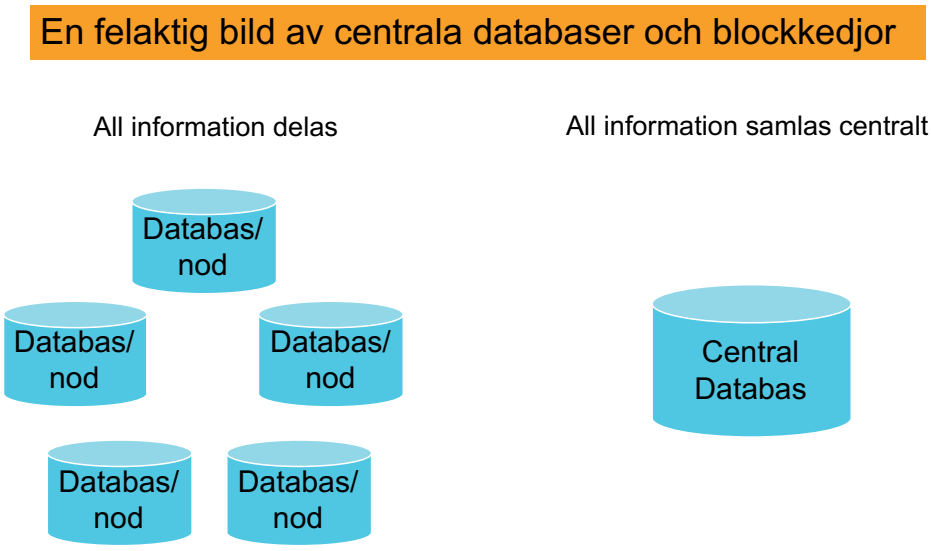
Att skilja identitet från identifiering är bara ett exempel. Vi kan nu dekonstruera data på en rad olika sätt:

• När skapades data? Exempel: En bild av en bilolycka som skickas till ett försäkringsbolag, en patentansökan eller en personalliggare på en restaurang.
• Är data manipulerad? Exempel: Bokföring hos ett företag, eller ett anställningsavtal.
• Vem har validerat uppgifterna? Exempel: Var uppgiften validera av en certifierare, ett betrott datacenter eller är det möjligt att validera av någon utomstående.
• Är uppgifterna kontrollerade av en auktoriserad organisation eller individ? Exempel: Utan att veta vem det är, bara att personen var auktoriserad eller någon som är behörig att lämna in uppgifterna.
• När kommer det att vara möjligt att komma åt uppgifterna? Exempel: För att förhindra att uppgifter om svar på ett test visas eller att pengar spenderas för tidigt.
• Har någon tittat på uppgifterna? Exempel: För att veta om någon har tittat på en patientjournal eller hemlig information i ett företagsvalv.
• Finns det en versionshantering, en unik källa till eventuella ändringar av denna handling/uppgift? Exempel: Den senaste versionen av lagen, en aktuell uppgift om F-skattsedel, utrymme för ROT och RUT avdrag,

• Är uppgifterna unika? Exempel: För att se till att det inte finns några kopior av en finansiell tillgång eller ett paket med läkemedel.

Dela delarna

Med blockkedjan har värdet av att dela med sig av data till andra blivit tydligt, i synnerhet att dela endast några valda delar av den dekonstruerade datan. Om två parter skriver ett kontrakt, tjänar båda dessa på att lagra beviset av sitt kontrakt hos en utomstående. De kan numera göra detta utan att dela med sig av själva kontraktet, bara beviset av detsamma.



Idag tänker sig många att vi antingen kan dela fullständig information eller ingen information alls. Det är en grov och mycket olycklig förenkling. Blockkedjan är inte den enda lösningen för att dela data på ett smart sätt, men den har tydliggjort de tekniska möjligheterna och värdet av att dela utvalda delar av data. Till exempel kan vi med hjälp av teknik dela beviset (ett digitalt fingeravtryck) av kontraktet samt tid, plats för ingående av detta etc., men inte själva kontraktet. Förtroende och datasäkerhet kan på detta sätt uppnås samtidigt.

Metod och val av lösningar

Metoden för arbetet har utgått från sju workshops i projektgruppen samt ett antal mindre möten för fördjupad diskussion och intervjuer m.m.

Under arbetet identifierades ursprungligen 19 tänkbara problem och möjligheter som grupperades i fem områden. Dessa var:
• Identiteter och egenskaper
• Digitala transaktioner och händelsedata
• Redovisning och revision
• Skattskyldighet
• Standarder och jämförbarhet för rapportering

Inom dessa fem områden valdes sedan fem möjliga områden ut som värdefulla och där det även fanns en rimlig sannolikhet att arbeta fram bra lösningar.
1. Digitala kvitton
2. Personalliggare
3. SINK, särskild inkomstskatt
4. Fullmakter
5. Företagsuppgiftstjänst

För tre av de ovanstående bedöms lösningarna redan idag vara tillräckligt färdiga för att kunna bygga tekniska piloter och gå vidare med att mer i detalj utreda de juridiska frågeställningarna m.m. För de övriga två krävs det fortfarande lite mer analys och tankearbete.

Att utveckla parallellt med utredande arbete för att snabba på utvecklingsprocesser har blivit vanligare i näringslivet, i synnerhet inom digital utveckling. Begrepp som ”design thinking”, arbete med prototyper och beta-tester är exempel på detta.

Samhällsnytta

Utgångspunkten har varit att välja lösningar som vi bedömer kan generera stor samhällsnytta. Nyttan bedöms efter tre kriterier; det värde som skapas, kostnaden för att uppnå värdet och tiden för att realisera värdet. Flera av de aktörer som involveras i projektet är tämligen riskaverta. Kostnaden för felsteg hos myndigheter, banker och revisorer kan vara stora. Det är samtidigt angeläget att betona att ett projekt som genererar fem miljarder i samhällsnytta per år är värdefullt att realisera. Ett års försening innebär en förlust, eller utebliven vinst, på fem miljarder för samhället.

Teknik, juridik och process

Projektet fokuserar på lärande och innovation. Detaljkunskap om juridik, processer och teknik har inte varit i fokus. I de mycket övergripande förslag på teknik, anpassning efter lagar och regler samt nuvarande och framtida processer har vi tagit hänsyn till samhällsnyttan. Krävs det en lagändring är vi medvetna om att det tar tid och försenar lösningen. Det som presenteras är en kvalificerad gissning av vad vi bör göra för att uppnå det värde vi vill uppnå inom rimlig tid. I några fall kan det också byggas tekniska lösningar som kan börja tillämpas redan innan ny lagstiftning är på plats.

Den slutliga tolkningen av lagar och regler kan vi inte veta säkert på förhand. Vi kan som information nämna att vi åtminstone har identifierat frågor som offentlighetsprincipen, eIDAS, GDPR (Anonymisering, pseudonymisering, saklig grund, rätten att bli glömd mm.), utgivning av kvitton, original av kvitton, bokföringslagen, överlåtelser av fullmakter för deklarationsombud m.m.

För att förstå lösningarna är det givetvis värdefullt med en viss kunskap om juridik, processer och teknik. När det gäller teknik finns en genomgång av de allra viktigaste begreppen/tekniker som används i slutet av rapporten. Är du som läsare bekant med vad en hash, ett merkleträd och en Certificate Authority (CA) är behöver du antagligen inte läsa denna del.

Beskrivning av lösningarna

Beskrivningarna av lösningarna följer en liknande struktur. Inledningsvis beskrivs dagens situation och vad vi vill förbättra. Därefter beskriver vi översiktligt en process som bedöms lämplig att utgå ifrån. Avslutningsvis finns en beskrivning av tankar och förslag kring governance och juridik, ID samt lagring av data. Vi bedömer dessa tre delar som särskilt angelägna att reda ut eftersom de är svåra, inte minst eftersom många blockkedjeprojekt fallerar på dessa tre områden.

Digital kvittohantering

Vilken nytta och vilket värde kan skapas?

Med en pågående digitalisering har digitala kvitton varit en funktion som många efterfrågat. Kassaregisterlagstiftningen gör det möjligt att kassaregistret producerar ett elektroniskt kvitto. För att ändå hantera digitala underlag har företagen tagit ett foto på papperskvittot och använda den digitala kopian av kvittot i sin bokföring. I dessa fall måste företaget ändå under en period spara det originalkvitto i papper som företaget tog emot. Att registrera och spara papperskvitton kräver stora resurser och försvårar moderna arbetsplatser där många helt eller delvis arbetar på distans eller av andra skäl gör resor och har utlägg från hotell, tåg, taxi, restauranger etc.

Orsaken till att digitala kvitton som är en kopia av ett fysiskt kvitto inte accepteras utan förbehåll är i huvudsak att de kan underlätta bedrägerier och försvåra skattekontroll. Vidare kan digitala kvitton kopieras och ett och samma kvitto kan användas för att göra avdrag och t.ex. få tillbaka moms i flera olika företag. Det är dessutom lättare att förändra ett digitalt kvitto om kvittot tillåts ha vilket format som helst. Det är till exempel lättare att obemärkt lägga till en nolla i en Wordfil än på ett papperskvitto.

Det finns idag lagkrav på såväl digitala som fysiska kvitton. Dessa reglerar bland annat tillverkardeklarerade kassaregister och de funktioner som ett kassaregister ska ha. Kassaregisterlagstiftningen tillåter att det tillverkardeklarerade kassaregistret tar fram ett digitalt kvitto. Den nuva-

rande lagstiftningen kräver emellertid samtidigt att en anställd som vill dra av kostnader för utlägg och ett företag som vill dra av kostnader och moms måste spara kvittot i original i bokföringen, d.v.s. det ursprungliga filformatet när det gäller digitala filer och pappersformat för papperskvitton, vilket försvårat den praktiska hanteringen. Tyvärr har införandet av digitala kvitton av den anledningen dragit ut på tiden i handeln och bland företagen. Det finns emellertid företag som påbörjat utgivning av digitala kvitton.

Diskussionen om digitala kvitton har rört en rad olika områden såsom ”svarta lådor” för kontantkassor, automatkonteringar i bokföringen, realtidsredovisning o.s.v. I slutändan har den lösning som föreslås i denna rapport en möjlighet att underlätta för de flesta av dessa frågeställningar. Utgångspunkten för att detta ska vara möjligt är att kvitton inte bara är digitala utan att de också är formatoberoende, d.v.s. det är den digitala informationen som är central och inte formatet, m.a.o. om det är en PDF eller liknande format.

Lösningen utgörs av en säker kvittohantering och bygger på två viktiga insikter.
1. Ett kvitto i sig har ett mycket begränsat värde. Det är ingen större fara om någon stjäl ett digitalt kvitto. Det är till exempel redan idag ofta möjligt att få en kopia på gamla kvitton från försäljningsstället.
2. Skatteverket och andra intressenter är framförallt intresserade av om ett kvitto redan har kostnadsförts och därmed påverkat redovisningen sedan tidigare i samma eller något annat företag. Även företag vill gärna veta om ett kvitto redan använts för ersättning till en anställd i en reseräkning, eller av ett annat bolag.

