Autenticitet hos digital information

Blockkedjeteknologi för upprätthållande av trovärdighet

Av: Jan Asplund

Handledare: Proscovia Svärd

Södertörns högskola | Institutionen för historia och samtidsstudier

Arkivvetenskap C, HT - 17

Självständigt arbete 15 hp

SÖDERTÖRNS HÖGSKOLA | STOCKHOLM
sh.se

Arkivvetenskap
Södertörns Högskola
14189 Huddinge

Abstract

Authenticity and integrity of digital information have been discussed extensively within the record management and archival sectors for several decades. The on-going projects and research in the area have resulted in an understanding of the potential problems when it comes to keeping authenticity in digital information. In recent years the blockchain technologies have gained attention as a potential solution to many of the problems associated with management and storage of digital records. The area of information security is getting more and more focused on preventing manipulation of existing data. The conclusions here is that blockchain technologies have potential to solve several problems associated with the management and storage of digital records. The archival sector can benefit from the use of blockchains to prevent time consuming and expensive work efforts to re-establish authenticity in digital information ones lost.

Keywords: Authenticity, Blockchain, Digital Records, Archives, Principle of Integrity, Digital information

Innehållsförteckning

1. Inledning

En inom många områden idag uppmärksammad teknologi är blockkedjeteknologin vilken ävenlyfts fram av flera forskare som en potentiell lösning på problem kring autenticitet och trovärdighet hos digital information. Blockkedjeteknologin lanserades 2008 av en anonym person eller grupp som kallade sig Satoshi Nakamoto i samband med lanserandet av kryptovalutan Bitcoin (Nakamoto 2008). Blockkedjeteknologin har uppmärksammats inom många olika discipliner och det pågår idag forskning kring dess potential inom många olika områden (Shrier m.fl. 2016). Teknologins potential ur arkivvetenskapliga perspektiv har diskuterats av framförallt Victoria Lemieux vid University of British Columbia och Hrvoje Stancic, co-director för InterPARES trust (Lemieux 2016a, Bralic m.fl. 2017). Eftersom att blockkedjeteknologin är ny och det ännu inte publicerats så mycket litteratur som visar på hur den skulle kunna användas i dokument och arkivhantering, fann jag det intressant att undersöka teknologins potential inom detta sammanhang.

Dokument och arkivhantering syftar till att upprätthålla en systematisk hantering av information. Med dokumenthantering i den här uppsatsen menas ”Records Management” som är en systematisk hantering av ”records” dvs. de dokument som ska upprätthållas enligt vissa kriterier såsom autenticitet och reliabilitet. Det är denna process som sedan leder till skapandet av arkivhandlingar. Skäl till att ha en fungerande hantering och systematisk sökbarhet av information kan vara antingen lagstyrda, motiveras av effektivitetsvinster samt ett historiskt ansvar att bevara det gemensamma kulturarvet eller den egna verksamhetens historia. Den information som finns bevarad i arkiven ska vara tillförlitlig, komplett och äkta (TAM-Arkiv 2014). I de första stadsliknande bildningarna uppstod tidigt behov av att upprätthålla autenticitet hos dokument för både rättskipning och beslutsfattande (Hoffman 2017). Autenticitet har alltså varit viktigt sedan länge vilket kan exemplifieras med att i antikens Rom anförtrodde högre ståndsperoner sina testamenten till vestalerna för säker förvaring då Vestastemplet ansågs vara den säkraste plats som fanns tack vare kombinationen av vestalernas strikta levnadsregler och höga anseende (Vestal Virgins of Rome 2017).

För att avgöra äkthet och trovärdighet hos medeltida dokument utvecklades ämnet diplomatik av Jean Mabillon i verket *De re diplomatica* från 1681 (Wendt 2013). Diplomatiken gav i sig upphov till nya discipliner med syfte att avgöra ursprung och

trovärdighet som till exempel paleografi, sfragistik och heraldik (Duranti 2010). Diplomatik kan jämföras med diplomatens uppdrag att förmedla korrekt information mellan olika länders regeringar, information måste förvaltas och förmedlas utan risk för förvanskning för att inte förlora trovärdighet och därmed sitt bevisvärde (John 2012 s. 47).

En stor del av den information som hanteras i samhället idag är digital och lagras i olika format på olika medier och plattformar. Precis som för samhället i övrigt så blir även en allt större andel av den information som bevaras hos arkiven skapad, bearbetad och lagrad på digitala enheter av olika slag. Som med pappersbunden information är det viktigt att digital information är autentisk och trovärdig för att vara till nytta inom rättskipning, forskning, förvaltning eller för affärstransaktioner. Den tekniska utvecklingen för hantering och lagring av information har i en historisk jämförelse gått fort de senaste decennierna. Kassettband, disketter, CD- skivor med mera lagrade revolutionerande stora informationsmängder på litet utrymme när de lanserades jämfört med pappersburen information. Utvecklingen går idag från fasta fysiska lagringsmedia mot att alltmer information både genereras, bearbetas och lagras i olika typer av molntjänster. Detta ställer andra krav på metoder för att sammanhålla information och upprätthålla dess autenticitet, något som är en utmaning för arkivinstitutioner och ställer krav på kompetens inom informationssäkerhetsområdet (John 2012). Mot denna bakgrund finner jag det intressant att undersöka om blockkedjeteknologin kan appliceras inom dokument- och arkivhanteringsområdet för att upprätthålla autenticitet hos digitala records.

1.1 Problemformulering

Vid skapande och lagring av information behövs ett säkerhetstänk från början. Telecomföretaget Ericsson motiverar sin satsning på säkerhetstjänster för digital information som bygger på blockkedjeteknologi med att det sker en förändring i attityd inom säkerhetstänkandet. Istället för att fokus som tidigare legat på att hindra obehörig åtkomst av information fokuseras nu mer på att hindra möjligheter till manipulation (Data Centric Security 2017). Det är viktigt att tänka på informationens livscykel, vem kommer använda informationen och om den kommer bearbetas vidare i den form den från början lagrades eller om den kommer användas som referens. Att lyfta fram och undersöka nya metoder och tekniker som har potential att hjälpa till med att upprätthålla autenticitet och trovärdighet hos digital information är viktigt för att hitta lösningar på problematiken. Autenticitet hos digitala records är något som är centralt för Arkivvetenskap och därför är blockkedjeteknologins potential och utveckling intressant.

1.2 Syfte och frågeställningar

Syftet med det föreliggande arbetet är att undersöka hur blockkedjeteknologi kan appliceras inom dokument och arkivhanteringsområdet för att upprätthålla autenticitet hos digitala records. För att uppfylla syftet kommer följande frågeställningar att besvaras:

1. Vilka problem kring digital informationsautenticitet diskuteras inom arkivvetenskap?

2. Hur skulle blockkedjeteknologi kunna lösa de problem kring autenticitet hos digital information som diskuteras inom det arkivvetenskapliga området?

3. Vilka potentiella för- och nackdelar finns kring blockkedjeteknologin?

1.3 Avgränsningar

Det föreliggande arbetet behandlar frågor kring autenticitet och trovärdighet hos digitala records ur ett arkivvetenskapligt perspektiv och med inriktning på risker kring förvanskning av informationen i dem. Undersökningen går inte in på säkerhetsfrågor som rör obehörig åtkomst av information eller metoder för att hemlighålla dokumentation av till exempel sekretesskäl eller andra anledningar. Arbetet undviker i möjligaste mån att gå in på datatekniska detaljer och systemvetenskapliga beskrivningar. Viss referering till områden utanför arkivvetenskapen är dock nödvändigt för att motivera undersökningen och få in den i större samanhang.