Den största nyttan med ett digitalt kvitto ligger sannolikt i att minska

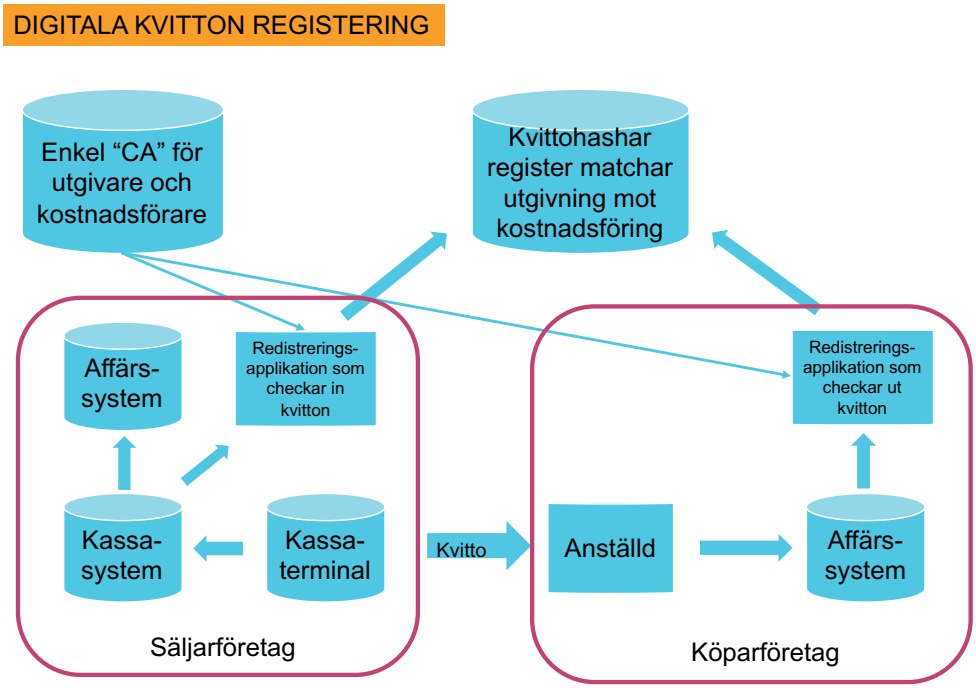
företagens och de anställdas administration och arbete med att redovisa och överföra papperskvittot till digital form samtidigt som papperskvittot ska arkiveras. Eftersom en helt digital lösning även möjliggör automatkonteringar i bokföringen i högre utsträckning kan betydande arbetsinsatser sparas.

En fullt ut digital hantering av kvitton, som dessutom underlättar automatkontering bedöms generera ett värde i Sverige på mer än tio miljarder per år i Sverige. Den beskrivna lösningen kan vara central för att uppnå detta. Används lösningen även för fakturor och motverkar exempelvis momsbedrägerier är potentialen ännu större. Möjligheten att samarbete med andra länder kan också öka och bidra till en minskning av internationella momsbedrägerier. Enbart inom EU uppskattas momsbedrägerier uppgå till mer än 300 miljarder per år.

En mjukvara/tjänst och arkitektur för digital kvittohantering

Följande situationer är lösningen tänkt att hantera:
• Möjliggöra digital lagring av digitala kvitton.
• Minska risken för misstag och bedrägerier med manipulerade kvitton och kvitton som kostnadsförs flera gånger.
• Underlätta för digitala transaktioner och händelsedata och möjliggöra realtidsrapportering och automatkonteringar i bokföringen.
• Processen kan utvidgas till att omfatta även fakturor och därmed minska risker med momsbedrägerier, inte minst med en framtida internationell lösning.

Övergripande arkitektur



Process

I enlighet med vad som står i avgränsningen är åsikterna som beskrivs i rapporten inte något som någon person eller organisation tar ansvar för. Såväl ID-hangering (CA) som Kvittoregister i denna lösning kan ligga hos Skatteverket eller en annan myndighet. I detta specifika fall har Skatteverket varit särskilt angelägna om att betona att det inte är ett ställningstagande från myndigheten att man önskar samla in information.

Steg 1: Transaktion
Säljaren tar emot en betalning och ger ut ett kvitto. Formatet på kvittot kan tillåtas vara valfritt. Målet är givetvis att alla kvitton ska bli helt digitala, men för att systemet ska gå att implementera snabbare behöver befintliga lösningar vara juridiskt giltiga åtminstone under en övergångsperiod.

Steg 2: Registrering av kvittot i kassaregistersystemet hos utgivaren
Det säljande företaget hämtar data om det utgivna kvittots innehåll från kassaterminalen/datorn. Innehållet består av två delar dels ett unikt ID som finns kopplat till varje kvitto och dels uppgifter om transaktionen dvs datum, tid, belopp, moms, artiklar som köpts.

Steg 3: Registrering av kvittohash hos kvittohashregistret
Den inhämtade informationen hos kvittot som beskrivs ovan krypteras till en hash. Till hashen läggs också en publik nyckel eller liknande kod som företaget registrerat hos en part liknande en certificate authority, CA, d.v.s. någon som kopplar ihop koden och företaget. Eftersom kvitton har ett lågt värde kan hanteringen av dessa nycklar hålla en lämplig och kostnadseffektiv lägre nivå och företag som vill registrera kvitton kan använda stora mängder nycklar om de vill. Kvittohashregistret har nu en hash av ett kvitto och en kod som en annan databas (CA för kvitton) kan knyta till ett företag (d.v.s. det företag som registrerat kvittot). Observera att själva originalinformationen inte finns hos kvittohashregistret.

Steg 4: Utläggsregistrering av kvittot
Den anställde som haft ett utlägg, t.ex .en tågresa, registrerar sitt digitala kvitto och ger in det till sin arbetsgivare. Arbetsgivaren, eller den anställde, registrerar informationen i affärssystemet. Eftersom det inte behövs något fysiskt kvitto kan kvittot sparas digitalt. Registrering och kontering kan

också lättare utföras automatiskt av ett system eller någon på en ekonomiavdelning eller redovisningsbyrå. Automatkonteringen underlättas om kvittot ges ut i ett digitalt maskinläsbart format.

Steg 5: Registrering av kvittot som kostnadsfört hos kvittoregistratorn
Den inhämtade informationen hos kvittot som beskrivs ovan krypteras till en hash. Eftersom kvittots innehåll är detsamma som det som registreras av kassaregistrets ägare kommer hashen att vara likadan. Till hashen läggs också en publik nyckel eller kod kopplad till det kostnadsförande företaget på motsvarande sätt.

Steg 6: Kvittoregistratorn matchar utgivarens hash med kostnadsförarens hash
Kvittoregistratorn har nu en hash av ett kvitto och en publik nyckel för det utgivande företaget. Denna hash kan sedan markeras som ”använd” när ett kostnadsförande företag registrerar samma hash. Kvittoregistratorn vet inte något om innehållet men kan validera att samma kvitto blivit utgivet och kostnadsfört.

Governance, juridik m m

Governance
Det centrala i arkitekturen är att det skapas en gemensam liggare för registreringen av de krypterade verifikationerna av kvittona. Om den gemensamma liggaren samlar in fullständig data, d.v.s. själva kvittona i sin helhet, blir databasen sammantaget oerhört stor och en betydande säkerhetsrisk. Idag finns det ett flertal länder, även i Europa, som är på väg i denna riktning, d.v.s. att skapa fullständiga databaser med försäljnings-

och leveransdata. I den föreslagna lösningen är det däremot möjligt att lämna ifrån sig data utan att denna kan återskapas, eftersom den är krypterad som hashar.

För att registreringarna inte ska vara helt oidentifierbara behövs dessutom unika avsändare av hasharna. Det behövs därför ett system som registrerar användarna och kan koppla dessa till respektive företag. De kommer därför att behövas privata och publika nyckar eller företagsspecifika koder för detta (eller något annat digitalt identifieringssystem.) Företagen kan välja att ha många nycklar och det kan dessutom skickas in extra transaktioner för att dölja mängden kvitton som registreras. Skatteverket bör ha tillgång till den gemensamma liggaren eftersom det inte kan finnas okända liggare. Det går att lagra dessa som en blockkedja men det är sannolikt enklast om Skatteverket är ägare av liggaren eller i vart fall har lagstyrd tillgång till liggaren i ett fastställt format.

Integrationen till den publika liggaren görs lämpligen maskin till maskin med ett API som respektive affärssystemsleverantör integrerar.

ID

Det är en fördel om ID-hanteringen hanteras separat eftersom det försvårar analys av databasen och eventuella kopplingar till data. ID-hanteringen kan med andra ord skötas av andra aktörer. Det finns en rad olika sätt att ytterligare dölja information, men man ska vara medveten om att detta är enormt mycket säkrare, med mindre komplett och mindre värdefull, försäljningsdata än vad många andra länder, inklusive Sverige, Norge och EU är på väg att bygga upp på annat håll.

Lagring
Lagring av kvitton, d.v.s. själva originalinformationen, sker i respektive affärssystem eller lagring som är kopplad till dessa, t ex kassaregistersystem. Kravet på att lagra kvitton i originalformat behöver i detta fall tolkas som, eller förändras till, att kvittot är utgivet i form av ett innehåll snarare än ett format. Så länge innehållet registreras i den gemensamma liggaren, kvittoregistratorn, är det att betrakta som ett original. Huruvida detta är förenligt med nuvarande lagstiftning är oklart. För det fall ny lagstiftning krävs kommer det däremot inte att behövas ny lagstiftning för befintlig hantering. Det som krävs är att möjliggöra även detta förfarande för att uppfylla kravet på lagring av original.

GDPR bedöms inte vara något problem för den här lösningen. Det är inte säkert att detta system kräver blockkedjeteknik i form av merkleträd eller konsensusalgoritm. Uppstår ett behov av exempelvis tidsstämpling, d.v.s. upprätta en tidsordning för registreringarna, kommer det fortsatt att vara möjligt att radera gammal data.

Personalliggare

Vilken nytta och vilket värde kan skapas?

Ett lagkrav på personaliggare har införts i en rad branscher i Sverige. Syftet har varit att minska förekomsten av svart arbetskraft.

En personalliggare kan föras manuellt (i bokform). Den ska då vara inbunden, och sidorna ska vara förnumrerade. Det betyder att man inte kan använda lösa papper eller exempelvis ett spiralblock. Skatteverket har tagit fram en manuell personalliggare som man kan använda, men en personalliggare kan också föras elektronisk. Det är samma krav på vad som ska antecknas i den elektroniska personalliggaren som i den manuella. I programmet måste alla händelser loggas, så att det framgår vem som har gjort en ändring och när. Systemet måste även vara utformat på ett sådant sätt att Skatteverket ska kunna granska uppgifterna bakåt i tiden. Inom byggbranschen finns ett mer avancerat system med ID-hantering som branschen tagit fram (ID06). I detta fall har vi begränsat oss till att titta på restaurangbranschen, men tillämpningen är generell för branscher som saknar ID-kontroll.

Värdet på lösningen bedöms främst bestå i minskat svartarbete och enklare hantering för företagen som måste administrera kraven på personalliggare.

En mjukvara/tjänst och arkitektur för personalliggare

Lösningen är tänkt att hantera följande situationer:
• Processen är i första hand tänkt att skapa en rutin för att registrera digitala verifikationer av personalliggarna, oavsett format.
• Detta innebär är att det i princip blir omöjligt att fuska med personalliggarnas innehåll samtidigt som alla uppgifter i personalliggarna förblir anonyma, d.v.s. omöjliga att dekryptera.
• Ytterligare en fördel är att det kan bli lättare att kontrollera historiken i personalliggarna vid skattekontroll.
• En notifiering om en utebliven registrering kan också skickas till företag redan samma dag om det är önskvärt, vilket minskar risken att glömma registreringen.
Värdet av lösningen bygger på antagandet att eventuellt fusk med svart arbetskraft kan minskas och att det blir lättare att skilja på situationer med felaktig rapportering som bygger på rena misstag till skillnad från medvetet fusk.

Process

Steg 1: Upprättande av personalliggare
Varje dag fylls personalliggaren i på samma sätt som idag. Givetvis är det en fördel om personalliggaren är digital men det går bra att ha en vanlig anteckningsbok, d.v.s. valfritt format kan fortfarande accepteras enligt de befintliga lagkraven.

Steg 2: Registrering av en verifikation
Från restaurangens affärssystem, tidrapporteringssytem, eller liknande där personalliggaren hämtas publiceras vilka som arbetar och när. Det går

också att lösa detta i de fall personalliggaren är analog. I det fallet används en app i en telefon. Med den tas ett foto av personalliggaren varje dag. En verifikation, d.v.s. en hash, av filen/fotot registreras tillsammans med en kod som kan identifiera den som registrerar verifikationen. Registreringen görs i en förutbestämd blockkedja, eller ett merkleträd.

Steg 3: Notifiering
Sker ingen registrering kommer en notifiering till företaget, t.ex. restaurangen, att personalliggaren behöver registreras.

Steg 4: Skattekontroll
Om Skatteverket ska göra en skattekontroll kan mobilen eller mjukvaran som registrerat verifikationerna enkelt kontrolleras. Den personalliggare som har en verifikation i blockkedjan är den som jämförs med den personal som arbetar på restaurangen. Det är omöjligt att manipulera personalliggaren eftersom den då inte stämmer överens med verifikationen. Det är också lätt att kontrollera till exempel den senaste månadens registreringar, d.v.s. det är lättare att bedöma om det är ett olycksfall i arbetet att en registrering missats eller om det är systematiskt. Eventuellt kan skattekontrollerna styras till de företag/restauranger som inte gjort registreringar, det förutsätter dock att blockkedjan med personalliggarverifikationerna (hasharna) är tillgänglig i någon form.

Governance, juridik m m

Governance
Det centrala i denna lösning är att beskattningen av personalen säkras i de digitala informationskedjorna hos de skattskyldiga själva, men samtidigt att risken att uppgifter manipuleras minskar ytterligare.

Ett krav är att de som håller registren har rutiner för att säkerställa vilka restauranger de håller verifikationer åt. Det vill säga det räcker med att det inte finns risk för flera olika register för samma restaurang. Ägandet av lösningarna kan därför vara helt privat. Restaurangerna behöver heller inte dela med sig av personalliggarna till registerhållarna, enbart krypterade verifikat.

ID
Det är möjligt för restauranger att göra flera registreringar av verifikationer samma dag. Till exempel om någon blir sjuk och en ersättare sätts in. Minst en registrering per arbetsdag behöver dock ske. För att säkerställa att endast en registrering per företag sker behövs ett ID som är kopplat till det specifika företaget. Detta ID kan överenskommas med företaget som samlar registreringarna, t.ex. kan en publik nyckel skickas från applikationen medan den privata nyckeln behålls. Stjäl någon nyckeln är det enkelt att göra en ny.

Lagring
Lagring av originalfilerna måste ske digitalt, men behöver endast ligga lokalt. Personalliggaren kan göras på papper men fotot som tas av liggaren behöver vara digitalt. Detta foto är också det som behöver sparas. I detta fall kan en översyn av bevaranderegelrna av personalliggaren behöva göras.

SINK/Realtid

Det har diskuterats i olika sammanhang att bokföring, intern- och externredovisning, skatteinbetalningar med mera över tid kommer att ske närmare transaktionstillfället. Idealt kan vara att detta sker i realtid.

Fördelarna med detta är flera:
1. det underlättar för företagen som får bättre beslutsunderlag och högre grad av kontroll,
2. det gör redovisning och revision mer relevant,
3. det undanröjer behovet av preliminära skattebetalningar
4. det säkerställer skatteinbetalningar redan när skattskyldighet uppstår.

Relativt komplicerade rättsliga regler kan hanteras snabbt i digitala automatiserade kedjor.

Avståndet från skatteredovisning i realtid i relation till dagens situation är samtidigt stort. Idag redovisas skatt generellt sett varje månad, var tredje månad eller till och med på årsbasis.

Digitalisering är i sig en bra grund för att kunna redovisa i realtid. Utökade möjligheter till automation och kommunikation maskin medmaskin, liksom utökade möjligheter till intelligenta system för automatisk riskhantering tar bort de manuella arbetsuppgifter som tidigare behövde genomföras för att ex vis sammanställa och hantera olika typer av skatteredovisning, betalningar etc.

Situationen idag

• Det är varierande kvalitet på rutinerna hos företagen idag. Arbetet går långsamt, omfattar ofta manuell hantering vilket innebär både osäkerhet och risker. Arbetet kan därför ge en skev bild av bolagets ställning och informationen släpar ofta efter verkligheten.
• Det finns olika sanningar vid olika tidpunkter. Både årsredovisningen och annan rapportering har idag en uppenbar svaghet i att den upprättas långt efter bokslutsårets slut. I en värld där realtid efterfrågas allt mer förlorar årsredovisningen sin relevans. När tidsperioden mellan årets slut och årsredovisningens publicering är lång blir det oklart vad som revideras. Hur såg bolaget ut vid det tillfället som avses och är den bilden fortfarande relevant?
• Idag sker redovisning i efterhand, viket försämrar kontroll och styrning av verksamheter. Många andra tjänster blir lidande när redovisningen som publiceras ligger långt efter de verkliga händelserna i tid. Kreditbedömningar, bedömningar av bolagets solvens o.s.v. blir sämre.

Alternativa tillvägagångssätt

För att åstadkomma realtidsredovisning och realtidbeskattning kan vi arbeta med olika angreppssätt:
• Underlätta digitalisering av kontanthantering, fakturering, inrapportering till myndigheter, riskhantering, redovisning och revision. Genom att driva på digitalisering skapas bättre möjligheter för att realtidsrapportering ska bli verklighet.
• Införa ett slutlig fastställande av skatt närmare transaktionstillfället på flera beskattningsområden. Skatten går redan på flera områden att fastställa direkt vid transaktionstillfället för exempelvis moms, punktskatter,

arbetsgivaravgifter (i samband med löneutbetalningar) och SINK.
• ”Split payments” innebär att betalning av skatt sker direkt till Skatteverket samtidigt som betalning sker till den som ska betalas, t.ex. en leverantör eller en anställd.
• De företag som har bra kontroll på sin verksamhet utvecklas bättre och har lägre risk. De som kan påvisa bättre processer bör kunna få fördelar i sin verksamhet och lättare att få lån, försäkringar, bättre betalningsvillkor o.s.v. Realtidsredovisning kan därför komma att drivas naturligt, både av företag, deras kunder och leverantörer.
• Ambitionen är att med automation, digitaliserade informationskedjor och realtidsredovisning och betalning (exempelvis genom s.k. split payments) så kan relativt komplicerade rättsliga regler och komplicerade verksamhetsregler och riskhanteringsmodeller, för beskattning hanteras snabbt och säkert i digitala kedjor. Det förutsätter att data och processer inte fritt går att manipulera. Detta kan möjliggöra den situation man tidigare velat uppnå genom regelförenklingsarbete, utan att öppna upp för de risker och ekonomiska snedvridningar som förenklingar av de rättsliga reglerna kan öppna upp för. Det kan bli enklare och mer förutsebart att hantera företagens beskattningssituation.
• För staten minskar risker runt skatteinbetalningar som ska ske senare än transaktionstillfället.

Realtid – ett första steg med SINK (Särskild inkomstskatt)

Ett första steg till att uppnå rapportering i realtid är att fokusera på beskattningssituationer där skatten slutligen fastställs redan i transaktionsögonblicket.

Det är också intressant att hitta ett användarfall som inte blir alltför omfattande i ett första steg, men som samtidigt erbjuder reell effekthemtagning både för enskilda och myndigheter.

SINK, Särskild inkomstskatt för utomlands bosatta, är ett lämpligt område av flera skäl. Särskild inkomstskatt betalas av personer som normalt är skattskyldiga i ett annat land men som exempelvis arbetar tillfälligt i Sverige under tillräcklig tid för att skattskyldighet i Sverige uppstår. SINK betalas också på exempelvis svenska pensioner för de pensionärer som bor utomlands.

Det är med andra ord en skatt som inte gäller så stor del av befolkningen. Ett annat skäl är att skatten är slutlig vid transaktionstillfället, även om det är en skatt på inkomst. SINK betalas med en rak procentsats på 25 % på bruttolönen, utan grundavdrag eller progressivitet. Vanlig beskattning av arbete (inkomst av tjänst) beskattas i efterhand, personen får deklarera och så matchas de skatteavdrag som arbetsgivaren har gjort mot den slutliga skatten och skatt att betala eller att återfå kan uppstå. Det finns grundavdrag, andra möjliga avdrag, värnskatt på högre inkomster etc. SINK är dock klar i utbetalningsögonblicket, det som återstår efter att lönen betalats ut minus avdraget för SINK är redovisning och inbetalning av skatten till Skatteverket, från arbetsgivaren.

Trots att det är en skatt på arbete finns med andra ord inga avdrag, ingen jämkning eller justering av skatten efter årets slut. Inkomsten i Sverige är däremot ofta ett beskattningsunderlag för Skattemyndigheten i arbetstagarens hemland, där det är en inkomst som oftast ska tas med i deras ordinarie inkomstbeskattning av arbetstagaren. Den skatt som betalas i hemlandet kan, beroende på lokal lagstiftning, justeras med hänsyn till den SINK som är betald i Sverige (man får räkna av den betalda svenska

skatten på den beräknade utländska skatten, eller så undantas eventuellt just den inkomstenen från att ligga till grund för skatt).

Ett antal frågor har hanterats genom gemensamma diskussioner inom gruppen:

• Kan affärssystemen (lönesystem) hantera betalningsuppdrag/redovisning?
  – Ja – det finns redan system framtagna för SINK som hanterar regler om tid etc.
  – SKV kan bidraga med att distribuera exempelregler via API.
• Kan redovisningsinformation motsvarande arbetsgivardeklaration på personnivå följa med en betalning?
  – Ja – det finns just nu en begränsad mängd tecken som kan hängas på en betalning (ex: SWISH).
  – Det internationella systemet för betalningar har emellertid förbättrats och snart kommer det vara möjligt att lägga med en XML-fil i betalningens ”payload” – hela redovisningen kan lämnas med betalningen.
• Kan redovisningsinformationen tillgängliggöras digitalt/automatiserat/säkert
  – Ja – genom exempelvis lösningar med liggare för det internationella informationsutbytet mellan skattemyndigheter.

Vilket värde kan skapas?

• När skattskyldighet uppstår är det bra om skatten betalas så snart den kan slutligen fastställas. Eftersom skatt är en prioriterad fordran och styrelsemedlemmar är solidariskt ansvariga för dessa är det en fördel för många parter om stora skatteskulder inte byggs upp i företag.
• I första hand ser vi SINK som ett första steg mot att redovisa och betala

skatt närmare transaktionstillfället. På sikt kan den hanteringen bidra till:

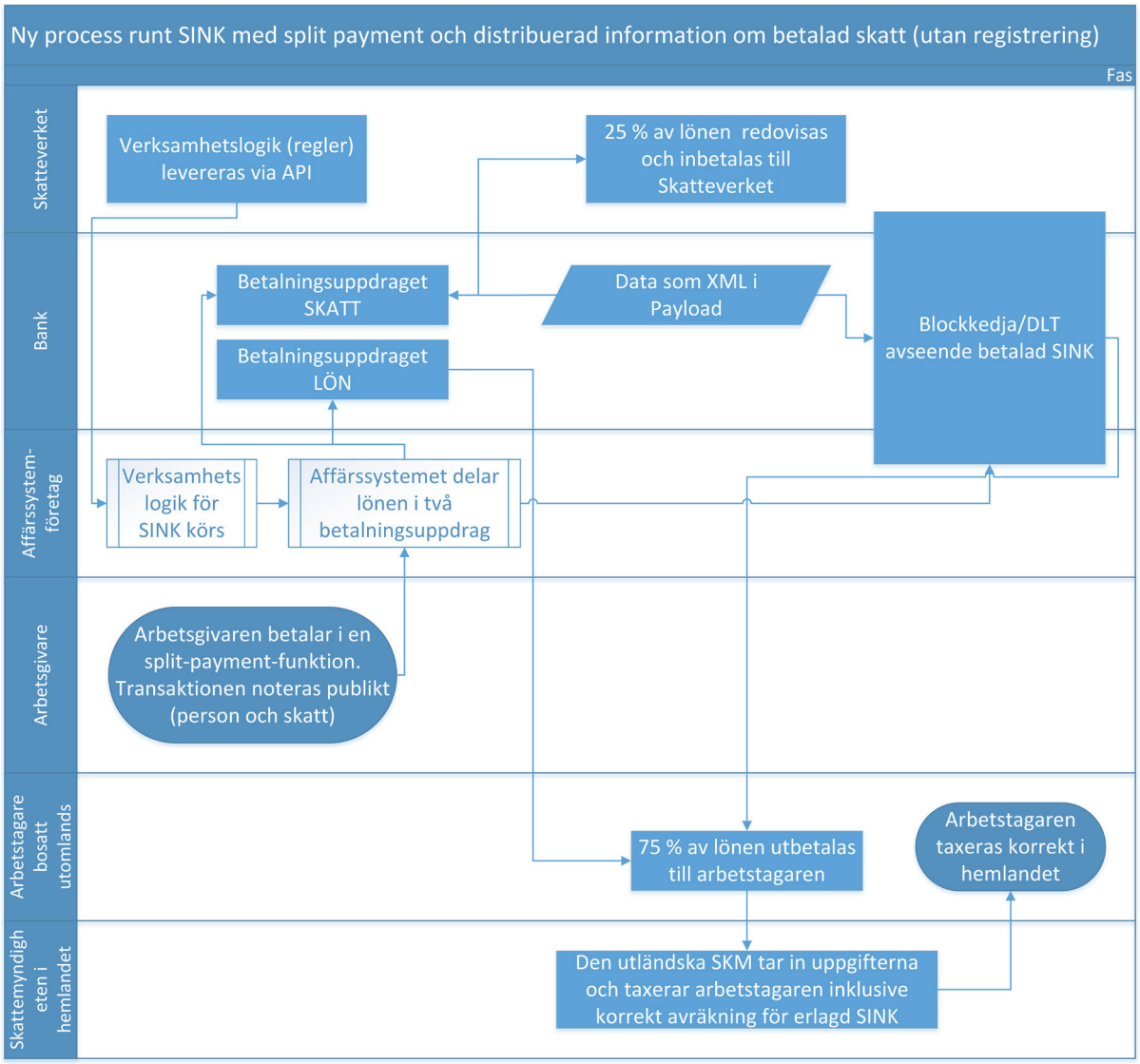
– Enklare access till uppdaterad data om bolagens och organisationernas ställning kan förbättra beslutsunderlag och befintliga tjänster, samt möjliggöra nya. Detta kommer i sin tur att underlätta working capital managment, likviditetshantering, belåning och försäkringar osv.

– Delning av data med olika intressenter underlättas när den är uppdaterad och säker.

– En redovisning som kan hämtas ur systemet vid behov eller åtminstone hamnar närmare i tiden vid delårsbokslut och årsredovisning är nödvändig för att dessa ska bibehålla sin relevans.

– På sikt kan det finnas mer relevanta sätt att redovisa till exempel efter behov, istället för efter tidsintervall, som styrs av förutbestämda regler.

Process


Ny process runt SINK med split payment och distribuerad information om betalad skatt (utan registrering)
Fas
Skatteverket
Bank
Affärssystem-företag
Arbetsgivare
Arbetstagare bosatt utomlands
Skattemyndigheten i hemlandet
Verksamhetslogik (regler) levereras via API
25 % av lönen redovisas och inbetalas till Skatteverket
Betalningsuppdraget SKATT
Data som XML i Payload
Blockkedja/DLT avseende betalad SINK
Betalningsuppdraget LÖN
Verksamhets logik för SINK körs
Affärssystemet delar lönen i två betalningsuppdrag
Arbetsgivaren betalar i en split-payment-funktion. Transaktionen noteras publikt (person och skatt)
75 % av lönen utbetalas till arbetstagaren
Arbetstagaren taxeras korrekt i hemlandet
Den utländska SKM tar in uppgifterna och taxerar arbetstagaren inklusive korrekt avräkning för erlagd SINK

Steg 1
Lönesystem eller annat affärssystem tar in gällande regler för hantering av SINK från Skatteverkets API.

Steg 2
Arbetsgivaren betalar ut lön i en split-paymentfunktion. Affärssystemet går igenom egna och Skatteverkets regelverk, konstaterar att lönen ska beskattas enligt SINK-lagstiftningen och delar upp lönen i två betalningsuppdrag. Information om beskattningssiutationen läggs till betalningen i form av en XML-fil.[2]

Steg 3
Betalningsuppdraget för lön går iväg till banken och effektueras. Betalningsuppdraget för SINK-skatt går iväg till banken tillsammans med tillhörande information. Banken verkställer betalningsuppdraget till Skatteverket och vidarebefordrar tillhörande information. Informationen tillförs en säker liggare (blockkedja/DLT) av Skatteverket. Skatten är nu fastställd och betald.

Steg 4
Liggaren tillgängliggörs för utländska skattemyndigheter och den skattskyldige personen. Den utländska myndigheten tillför informationen till arbetstagarens inkomstbeskattning. Arbetstagaren kan kontrollera att informationen är korrekt redan i liggaren.

Governance

Skatteverket och rådgivare har en möjlig nyckelroll i att ta fram accepterade lösningar för uppdaterade tolkningar av regelverk maskin motmaskin,

[1] Informationen som bifogas betalningen ersätter registreringsinformationen för SINK-beslut och arbetsgivardeklaration på individnivå. Informationen uppfyller därmed hela personen och arbetsgivarens redovisningsskyldighet gentemot Skatteverket. Inget ytterligare krävs.

exempelvis via API:er. Det kan därför uppstå frågetecken kring tolkningar av skattebelopp, skattskyldighet med mera.

ID-hantering

ID-hanteringen idag består bland annat av att ett samordningsnummer (motsvarande ett svenskt personnummer fast för utomlands bosatta som inte ska folkbokföras) skapas för arbetstagaren. Processen för att skapa samordningsnummer ligger hos Skatteverket. Processen tar emellertid idag för lång tid eftersom den är manuell. Det behöver därför skapas förutsättningar för automatisering av den här processen inom Skatteverket.

Ett system för att skapa en kod som kan avkryptera ett SINK-beslut skickas till individen. Denne behöver dock inte knytas till koden utan koden är en dekrypteringsnyckel. Dekrypteringsnyckeln kan ges till skattemyndigheten i hemlandet för att den anställde ska få korrekta uppgifter om den svenska inkomsten och skatten i förtrycket till sin inkomstdeklaration.

Lagring och tillgängliggörande genom automatiskt internationellt informationsutbyte i realtid

En möjlig önskvärd ambition är att Skatteverkets interaktion med utländska skatteverk kan inriktas på att respektive myndighet hämtar uppgifter vid behov. I dagsläget är det den skattemyndighet som har information som skickar stora mängder data till andra skattemyndigheter baserat på datainnehavarens bedömning av vad som kan vara intressant, och för vilka utländska myndigheter. Utbytet sker med stöd av internationella avtal

mellan staterna och EU-direktiv. Denna utveckling förutsätter internationell samverkan.

Om man sätter upp en blockkedja/DLT som:
1. Den skattskyldige själv kan hämta sin information ifrån, och
2. Den utländska skattemyndigheten samtidigt kan hämta information från om sina skattskyldiga, så vänder vi på informationsutbytet så att aktörerna hämtar det de behöver, istället för att Skatteverket skickar den information som de tror att parterna behöver. Informationsutbytet mellan skattemyndigheter kan då ske i eller nära realtid (tillgängliggörande).

Dela information mellan myndigheter

Uppgifter om arbetstillstånd för personer som kommer från ett icke EU-land finns idag hos Migrationsverket. Skatteverket behöver kontrollera dessa uppgifter för att kunna godkänna en arbetstagare för SINK. Ett system för att underlätta för svenska myndigheter att hämta information från andra svenska myndigheter skulle därför vara värdefullt för denna lösning.

Fullmakter

Vilken nytta och vilket värde kan skapas?

Vi bedömer att fullmakter kan hanteras på tre olika sätt:
1. En central tjänst för fullmakter som upprättas eller ackrediteras av en eller flera myndigheter. En utredning av detta gjordes av flera myndigheter under ledning av Pensionsmyndigheten 2012. Det bedömdes värdefullt men komplicerat att upprätta en nationell tjänst.
2. En eller flera mjukvaror eller applikationer som kan användas av olika organisationer efter eget önskemål. En myndighet, intresseorganisation kan ackreditera dessa men det är inte nödvändigt.
3. En tjänst för olika individer att samla information om fullmakter kopplade till sig på samma sätt som ”Mina meddelanden”, kan det upprättas en speciell funktion såsom ”Mina fullmakter”. Tjänsten ”Mina fullmakter” skulle kunna utvidgas till en mer generell tjänst ”Mina dokument” för värdefulla handlingar. För en sådan tjänst är det en fördel om myndigheter upprättar eller åtminstone godkänner eller ackrediterar tjänsten.

Den största nyttan finns sannolikt i att effektivisera och säkra upp arbetet med fullmakter hos banker, företag/organisationer och företagens redovisningskonsulter och revisorer. De som har störst nytta kommer också snabbast att utnyttja en ny lösning, i synnerhet som de är professionella användare och därför kan tvingas att införa processerna av sina arbetsgivare. Arbetet med att ta fram en lösning kan också inledas av en mindre grupp företag, banker, revisorer m.fl. och tjänsten kanske även kan implementeras utan myndighetsbeslut. Utgångspunkten har därför varit att

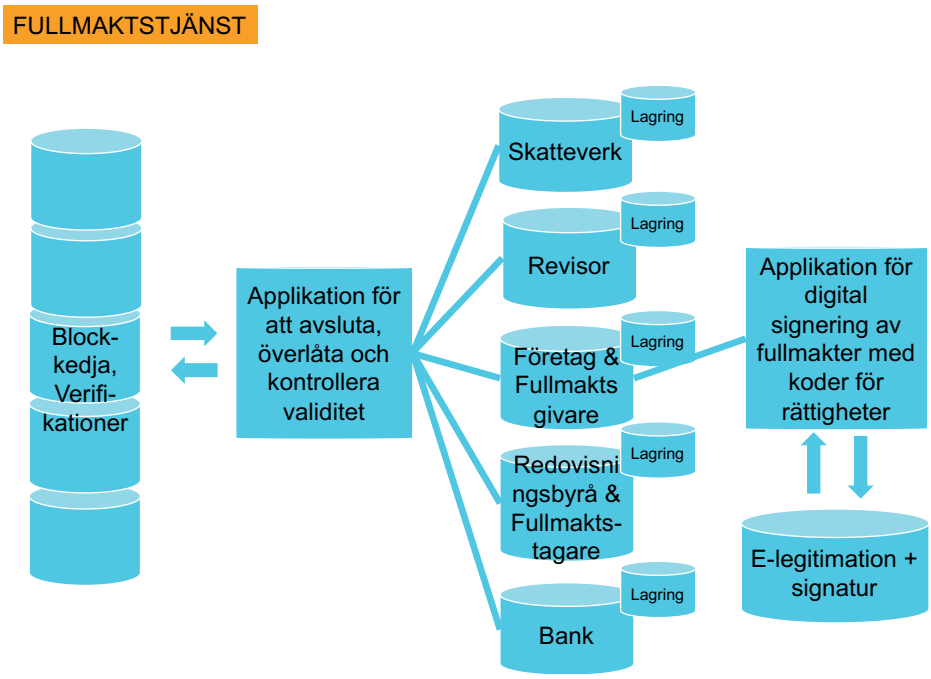
börja med behoven hos behoven hos banker och redovisningskonsulter. I slutändan visar det sig att lösningen för fullmakter gärna kan börja etableras med den utgångspunkten men att det är relativt enkelt att beakta även myndighetsfullmakter, till exempel deklarationsombud, och fullmakter för medborgare i allmänhet.