1.4 Metod

Undersökningen genomförs med en kvalitativ metodologi. Kvalitativa metoder går ut på att förstå det fenomen man studerar genom att skapa en helhetsbild kring vilka faktorer som spelar in för att tillslut utifrån insamlad data skapa ny kunskap om företeelsen (Pickard 2013 s. 267). I en kvalitativ undersökning samlas data in och analyseras kontinuerligt under processen. För att samla in data till undersökningen har jag gjort en litteraturstudie, vilken är en är en systematisk genomgång av för ämnesområdet relevant vetenskaplig litteratur. Den litteratur som används vid en litteraturstudie bör i möjligaste mån bestå av originalartiklar publicerade i vetenskapliga tidskrifter (Korhonen & Lindström 2016). Litteraturstudien klargör undersökningens mål och visar vilka kunskapsområden som är relevanta samt formar det empiriska ramverket (Pickard 2013 s.25). Det är litteraturstudien som ligger till grund för

teoribeskrivning av de för ämnet grundläggande begreppen autenticitet, diplomatik, trovärdighet, proveniens och informationssäkerhet.

Efter att ha gjort sökningar på begreppet blockchain tillsammans med ord som information, archive och records i vetenskapligt inriktade sökmotorer som Google Scholar och Söder Scholar kan konstateras att det ännu inte publicerats någon större mängd forskning kring blockkedjeteknologins användande i dokument och arkivhantering. Vid sökningar efter litteratur i databaser och sökmotorer användes även den svenska benämningen blockkedja tillsammans med begrepp som informationssäkerhet, dokument och arkivhantering. Bristen på publicerad forskning inom området bekräftas av den genomgång av vetenskaplig litteratur rörande blockkedjeteknologi som gjordes 2016, vilken då visade att över 80 % av artiklarna handlade om kryptovalutan Bitcoin och således mindre än 20 % av artiklarna berörde något annat potentiellt användningsområden (Yli-Huumo m.fl. 2016). För att hitta information kring användandet av tekniken har jag förutom vetenskapliga artiklar även använt mig av tidskrifter, nyhetspublikationer och information från företag och organisationers hemsidor, för att få en så bred och aktuell bild av användandet av teknologin som möjligt. Mitt mål var att hitta några pågående fall som använder blockkedjeteknologi för att undersöka i form av fallstudier men hann inte få till en fallstudie inom tidsramen för arbetet. Jag kontaktade personer som jobbar på företag som håller på med blockkedjor i olika sammanhang för att försöka nå personer inom arkivområdet som eventuellt skulle kunna hjälpa till med att hitta lämplig pågående projekt och verksamheter inom blockkedjeområdet. Delar av den kommunikation jag haft med olika företag har dock använts som komplement till litteraturstudien. För att få en bild av hur känd teknologin är bland yrkesverksamma inom arkivområdet i Sverige genomförde jag en enklare enkätundersökning. Undersökningen utfördes i Facebookgruppen ”Arkivarier i Sverige” som består av ca 1400 medlemmar vilka är yrkesverksamma som arkivarier eller inom närliggande områden. Enkäten bestod av tio påståenden där deltagarna valde det som beskrev deras kännedom om blockkedjor bäst. De tio alternativen kan omsättas till siffror där 1 blir lika med att man aldrig hört talas om blockkedjor till och med 10 som motsvarar att man varit med och utvecklat ett färdigt fungerande system som bygger på teknologin. De svar jag fick från kontakt med företag och resultatet från de 107 svarande i enkätundersökningen redovisas under rubrik *5 Svenska Blockkedjeprojekt och Kunskap bland arkivarier*.

Detta betyder att undersökning till största delen består av en litteraturstudie vilken kompletteras med en mindre empiriskstudie samt information från direktkontakt med personer som arbetar med blockkedjor.

De teman som jag har använt mig av under rubriken litterastudie och de data jag samlade in via email kontakt och enkätundersökningen ligger till grund för de teman som redogörs för i det följande arbetet. Genom litteraturstudien och en kvalitativ innehållsanalys kunde viktiga aspekter identifieras vilka bildar de teman som redovisas under litteraturstudien. En kvalitativ innehållsanalys analyserar texter och kommunikation med fokus på att identifiera likheter och skillnader efter att först ha skapat en helhetsbild (Arving 2012).