Värdet på lösningen bedöms betydande, i synnerhet eftersom lösningen kan utgöra en grund för flera olika typer av fullmakter och behörigheter.

En mjukvara/tjänst och arkitektur för fullmaktshantering

Följande situationer är lösningen tänkt att hantera
1. Revisorn begär ut en fullständig lista på fullmakter för att kontrollera att inköp, avtal m.m. har tecknats av behöriga personer. Detta är revisorn skyldig att göra vid revision.
2. En person vill bevisa att vederbörande har en fullmakt och att fullmakten är giltig men även att personer får företräda/agera ombud i en given situation.
3. Redovisningskonsulten, företaget, eller banken, vill få en översikt över vilka giltiga fullmakter som finns, vem som är fullmaktstagare och vem som är fullmaktsgivare.
4. En fullmakt ska avslutas, till exempel för att en person avslutar sitt arbete som redovisningskonsult för ett företag, eller för att en fullmakt ska dras in.
5. En redovisningskonsult ska gå på semester och behöver överlåta sina behörigheter att företräda företaget på någon annan.

Övergripande arkitektur



Process

Upprättandet av fullmakterna sker på vanligt sätt i den digitala världen, d.v.s. en digital fil med innehållet i fullmakten signeras med ett digitalt ID och en digital signatur knyts till fullmakten. Fullmakten är nu giltig. Tanken är här att giltigheten samtidigt styrs av ett externt register i blockkedjan. Fullmakten är giltig om och endas om nödvändig status på fullmakten är registrerad i blockkedjan. Detta formuleras i fullmakten, d.v.s. vilka publika nycklar som har rätt att avsluta fullmakten, samt till vilka publika nycklar fullmakten kan överlåtas (om någon).

Steg 1
Fullmakten upprättas digitalt, vilket inkluderar giltighetstid, vem som är fullmaktstagare, vem som är fullmaktsgivare, omfattningen på fullmakten d.v.s. vad den kan användas till. Såväl fullmaktsgivaren som fullmaktstagaren fyller också i varsin publik nyckel som ger behörighet att avsluta fullmakten. Eventuellt registreras flera publika nycklar, eftersom det kan finnas intresse av att ge fler personer och organisationer rätt att avsluta och eller överlåta fullmakterna.

Steg 2
Fullmakten signeras digitalt med en godkänd eID t.ex. mobilt bankID eller Freja eID och en godkänd underskrift t.ex. från CGI knyts till fullmakten.

Steg 3
Fullmakten registreras i blockkedjan för fullmakter men endast som en hash, d.v.s. ett digitalt fingeravtryck för fullmakten. Bredvid hashen finns de publika nycklar som har rätt att avsluta fullmakten, vilka åtminstone bör finnas hos fullmaktsgivaren och fullmaktstagaren. Processen är nu klar och fullmakten kan användas.

Användarfall:
1. Revisorn begär ut en fullständig lista på fullmakter för att kontrollera att inköp, avtal mm har tecknats av behöriga personer. Detta är revisorn skyldig att göra vid revision.

Lösning:
Revisorn begär ut en lista på alla fullmakter som företaget har och deras digitala fingeravtryck, hashar. Hasharna för fullmakterna kontrolleras mot blockkedjan via ett enkelt API som bara behöver kontrollera att full-

makterna inte avslutats. Har de avslutats i blockkedjan behöver revisorn kontrollera när det gjordes och att fullmakterna endast användes när de var giltiga.

2. En person vill bevisa att vederbörande har en fullmakt och att fullmakten är giltig men även att personer får företräda/agera ombud i en given situation.

Lösning:
Ombudet visar upp fullmakten – t.ex. för banken. Banken gör en slagning i blockkedjan via ett enkelt API och kan bekräfta att den finns och att den fortfarande är giltig.

3. Redovisningskonsulten, företaget, eller banken, vill få en översikt över vilka giltiga fullmakter som finns, vem som är fullmaktstagare och vem som är fullmaktsgivare.

Lösning:
En förutsättning är att de anställda har förberett förfrågningar kring fullmakter och deras giltighet genom att skicka in de publika nycklar som respektive redovisningskonsult, bankanställd, företagsanställd m.fl. har registrerat i fullmakter. Respektive organisation kan välja om även de privata nycklarna ska sparas centralt. På organisationsnivå kan man då kontrollera samtliga giltiga och avslutade fullmakter som är registrerade.

4. En fullmakt ska avslutas, till exempel för att en person avslutar sitt arbete som redovisningskonsult för ett företag, eller för att en fullmakt ska dras in.

Lösning:
Den som vill avsluta fullmakten går in i ett gränssnitt som är uppkopplat till blockkedjan och registrerar den privata nyckel som tillhör den publika nyckel som finns knuten till fullmakten i blockkedjan. Den som har den privata nyckeln har rätt att avsluta fullmakten och den är därför registrerad som avslutad och kan därefter inte användas. Observera att denna rätt att avsluta fullmakten kan finnas hos flera personer och organisationer. Det kan exempelvis vara möjligt att avsluta en fullmakt för såväl en redovisningskonsult som dennes arbetsgivare.

5. En redovisningskonsult ska gå på semester och behöver överlåta sina behörigheter att företräda företaget på någon annan kollega.

Lösning:
Det finns lite olika sätt att lösa detta. Vanligtvis vill en redovisningskonsult kunna överlåta en fullmakt under t.ex. sin semester för att därefter kunna bli fullmaktstagare igen efter semestern. Det krävs en lite annan logik i denna situation eftersom den privata nyckeln inte kan publiceras och sedan användas igen. Redan i fullmaktens upprättande är det troligen nödvändigt ur juridisk synvinkel att tilldela rollen som möjlig framtida fullmaktstagare. Med andra ord, det bestäms vilken person som kan bli fullmaktstagare under semestern redan vid upprättandet. En publik nyckel även till denna person knyts då till hashen av fullmakten i blockkedjan. Dessa personer kan i sin tur sedan överlåta fullmakten mellan sig. Det går att lösa med kryptering även utan att avslöja den privata nyckeln. En väldigt viktig egenskap är att detta möjliggör att säkerställa vilken person som har fullmakten att företräda bolaget vid varje tillfälle och att det endast är en person i taget. Givet att fullmakten redan vid upprättandet

har flera fullmaktstagare är det inte att betrakta som en traditionell överlåtelse av en fullmakt. Eventuellt kan därför fullmakter för deklarationsombud aktiveras för en annan person trots att en överlåtelse enligt lag i dagsläget inte är tillåten. Det beror på att det inte är en överlåtelse utan snarast en aktivering av en inaktiv fullmakt. Givetvis får detta inte ske om det betraktas som ett kringgående av lagstiftningen. Bedömningen är att lagstiftaren har haft för avsikt att begränsa överlåtelser av fullmakter till personer som fullmaktsgivaren inte accepterat eller godkänt. I detta fall har fullmaktsgivaren godkänt fullmaktstagaren på förhand och även fastställt villkoren för detta.

Governance, juridik m m

Governance
Det centrala i arkitekturen är att själva fullmakterna skiljs från blockkedjan. I blockkedjan finns ett merkleträd som sparar giltighetsinformation om fullmakterna. Eftersom informationen i blockkedjan inte går att identifiera, varken vem som äger de privata nycklarna eller innehållet i fullmakterna är governancefrågan flexibel.

Det är tänkbart att företag, banker, redovisningskonsulter, ERP-systemleverantör m.fl. kan tänkas tillhandahålla denna arkitektur som en tjänst. Det viktiga i arkitekturen är att säkerställa att data inte kan manipuleras. Det finns fortsatt fördelar med att hantera databasen som en blockkedja eftersom det är blockkedjan som skapar redundans och minskar risken att någon enskild skaffar sig ett monopol med databasen som grund.

ID

En väldigt viktig del i lösningen är att skilja på upprättandet och avslutandet av fullmakter. Upprättandet av en fullmakt kräver mycket hög säkerhet. Vi vill inte att det skapas fullmakter av obehöriga. För detta syfte behövs säker identifiering och signaturer. För de privata nycklar som används är säkerheten inte lika avgörande. Den enda användningen av de privata nycklarna är att avsluta fullmakten. Det behövs därför inte någon CA Certificate Authority för hanteringen av de publika och privata nycklarna i blockkedjan. Hanteringen av fullmakternas giltighet, d.v.s. aktivering, avaktivering och avslut kan däremot hanteras med privata nyckar som genereras lokalt. Denna hantering kan banker och redovisningskonsulter se som affärskritisk och hantera med hög säkerhet, men för enskilda fullmaktsgivare är det ingen fara om en publik nyckel som är kopplad till en fullmakt kommer i orätta händer. Fullmakten kan avslutas, men den kan inte användas på annat sätt än den var tänkt.

Lagring

Lagring av fullmakterna, d.v.s. själva originalinformationen, kan göras väldigt flexibel. Det går att lagra dessa i en molntjänst, på en vanlig dator eller i en struktur för fullmakter hos professionella aktörer med många fullmakter.

Lagringen av själva databasen med verifikationer bör vara ett merkleträd och gärna en blockkedja.

Företagsuppgifter

Hanteringen av företagsuppgifter är intressant ur flera perspektiv.
• Företagen är intresserade av att rapportera på ett enkelt och standardiserat sätt – och helst bara en gång. The once-only principle är en målsättning för myndigheter för att underlätta för företagen. Den principen har också blivit lag eller praxis i flera länder som Estland och Norge.
• Det kan även vara intressant för företag att kunna dela med sig av information på ett effektivt sätt till andra aktörer än myndigheter, t.ex. för att enklare få krediter, kunna göra inköp med bra betalningsvillkor o.s.v.
• För många olika aktörer är det också intressant att ta del av information om företag på ett enkelt och standardiserat sätt för att känna sig trygg med sin motpart, säkerställa efterlevnad av lagkrav, jämföra data mm.
• Även data som är omarbetad och säljs, kan med fördel bygga på en infrastruktur som är kvalitetskontrollerad och transparent. Området växer med krav från lagstiftare t.ex. för Environmental, Social and Governance reporting (ESG) olika hållbarhetsaspekter, andra typer av certifieringar etc. Jämför även med ”Integrated reporting” som är ett begrepp inom redovisning och revision där mjuka faktorer, t ex hållbarhetsredovisning, ökar i betydelse.

I alla ovanstående situationer är det givetvis också angeläget att hanteringen kan ske med hög kvalité på data, hög IT-säkerhet och med en lämplig grad av anonymitet för såväl uppgiftslämnaren som uppgiftssökaren.

De olika tillämpningar som hittills diskuterats i projektet är:
1. Standardiserad inrapportering av företagsdata till myndigheter
Standardisering av inrapportering är en fråga som Bolagsverket arbetar med aktivt, bland annat genom samarbetet Nordic Smart Government.

Vad beträffar standarder för bolagsuppgifter är blockkedjeteknik och annan krypteringsteknik som sådan inte något som skapar en större fördel vad vi känner till, och det är därför rimligt att låta slutsatserna från samarbetet inom Nordic Smart Government bli tydligare med vad de vill åstadkomma och hur, innan försök på det området föreslås från denna projektgrupp.

2. En samordningstjänst för tillgänglig basdata om företag
En samordningstjänst för grundläggande information om företag där det redan finns rapporteringsskyldighet till myndigheter och information som företagen gärna vill dela bedöms vara både värdefull och en bra start.

3. Holistisk identifiering av organisationer med olika former av data
Insamlingen av bred information om företag kan ses som en övergripande lösning för att samla och dela olika former av uppgifter där det finns lagkrav och där det av andra skäl kan vara värdefullt. Anslaget i detta förslag är relativt omfattande, där föregående punkt kan vara ett första steg. En möjlig utgångspunkt är att lägga fokus på att etablera strukturen och basinformation, d.v.s. punkt 2.