1.5 Begreppsdefinitioner

I uppsatsen används följande begrepp:

Algoritm
Programmering av datorer går ut på att beskriva algoritmer som ska utföras av maskiner och samtidigt förstås av människor. En algoritm är en stegvis procedur av definierade och utförbara instruktioner avsedda att utföra en uppgift eller lösa ett problem. Algoritmer används ofta med kravet att proceduren ska ha ett slut (Algoritmer 2009).

Blockkedjeteknologi
Blockkedjeteknologi är en metod att skapa unika verifikationer för digitala filer. Med hjälp av en algoritm, eller kryptografisk hash, kan vilken digital fil som helst förses med en unik kod. Blockkedjor kan jämföras med en öppen liggare eller huvudbok där varje ny notering måste göras av minst två personer samtidigt (Lemieux 2016b). Mer om blockkedjeteknologi följer under rubrik *4.3 Hur blockkedjeteknologi fungerar*.

Diplomatik
Den vetenskapliga disciplinen diplomatik undersöker autenticiteten hos äldre dokument. Från början var det främst medeltida kyrko- och klosterprivilegier och andra juridiska dokument vars bevisvärde behövde bekräftas (Fritz 2017). Begreppet diplomatik utvecklades och breddades under 1980 och 90 talen till att även innefatta digitala dokument och används idag i samband med undersökning av digitala records och annan elektronisk information i arkiv och dokumenthanteringssamanhang (InterPARES 1 2001).

Hash och Hashsumma

En metod att ersätta längre söknycklar med ett kort men obegriplig tal kallat hashsumma. Med hjälp av en algoritm förvandlas begripliga tecken till en slumpmässig serie tecken vilken tar mindre plats samtidigt som den gör uppgifter obegripliga för den som inte har en hashfunktion eller hashnyckel, som kan tyda hashsumman (Hash och hashing 2010).

Exempel på kryptering med hashfunktion följer här. Hashsumman för denna uppsats var klockan 12.11 den 23 November 2017: 288b739b2880fd8e31c42eade279fcfe. Hashsumman är uträknad av algoritm MD5 vilken är Internet standard RFC 1321. Några minuter senare lägger jag till denna rad i uppsatsen och samma algoritm, MD5, resulterar i en helt annan hashsumma: 291e0713c28d20a4dbaec3de8486a8b9 Programmet som genererat dessa summor har en funktion för att jämföra hashsummor och talar om att summorna inte matchar, det är alltså inte längre samma information i filen. Det finns en mängd olika algoritmer för kryptering. Bitcoin använder till exempel algoritmen secp256k1. Andra algoritmer resulterar i hashsummor med annat antal tecken, vissa algoritmer ger flera hundra tecken långa hashsummor, vilket gör att det är viktigt att veta vilken algoritm som använts. Detta kan dock räknas ut från hashsummans teckenantal. Programmet som användes för att skapa hashsummorna ovan hämtades från sidan http://www.winmd5.com/ den 23 november 2017.

Kvantdator

En kvantdator skiljer sig från traditionella datorer genom att den består av qbits istället för vanliga bits. En bit i en traditionell dator är antingen 1 eller 0. En qbit kan däremot vara både 1 och 0 samtidigt. Två vanliga bit kan således representera antingen 10 eller 01. Två qbit kan däremot representera fyra tal: 10, 01, 11,00. Detta leder till en betydligt snabbare dator vilken på kort tid, enstaka sekunder, kan utföra beräkningar som med traditionella datorer skulle kunna ta flera dagar eller till och med månader (Marjomaa 2017).

Nod

En nod är en knutpunkt i ett nätverk. En nod kan vara en enhet som tar emot och skickar information, ofta där en förbindelse delar sig och fördelar information åt flera håll. En nod kan även bestå av de apparater som knyts ihop av ett nätverk (Nod 2017).