4. En tjänst för att jämföra företag i samma bransch
Denna typ av tjänst kan baseras på offentliga data och bör kunna skapas men är sannolikt beroende av att andra delar finns på plats så att data från t.ex. Bolagsverket, SCB och Skatteverket kan samordnas, och i vissa fall även kanske avidentifieras. Vi bedömer att det är bättre att börja med punkt 2 och därigenom skapa förutsättningar för detta vid ett senare tillfälle.

5. En tjänst för att konsolidera data från olika företag, exempelvis inför uppköp eller sammanslagning av företag. Detta leder till i stort sett samma resonemang som under punkt 4.

Vilket värde kan skapas?

Redan idag finns det företag som arbetar med att tillhandahålla tjänster av denna karaktär. Det är därför viktigt att fundera över vad en liknande tjänst skulle tillföra.

1. Ett skäl kan vara att ansvaret för att information är korrekt och uppdaterad ofta är ett myndighetsansvar och att ansvaret kan bli mer otydligt med en mellanhand.

2. Ett annat skäl är att myndigheter har ett ökat krav på sig att tillgängliggöra data. Begrepp som ”open data”, ”open source” och ”open science” betonas allt mer i rapporter och regelverk såväl i Sverige som inom EU. Det är därför lämpligt att information som redan finns hos myndigheter i framtiden tillgängliggörs på ett mer öppet och tillgängligt sätt.

3. En tillgänglig infrastruktur för olika typer av data möjliggör nya tjänster. Banker åläggs nu att upprätta APIer, enligt PSD2, för att underlätta för tredjepartstjänster att använda bankernas data. Det är rimligt att offentlig data tillgängliggörs för att underlätta tredjepartstjänster åtminstone på motsvarande sätt.

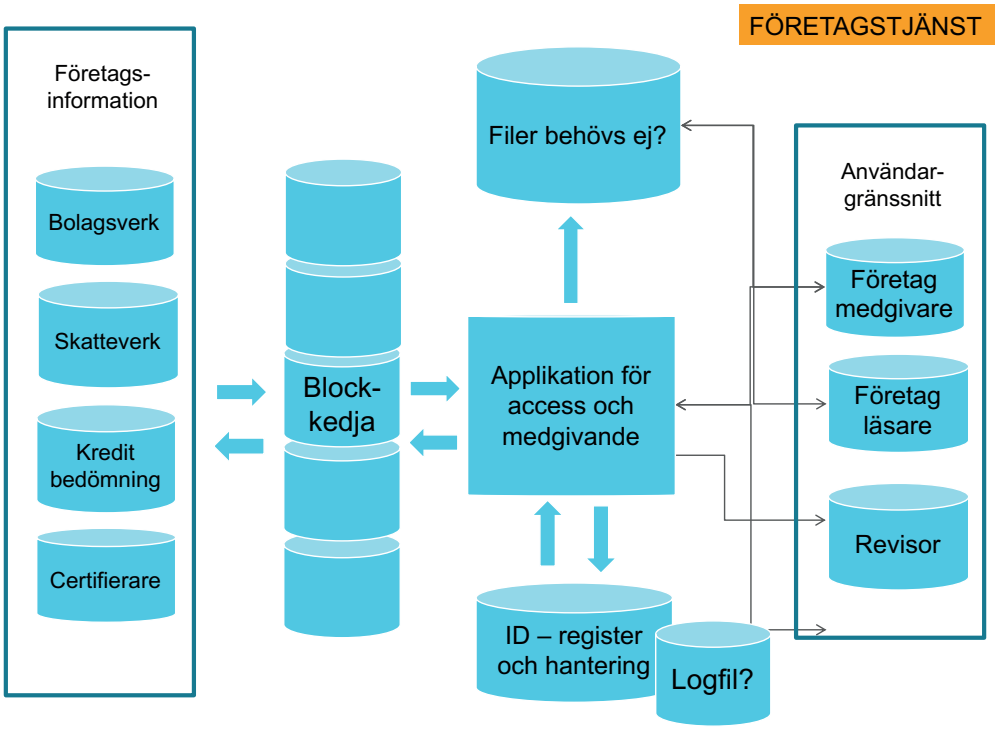
4. Det är en fördel om tjänsten är öppen för att bygga tjänster där företag och andra parter också kan bygga ut och tillföra information om sina egna organisationer eller för dem som vill sälja data.

5. Med införandet av GDPR kan det finnas fördelar om infrastrukturen ägs, förvaltas, eller överses av en eller flera myndigheter. Det kan tydliggöra rätten att lagra den underliggande datan.

Ett uppslagsverk för grundinformation i standardformat kan omfatta exempelvis:

• F-skatt
• Information om hur vill jag bli fakturerad. Här är Finlands höga andel digitala fakturor intressant och kanske kan Sverige inspireras? Kan tillgänglighet till digital faktureringsinformation underlätta?
• Betalningsformation
• Certifieringar, ESG, Certified Tax Payer, Authorised Economic Operator hos Tullverket. Att kunna kontrollera certifiering, att den är giltig och har utfärdats av relevant aktör.
• Lagerförare Ja / Nej
• Eventuellt kan frivillig registrering, alternativt tvingande registrering, av uppgifter som kan vara stöd för bedömning för andra vara en del av en tjänst. Exempelvis ett sätt att visa upp betaltider för leverantörsfakturor.

Översikt tänkbar arkitektur



Lösningsförslag/nästa steg

För denna tjänst finns det inte ett färdigt lösningsförslag. Det går att bygga en infrastruktur liknande beskrivningen ovan och vi tror sammantaget att det går att skapa stor samhällsnytta med en tjänst på detta område. Vi har däremot inte identifierat en enskild tjänst som i sig motiverar stora investeringar. Det räcker troligtvis inte med att bara ha en tjänst för att kontrollera ”har företaget F-skattsedel”. Vi har istället olika typer av data som har olika förutsättningar och därför kanske kräver olika lösningar.

I huvudsak ser vi två delar som behöver fördjupas.
1. Vilken typ av data och hantering av data är önskvärd?
2. Vilka lösningar finns redan idag i andra länder och vad fungerar bra och mindre bra med dessa lösningar?

Exempel på frågeställningar kring data

Vems data ska systemet omfatta? Är det enbart myndighetsägd data? Är det data som ägs av den som uppgiften berör? Är det data som samlas in och ägs av företag om andra företag? Ska systemet tillgängliggöra data helt fritt? Ska tillgängligheten vara begränsad i någon form? Ska det kosta något att få tillgång till informationen? Ska den som hämtar ut uppgifter registreras i systemet? Ska inhämtningen av data begränsas till de som har särskilt lagstöd för att hämta uppgifter? Ska systemet reglera vem som får tillgång till uppgifterna så att den som uppgifterna handlar om först får godkänna inhämtningen av dessa? Ska det finna data som inte går att förmedla trots medgivande?

Om en lösning ska hantera alla dessa frågor blir det stort och komplext.

Nöjer vi oss med enskilda tjänster blir det i stället viktigare att kostnaden för den enskilda tjänsten motiveras av ett stort värde. Vi behöver då se till att det finns organisationer och personer som vill använda tjänsten och som ser fördelar relativt dagens situation.

Förebilder i andra länder

Under projektets gång har vi fått uppgifter om att det finns tjänster i andra länder som kan fungera som inspiration.

Storbritannien
Erfarenheter från Storbritannien säger att användningen av vissa typer av data ökar markant genom att tillgängliggöra dessa. Det kan vara ett exempel på att tillgängliggöra data fritt på ett enkelt sätt. Vi vet inte om systemet också kan hantera data som ska begränsas i tillgänglighet. Det kan vara ett intressant exempel att undersöka vidare.

Norge
Ett annat land som har ett system som tycks fungera bättre avseende hantering av företagsuppgifter än Sverige är Norge. Där finns bl.a. en tjänst som heter Altinn. Tjänsten fungerar som en portal och blir ett naturligt gränssnitt för många olika typer av data. Norge har också historiskt varit framgångsrikt med att dela relevanta uppgifter mellan myndigheter. Det underlättar för företagen eftersom de inte behöver rapportera samma uppgifter i olika format till många myndigheter, som är fallet i Sverige. Vi vet inte om den norska hanteringen innebär medgivande till att hämta uppgifter eller hur de säkerhetsrisker som finns med ett centralt system hanteras idag.

Estland
I Estland finns ett befintligt system för inhämtning av data mellan myndigheter, X-road. Lösningen är en viktig del i Estlands IT-infrastruktur. Systemet innebär att en central myndighet överser systemet men kan samtidigt inte kontrollera vilken data som överförs mellan myndigheter i systemet. Det framstår som intressant ur säkerhetssynvinkel. Finland har nu anslutit sig till lösningen och Estland och Finland har tillsammans bildat NIIS, Nordic Institute for Interoperability Solutions. De arbetar med att skapa en tjänst som gör att viss datainhämtning kan kräva medgivande på förhand. Redan idag finns emellertid en loggfunktion som göra att de aktörer som hämtar ut data utan lagstöd kan straffas. Förmodligen räcker detta för att hantera data som kräver medgivande i många fall, men för att systemet skulle kunna användas på bred front bland myndigheterna i de aktuella fallen, var man emellertid tvungen att införa tvingande lagstiftning.

Sammantaget finns det allt fler exempel på lösningar i andra länder. Bolagsverkets arbete i Norden med Nordic Smart Government har troligtvis ännu mer kunskap om nuläget. Det behövs mer arbete med underlag innan vi inom detta projekt vill rekommendera någon enskild lösning att gå vidare med.

STOCKHOLM
Norrköping
Linköping
Jönköping
Göteborg
Halmstad
Hälsingborg
COPENHAGA
Malmö
Trelleborg
Karlskrona
Kalmar
Ottenby
I. Öland
I. Gotland
Visby
I. Bornholm
Rønne
MAREA BALTICA
Le Havre-Leningrad 2400 km.
Oslo
Arendal
Uddevalla
Karlstad
Västerås
Örebro
Uppsala
Gävle
Helsinki
Hankö
Tallin
Haapsalu
I. Hiiumaa
I. Saaremaa
Pärnu
Tartu
Valga
Ventspils
Liepaja
Riga
Elgava
Klaipeda
Daugavpils
Kaunas
Vilnius
Vileika
MINSK
Sovetsk
Kaliningrad
Suwałki
Olsztyn
Elk
Białystok
Baranovici
Gdynia
Sopot
Gdańsk
Tczew
Malbork
Hel
Golful Gdańsk
Darłowo
Koszalin
Szczecin
Sassnitz
Stralsund
Rostock
Wismar
I. Rügen
I. Falster
I. Fehmarn
Golful Pomeraniei
Bydgoszcz
Toruń
Gorzów Wielkopolski
Potsdam
BERLIN
Magdeburg
Dessau
Torgau
Dresden
Poznań
Kalisz
Łódź
VARŞOVIA
(WARŞZAWA)
Brest
Pinsk
Lublin
Radom
Wrocław
Częstochowa
Opole
Wałbrzych
Sosnowiec
Katowice
Gliwice
Kielce
Stalowa Wola
Kovel
Lutk
Novograd-Volinsk
Ostrava
Cracovia
(Kraków)
Jarosław
Lvov
Ternopol
Brno
PRAGA (PRAHA)
Tabor
Skagen
Hjørring
Ålborg
Randers
Århus
I. Samsø
Odense
Korsør
I. Fyn
I. Funen
Skagerrak
Vilia
DEALURILE BIELORUSE
Pripeat
Tampere
Turku
Lahti
Kotka
Narva
LENIN
Riga
Golful

Övriga stödtjänster

I projektet har det identifierats fyra stödtjänster som är en förutsättning för många andra tjänster. Det mest naturliga är troligtvis att den nya myndigheten för digital förvaltning, DIGG, får ansvaret för dessa tjänster framöver, åtminstone som samordnare eller beställare. Eftersom DIGG är en relativt ny och liten myndighet kan det uppfattas som många och stora saker, å andra sidan är det projektets bedömning att dessa tjänster är några av de få som är mest centrala för digitaliseringen och att ansvaret inte kan delas upp på många olika myndigheter. För tre av dessa tjänster finns det för övrigt redan ett ansvar eller ett regeringsuppdrag för DIGG.

De fyra tjänster som bör finnas är:

1. Ett ramverk för eID-tjänster, med tillhörande underskriftstjänster.
   – Kring denna fråga pågår det redan ett arbete och e-legnämnden har nu blivit en del av DIGG. Se vidare information under avsnittet om teknik.

2. En tjänst för adresser/digital post till organisationer och medborgare
   – Tjänsten ”mina meddelanden” har flyttats från Skatteverket till DIGG. Medan frågan om en identifieringstjänst för organisationer har både för- och nackdelar finns det klara fördelar med att ha en tjänst för att skicka meddelanden till organisationer i likhet med den analoga världen. Till exempel kan en personalliggartjänst övervaka om någon missat att registrera sin personalliggare och ett meddelande kan skickas till an digital ”postlåda” som ”mina meddelanden” i det fall det är aktuellt. I exemplet med digitala kvitton kan det vara ett sätt att kunna

skicka ut nya koder för organisationen att registrera sina kvitton med, t.ex. om de gamla saknas eller tappats bort.

3. En kommunikationstjänst för effektiv inhämtning och delning av myndighetsinformation
   – I arbetet med SINK har behovet av att enkelt utbyta information mellan myndigheter identifierats. Migrationsverket har uppgifter om arbetstillstånd som Skatteverket behöver för att kunna fatta beslut om SINK. I fallet med en företagstjänst är frågan om delning av information mellan såväl myndigheter som företag och privatpersoner central.
   – Kring denna fråga finns ett regeringsuppdrag och ett projekt där Skatteverket, Lantmäteriet, Bolagsverket m.fl. ingår och som samordnas av DIGG. Inom ramen för detta tittar man exempelvis på estländska X-road. Frågan om delning av myndighetsinformation har många juridiska aspekter att ta hänsyn till. Beträffande teknik är det en intressant lösning som Estland använder och den är vad vi vet den mest använda och väl fungerande infrastrukturen för att dela information. Finland har nu anslutit sig till systemet och de har bildat en separat organisation för att utveckla och drifta tekniken, NIIS. Tekniken omfattar många av de egenskaper som karaktäriserar blockkedjeteknik, d.v.s. privata och publika nycklar, hashar, merkleträd och en infrastruktur för peer to peer kommunikation. Det är däremot inte en konsensusalgoritm där databaser har synkroniserad information. Den centrala organisationen håller framför allt reda på att identiteterna är godkända och kan ta emot och skicka förfrågningar. De håller också en logg över förfrågningar. Den centrala myndigheten samlar däremot inte in informationen och kan heller inte läsa vad som skickas inom nätverket.

4. En notariattjänst för rättssäker validering av digital information
   – Förutom de ovanstående tjänster, där det redan pågår ett arbete och

ansvaret för detta är delegerat, är behovet av en digital notariattjänst stort. I dagsläget finns det oklarheter när det gäller digitala bevis och deras rättsverkan, arkivbeständighet och tolkningen av lagringsmöjligheter enligt GDPR. En myndighetstjänst skulle fylla ett mycket värdefullt behov av att kunna registrera ”kombinationshashar”, d.v.s. topphashar av andra blockkedjor och tjänster. I praktiken är detta en blockkedja, eller ett merkleträd dit licensierade aktörer kan registrera bevisinformation (vanligen hashar) och eventuellt mot en ersättning. Den myndighetskontrollerade tjänsten kan garantera rättsverkan, arkivbeständighet och de krav som GDPR ställer. I dagsläget kan det exempelvis finnas en oklarhet om ett bevis t.ex. en hash av ett digitalt avtal får sparas trots att det vid upprättandet av avtalet är uppenbart att avtalsparterna önskar att det ska finnas ett digitalt bevis åtminstone under en bestämt tid, exempelvis avtalets längd. I fallet med fullmakterna skulle det kunna vara värdefullt att kunna hänvisa till att verifikationerna som bekräftar fullmaktens validitet och avslutande finns lagrade eller bekräftade i en myndighetskontrollerad notariattjänst.
– Detta kan liknas vid en registrering hos Post- och Inrikes Tidningar anpassad för den digitala världen och dess möjligheter.
– Det finns liknande tjänster hos exempelvis Guardtime men av nämnda skäl underlättar det att veta de specifika förutsättningarna enligt svensk lag. Det kan också finnas ett intresse av att spara mer information i notariattjänsten och en betalningsvilja för att kunna göra det. Så gott som samtliga aktörer som arbetar med blockkedjetekniken och som ställts inför frågan om behovet av en liknande tjänst förstår värdet av detta. För svenska myndigheter skulle en sådan tjänst kunna bli en viktig infrastruktur för att i sin tur skapa säkra system för versionshantering, originalhandlingar med mera, något som bland annat Digitaliseringsrättsutredningen uppmärksammat och ett flertal myndigheter i dagsläget ser som utmanande frågor.

Tekniska förklaringar

För att förstå de lösningar som beskrivs i rapporten är det några tekniska begrepp som är värdefulla att känna till. Dessa beskrivs översiktligt nedan.

För mer djupgående analys av tekniken är det lämpligt att utgå ifrån begreppen nedan, PKI, Certificate Authourity, Merkle tree, Hash osv och söka sig vidare på Internet. En välskriven bok om kryptering är The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography av Simon Singh. Det är med andra ord ett förslag och en rekommendation att börja med att förstå kryptering och först därefter blockkedjan.

Något mer utförliga beskrivningar av blockkedjetekniken och dess tillämpningar från svenska projekt finns här.
https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

https://www.kairosfuture.com/se/publikationer/rapporter/blockchain-use-cases-for-food-tracking-and-control/

Privata och publika nycklar

Traditionell kryptering har byggt på tanken att det finns ett dokument, t.ex. ett avtal, som krypteras med en krypteringsnyckel. Resultatet blir ett oidentifierbart meddelande. Den som på ett eller annat sätt får tag på krypteringsnyckeln, eller knäcker koden, kan återskapa ursprungsmedde-

landet. Denna krypteringsteknik kallas synkron. Den som har kunskap om krypteringsnyckeln kan dekryptera meddelandet.

Privata och publika nycklar är ett vanligt sätt att generera koder med ytterligare en finess. Vi kan veta att någon har en krypteringsnyckel – utan att visa upp den för oss. Den som krypterar har då inte samma krypteringsnyckel som den som dekrypterar. Denna teknik kallas asynkron och har revolutionerat användandet av digital teknik, till exempel Internet. I väldigt många sammanhang i den digitala världen vill vi veta vem som agerar på andra sidan nätverket, någon form av elektronisk identifiering, eID, behövs oavsett om det är ett internt nätverk eller Internet.

Privata och publika nycklar är en lösning på det problemet. Den som ska identifiera sig har då tillgång till en privat nyckel, d.v.s. en kod med siffror och bokstäver. Till den privata nyckeln hör en speciell publik nyckel. Den publika nyckeln kan delas ut fritt, till exempel på Internet. Om Astrid vill identifiera sig kan Bertil veta att det är just Astrid som skrivit ett meddelande, gjort en signatur på ett dokument, eller liknande. Bertil vet det eftersom ett meddelande som krypteras med den privata nyckeln kan dekrypteras med den tillhörande publika nyckeln. Med andra ord kan Bertil dekryptera meddelandet med den publika nyckeln. Om dekrypteringen är lyckad vet han att det måste ha varit en person med tillgång till Astrids privata nyckel som har krypterat meddelandet – i annat fall skulle det inte gå att dekryptera med Astrids publika nyckel. Tekniken fungerar också åt andra hållet, d.v.s. Bertil kan kryptera ett meddelande med Astrids publika nyckel – och bara Astrid kan läsa det med den privata nyckeln. Bertil kan däremot inte dekryptera sitt eget meddelande, trots att han gjorde krypteringen med Astrids privata nyckel.

Eftersom det är lätt att generera nya privata och publika nycklar föreslår vi den tekniken i några av lösningarna i rapporten.

Certificate Authorityu, CA

Ett problem kvarstår emellertid i exemplet ovan. Hur vet Bertil att den publika nyckeln han kan få tillgång till verkligen tillhör Astrid? En annan person, vi kan kalla honom Edvin, kanske har lagt ut en publik nyckel och påstår att det är Astrids? För att garantera att den publika nyckeln tillhör Astrid finns en Certificate Authority, ofta kallad CA. Denne har till uppgift att hålla ordning på vilka publika nycklar som tillhör vilken individ. Observera att CA:n inte behöver kunna Astrids privata nyckel. CA:n kan däremot påstå att en annan nyckel är Astrids och därmed lura Bertil. Om någon hackar CA:n är det därför ett stort problem eftersom denne kan påstå att alla andra har felaktiga nycklar. Säkerheten kopplad till CA:n är därför central. Den infrastruktur som omfattar privata och publika nycklar, CA mm kallas ibland Public key infrastructure (PKI).

I Sverige är det vanligast med identifiering med Mobilt Bank-ID, och företaget Finansiell ID-teknik är CA för dessa eID. Det finns emellertid flera legitimationer som kan användas av privatpersoner för att identifiera sig, d.v.s. de har lagstöd som e-legitimationer, exempelvis e-legitimation från Telia. Nu finns även ett myndighetsgodkännande som kan ges i form av att bli godkänd som svensk e-legitimation, vilket Freja eID blivit.

Per den 29 september 2018 är eIDAS, EUs lagstiftning för e-legitimationer och betrodda tjänster bindande för EU:s medlemsländer. Detta medför att alla e-legitimationer som blivit godkända enligt eIDAS kommer att behöva accepteras i alla länder inom EU som godkända e-legitimationer. För att det ska bli praktiskt möjligt att integrera tiotals, kanske hundratals godkända ID-lösningar, har eIDAS ålagt varje land att inrätta en form av ID-växling. Den nyinrättade myndigheten för digital förvaltning, DIGG, har fått ansvar för e-legitimationsnämnden och har

också byggt denna typ av växlingstjänst. I växlingstjänsten ingår två delar, en för utgående eID dvs identifiering som gjorts med ett svenskt eID och ska användas i ett annat land. Den andra tjänsten finns för att inhämta ett godkännande av eID från ett annat land som använder en svensk tjänst. I praktiken är arbetet med att sätta upp dessa växlingstjänster inte alls färdigt i den utsträckning EU-lagstiftningen egentligen kräver. Ett tiotal medlemsländer verkar dock vara på god väg med att upprätta systemet.

Utöver de funktioner där det redan finns ansvariga myndigheter finns det ett värde av att kunna säkerställa mer information om individers roller och befogenheter.

Detta område omfattar frågor som behörigheter, befogenheter, ombud, fullmakter, ställningsfullmakter och KYC (Know Your Customer) av individer. I denna rapport har vi tagit fram ett förslag på lösning för fullmakter. Det finns ett antal andra pågående arbeten kring dessa frågor utöver eIDAS. Några exempel är:

- Frågan om behörigheter hanteras vanligen av dagens IT-system för respektive organisation.
- Frågan om KYC är något som är särskilt värdefullt för banker och kreditinstitut. Där finns ett pågående projekt mellan de nordiska bankerna med blockkedjeteknik som stöd för att upprätta detta.
- Hantering av ombud är en fråga som nu ska utredas i ett myndighetsgemensamt projekt.
- I mars 2019 ska en utredning presenteras som ska utreda frågan om ett nytt svenskt myndighetsägt ID som väntas ersätta körkorten, men det är alltså tillsvidare inte ett eID
- Det finns ett nordiskt samarbete kring ID, NOBID

Underskrifter och betrodda tjänster

eIDAS reglerar förutom eID även betrodda tjänster eller digitala signaturer. Förutom att göra en identifiering av en person så behövs det ibland ett bevis på att en person blivit identifierad, skrivit under och att det beviset kan knytas till ett dokument, i praktiken en digital fil. För detta syfte behövs en signeringstjänst.