Record

I denna undersökning används begreppet ”record” i samma betydelse som ordet har på engelska. I Riksarkivets projekt e-arkiv och e-diariums, eARD, begreppslista definieras

record: ”*Information som skapas, tas emot och underhålls som bevis och/eller tillgång av en organisation eller person för att uppfylla legala förpliktelser eller utföra transaktioner i sin verksamhet, oavsett medium eller format.*” (eARD 2013, Riksarkivet uå). ISO 15489 definierar record enligt följande: “*information created, received, and maintained as evidence and information by an organizaton or person, in pursuance of legal obligations or in the transaction of business*” (Lemieux 2016b s 2). Enligt de ovan refererade definitionerna är alltså ett record information som är under någon form av behandling och kan användas för att bevisa något.

Mer specifik definition för ett Digitalt record återfinns i Interpares 2 Project Dictionary under begreppet Digital Record (2017):

> “n., A digital document that is treated and managed as a record. [Archives]
>
> n., A record whose content and form are encoded using discrete numeric values (such as the binary values 0 and 1) rather than a continuous spectrum of values (such as those generated by an analogue system).
>
> n., A record that has been captured and fixed for storage and manipulation in a computer system and that requires the use of the system to be intelligible by a person.”

2 Det teoretiska ramverket

Det teoretiska ramverket byggs upp genom diskussioner av fundamentala begrepp för upprätthållande av trovärdighet, autenticitet och äkthet hos information. Proveniens och integritet är de begrepp som är viktigast att uppfylla för att information ska bibehålla sitt värde och autenticitet är i sin tur fundamentalt för att upprätthålla integritet. Trovärdighet inbegriper förutom informationens integritet även att den är pålitlig i betydelsen att den är sann vid tillfället den dokumenteras.

2.1 Proveniens

Uppgifter om proveniens är fundamentalt för upprätthållande av bevisvärde hos information (Factor m.fl. 2009). Proveniens är kännedom om vem som är upphovsman, tidigare ägare samt förvaringsplatser med mera för ett dokument, bok, record eller liknande. Provenienssprincipen som har sitt ursprung i respect des fonds betyder att records med olika ursprung ska behållas i sin ursprungliga kontext och inte blandas med records från andra ursprung eller processer (provenance 2017).

2.2 Integritetsprincipen (Principle of Integrity)

Till grund för diskussionen ligger Association of Records Managers & Administrators, ARMA, Principle of Integrity som går ut på att ett informationshanteringsprogram som används för att skapa och hantera records och annan information ska kunna garantera autenticitet och trovärdighet. Principle of Integrity är en av ARMAs Generally Accepted Recordkeeping Principles, GARP, vilka är åtta formulerade grundprinciper kring hantering av records. Utöver Principle of Integrity benämns de övriga principerna: Accountability, Transparency, Protection, Compilance, Availability, Retention och Disposition. Principerna går ut på att belysa vikten av att det finns möjligheter att spåra och bekräfta autenticitet hos information och därigenom upprätthållen integritet. Principerna beskriver även vikten av säker förvaring av information i kombination med sökbarhet och åtkomlighet (GARP 2017). Det är Principel of Integrity som kommer att användas i den här uppsatsen eftersom att begreppet integritet per definition ställer krav kring autenticitet, trovärdighet och proveniens, precis de förutsättningar som avgör värdet hos information.

Enligt Principle of Integrity är en organisations ledning direkt ansvarig för informationens integritet, alltså att informationen kan visas vara autentisk och omanipulerad för att inte förlora sitt bevisvärde. För att leva upp till det så krävs att organisationer formulerar dokumenthanteringsplaner som bidrar till att upprätthålla bevisvärdet hos information som skapas och bearbetas. Även krav kring kompetens hos de som arbetar med informationen och ett livscykeltänkande kring informationen finns formulerade, liksom möjligheten att kontrollera informationens autenticitet (Principle of Integrity 2017).

2.3 Autenticitet

Autenticitet är synonymt med begrepp som äkthet och tillförlitlighet. Autenticitet för en digital handling betyder att handlingen verkligen är vad det utger sig för att vara, handlingen har skapats eller skickats av den person som uppges ha skapat eller skickat den, samt handlingen har skapats eller skickats vid den tidpunkt som uppges. Autenticitet betyder att ifrågasättande av handlingen ska vara möjligt att pröva (Hänström 2007).