En hash, ett digitalt bevis

Den kanske viktigaste tekniska komponenten i det som idag kallas blockkedjeteknik är möjligheten att skapa unika verifikationskoder av digitala filer, dvs foton, transaktionslistor, register, avtal, videofilmer, patent m.m. Verifikationer kan skapas av allt som går att lagra som en digital fil. Verifikationerna gör det möjligt att fastställa att digitala filer inte har ändrats, en funktion som är oerhört central. Detta är viktigt eftersom det inte finns några tillförlitliga sätt att veta om en digitalfil har ändrats, med mindre än att krypteringsteknik används som innehavaren av den digitala filen inte själv kontrollerar.

Med hjälp av en avancerad ”fingeravtrycksalgoritm” kan vilken digital fil som helst få en unik verifikationskod. Tekniskt kallas detta för en kryptografisk hash. Ett exempel på en algoritm som skapar kryptografiska hashar är SHA256. Denna algoritm tar alla ettor och nollor som beskriver ett digitalt dokument och räknar om dessa enligt ett bestämt, men oförutsägbart mönster. Oberoende av vilken datamängd ursprungsfilen har är resultatet alltid en mindre kod som alltid har samma format, dvs antal tecken.

Hashen uppfanns redan på 50-talet men användningen har tagit fart på senare tid. Den allra viktigaste egenskapen hos en hash är att den inte kan backas. På samma sätt som det inte går att återskapa en människa från den begränsade information som finns i ett fingeravtryck går det inte att återskapa en digital fil från en hash. Till skillnad från den krypteringsteknik som i flera tusen år varit den enda kända är det alltså inte möjligt ens för den som känner till krypteringsalgoritmen att förstå hur ursprungsfilen ser ut. Jämfört med synkron och asynkron kryptering finns det för hashar ingen dekryptering alls. Det går inte att återskapa ursprungsfilen.

Hashen kan bestå av 64 tecken, vilket är alldeles för lite information för att förstå hur en bokföringsfil med en årsredovisning ser ut. Om bokföringsfilen omfattar flera megabyte kan det inte återskapas med ett fåtal siffror och bokstäver.

Antalet kombinationer hashar är samtidigt ett större tal än en etta med 64 nollor efter (eftersom det innehåller bokstäver också). Sannolikheten att två hashar av en tillfällighet blir likadana är därför i praktiken noll. Det betyder att den som har ursprungsfilen kan återskapa hashen, d.v.s. fingeravtrycket, men ingen annan. Samtidigt kan ägaren av filen inte göra en ändring utan att det märks för någon som har den ursprungliga hashen.

Denna egenskap är helt avgörande för de lösningar som beskrivs i denna rapport. Fullmaktsgivaren och fullmaktstagaren kan exempelvis dela med sig av en hash avseende sin fullmakt utan att avslöja innehållet i fullmakten. Givet att innehållet i ett digitalt kvitto är tillräckligt omfattande går det inte att utifrån en hash som ligger i ett kvittoregister förstå kvittots innehåll. Möjligheten att vara anonym är avgörande i dessa fall.

Merkleträd

Låt oss anta att en fullmaktstagare och fullmaktsgivare vill att det ska finnas ett bevis för fullmaktens innehåll och att detta inte är manipulerat. De kan då låta en tredje part förvara en hash av fullmakten. Nackdelen med detta är naturligtvis att denna tredje part, eller någon anställd hos denna kan manipulera hashen. För att eliminera detta problem läggs hasharna in i en ordningsföljd där varje hash som ska läggas till utgör en del i en ny hash. I exemplet med fullmakten tar vi den första hashen nr 1 av fullmakt nr 1. När det kommer en ny hash av fullmakt nr 2 tar vi dessa två hashar 1 och 2 och gör en ny fil och gör en ”kombinationshash” hash 1+2 av den nya filen. När det kommer en tredje fullmakt tar vi ”kombinationshashen” slår ihop den med den nya fullmaktshashen nr 3 och skapar en ny ”kombinationshash” (1+2)+3.

Resultatet av detta förfarande leder till att den sista kombinationshashen låser all underliggande information. Ändras någon av fullmakterna 1, 2 eller 3 kommer denna hash och kombinationshasharna inte längre att stämma.

Eftersom alla nya hashar som kommer in i merkleträdet använder den sista kombinationshashen får vi dessutom en tidsordning för all information. Vi vet att den sista fullmakten nr 3 kommer att få sin verifikation sammanslagen med en kombinationshash som innehåller hänvisningar till alla tidigare fullmakter. Hash 1 och 2 måste därför ha registrerats före hash nr 3.

Tidsordningen eller tidsstämplingen som den ibland kallas, är värdefull eftersom vi kan veta vilken fullmakt och vilken information om fullmakten som är den senaste. I fallet med personalliggare är det också värdefullt

att veta när personalliggarna registrerats. Görs det en uppdatering vet vi vilken version som gäller. Har det gjorts registreringar av personalliggare varje dag den senaste månaden är detta lätt att kontrollera. Det är heller inte möjligt för den som tillhandahåller merkleträdet att göra ändringar, givet att kombinationshasharna publiceras, åtminstone en gång per dag till exempel. En av de mest använda aktörerna på denna arena är Guardtime som samarbetar med de estländska myndigheterna, USAs försvarsdepartement, Ericsson, Verizon etc. De publicerar sin kombinationshash, också kallad tophash, i Financial Times en gång i månaden.

Blockkedja

Det som vanligtvis avses med en blockkedja är att merkleträdet också ska vara säkert för manipulation och inte vara beroende av en enda databas. Ytterligare ett skäl är att det kan finnas en möjlighet att ägaren av merkleträdet prioriterar inkommande hashar för egen vinning, något som är väldigt värdefullt på finansmarknaderna. Om någon fick en möjlighet att registrera sin handel med aktier före andra skulle det vara oerhört värdefullt. Givet att kombinationshashen hålls hemlig under ett par dagar kan det också vara möjligt att göra ett nytt träd och stoppa in nya hashar och därmed göra en ny tidsordning mm. För att undvika detta problem kan det därför vara viktigt att ordna databaserna i en distribuerad struktur där fler aktörer kan säkra ordningsföljd av datan, att den följer uppsatta regler, att den inte förstörs osv. Det innebär att det finns flera databaser som alla innehåller samma merkleträd. Olika system för blockkedjor använder sig av särskilda algoritmer för att säkerställa att alla databaser är synkroniserade, dessa algoritmer kallas konsensusalgoritmer. Genom att låta flera aktörer ha en synkroniserad databas med merkleträdet ökar förtroendet för den.

Publika blockkedjor

De blockkedjor som framför allt förknippas med kryptovalutor kallas publika blockkedjor. Denna teknik används inte i de förslag som beskrivs i denna rapport. Ett par problem som ibland lyfts fram med publika blockkedjor är därför inte relevanta. Exempel på problem som ofta tas upp i samband med blockkedjor, men som alltså inte är aktuella i våra exempel i denna rapport är t.ex.:

1. Energiåtgång – publika blockkedjor använder ofta en teknik som kallas Proof of Work. Den tekniken kräver stora mängder energi.

2. Skalbarhet – publika blockkedjor har kapacitetsbegränsningar. Det går inte att registrera för stora mängder data i dessa.

3. Transaktionshastighet – publika blockkedjor har svårigheter med snabbheten att registrera hashar och annan information.

4. Radera uppgifter – i publika blockkedjor går det inte att radera gammal information. Det beror på att blockkedjor som används till kryptovalutor behöver vara tydliga med hur många kryptovalutor som skapats sedan blockkedjan startade.

5. Stölder och förluster – stulna eller borttappade privata nycklar kan innebära att stora belopp går förlorade. Det är möjligt att förlora privata nycklar även i de beskrivna lösningarna, men förlusterna är i dessa fall små eller obefintliga.

Blockchain har beskrivits som en trustless-teknik, d.v.s. en teknik där du inte behöver lita på andra. I praktiken har detta sitt ursprung i publika

blockkedjor som Bitcoin eller Ethereum där en enskild individ eller organisation inte kan ändra registreringar som gjorts av systemet. Om du har sålt dina Bitcoin finns det inget sätt att ta tillbaka pengarna eller ta bort registreringen. Det kan göras en ny transaktion men den gamla kan inte göras ogjord. Den som kontrollerar den privata nyckeln som har tillgång till respektive Bitcoin kan spendera dessa och när det är gjort är det någon annan som har kontrollen. I slutändan betyder det att var och en måste lita på sig själv när det gäller förvaringen av de privata nycklarna, vilket är riskabelt. Få människor vill att deras pension går förlorad bara för att de tappat bort en personlig kod, datorns hårddisk blir hackad eller går sönder. I fallet med Bitcoin använder därför de flesta ett förvaringsinstitut, någon organisation som tar ansvaret för att lagra dessa privata nycklar, vilka i sin tur kontrollerar Bitcoin. När ett förvaringsinstitut hackas av någon på insidan eller utsidan, vilket har hänt, vill ägarna ha ett system för tvister för att få tillbaka sina pengar. Detta gör att de rättmätiga ägarna till kryptovalutor har ett stort behov av någon form av försäkring, brottsbekämpning eller annat skydd, vilket, åtminstone idag, förutsätter institutioner i den övriga världen.

FAR är branschorganisationen för revisorer, redovisningskonsulter, skatterådgivare, lönekonsulter och specialister. FAR bidrar till branschens utveckling genom rekommendationer, utbildning och remissverksamhet. FAR arrangerar utbildningar, ger ut böcker, regelverk och digitala tjänsten FAR online, samt två tidningar - Balans och Resultat. FAR:s uppdrag är att hjälpa branschen att göra nytta för näringsliv och samhälle. Detta sker främst genom: Utveckling av god yrkessed, Kompetensutveckling, Opinionsbildning .Våra medlemmar, cirka 5 100, är auktoriserade och godkända revisorer, auktoriserade redovisningskonsulter, skatterådgivare, auktoriserade lönekonsulter och andra specialister, exempelvis inom hållbarhetsredovisning.

Skatteverket är till för alla i samhället. Vi vill att det ska vara lätt att göra rätt – till exempel när du betalar skatt, säljer eller köper bostad, startar och driver företag, flyttar eller gifter dig. Vårt uppdrag från regeringen består av tre delar: Bidra till ett väl fungerande samhälle för privatpersoner och företag, Bidra till att säkra finansieringen av den offentliga sektorn, Motverka brottslighet. Det innebär att vi arbetar med skatter, folkbokföring, äktenskapsregistret, fastighetstaxering, bouppteckningar, id-kort och att utreda skattebrott. Vi är också borgenär åt staten. Vi har drygt 10 000 medarbetare och har verksamhet i hela landet.

Kairos Future är ett internationellt konsult- och analysföretag som hjälper företag att förstå och forma sin framtid. Genom trend- och omvärldsanalys, innovation, strategi och mjukvarustöd för AI-driven analys, omvärldsbevakning och innovation, hjälper vi våra kunder att omsätta de stora sammanhangen till konkret handling. Kairos Future grundades 1993, vårt huvudkontor finns i Stockholm och vi har egna kontor eller samarbetspartners över hela världen.

Kairos Future AB | P.O. Box 804 | S-101 36 Stockholm | Sweden
Phone: +46 (0) 8-545 225 00 | www.kairosfuture.com