2.3 Trovärdighet

Trovärdighet handlar om att man agerar utan att själv ha de kunskaper som krävs för att agera rationellt. I fall med digital information så sätts vanligen högre tilltro till information som

formulerats eller skrivits under av någon med för ämnet lämplig akademisk titel än information utan författare (Duranti & Rogers 2012). Ett annat exempel på trovärdighet hos information är om man går in i en hiss där en skylt talar om hissens maximala lastvikt. Normalt litar man på att hissen kommer klara av att åka trots den extra vikt man själv utgör utan att själv göra några kontrollerande tester. Man sätter stor tilltro till att informationen på skylten är korrekt, i många fall även att informationen är aningen försiktig kring formulering av max vikt och antal passagerare. Trovärdighet består av de två delarna; pålitlighet och autenticitet (reliability and authenticity) tillsammans med närliggande begrepp som identitet, integritet och proveniens (Lemieux 2016).

Duranti & Rogers (2012) identifierar ett antal problem kring hur trovärdighet upprätthålls för information i molntjänster och vad som måste beaktas innan information delas eller lagras i molntjänster av olika slag. Både juridiska frågor och hur åtkomst ska kunna säkras även om de som ligger bakom tjänsten av olika skäl försvinner eller säkerhetslösningar förändras. Även om både de juridiska aspekterna och åtkomstmöjligheter säkras krävs även garantier för att information inte ska kunna ha förvanskats.

2.4 Informationssäkerhet

Även om Ada, Gupta och Sherman (2009) sammanställde lämpliga teorier för användande vid olika typer av undersökningar inom informationssäkerhetsområdet; Social Technical Systems theory, Activity theory, Distributed Cognitive theory, Grounded theory, Generated Deterrence theory, Social Cognitive theory så menar Duranti (2009) att utvecklande och tillämpning av lämpliga teorier för informationssäkerhetsområdet fortfarande behöver tid för att etableras. John (2012) diskuterar övergången från att digital information lagras på fasta enheter som hårddiskar, disketter, USB-minnen och liknande till att allt mer information både skapas, bearbetas och lagras i molntjänster och vilken påverkan på kunskap och kompetens det får bland de som arbetar med arkivmaterial och samlingar vid stora insamlande institutioner som arkiv, bibliotek och vissa museer.

Mattila m.fl (2016) jämför säkerheten hos plattformar som kontrolleras av enskilda (individual platforms) respektive delade (shared platforms) i samband med gemensam produktutveckling. De lyfter fram risken att om en enskild deltagare kontrollerar molnplattformen så kan den stängas av eller manipuleras och göra informationen oåtkomlig

för övriga deltagare. Samtidigt är det svårt att kontrollera att information inte blivit manipulerad eller raderad när den ligger i en molnbaserad plattform (Chung m.fl. 2017).

3 Tidigare forskning

Att säkerställa autenticitet hos digital information blir en allt större del av arkivariens arbete. De utmaningar detta medför gör det viktigt att följa med i diskussioner och utveckling av både metoder och tekniska lösningar för bevarande och upprätthållande av autenticitet och trovärdighet. Utmaningar kring att upprätthålla trovärdighet hos digital information diskuteras av bland andra Duranti och Rogers (2012). I artikeln *Trust in digital records: An increasingly cloudy legal area* från 2012 ställer Duranti och Rogers upp en rad frågor och utmaningar kring vad som måste beaktas för att trovärdighet och åtkomstsäkerhet hos digital information ska kunna upprätthållas. De oklarheter som formuleras handlar om juridisk osäkerhet när information lagras på eller kontrolleras av servrar i olika länder. Det kan vara svårt för enskilda användare att ta reda på var informationen fysiskt finns lagrad. Kan sekretess av något som helst slag anses vara upprätthållen när information görs tillgänglig på servrar eller i molntjänster som ägs och underhålls av tredje part? Vilka garantier ger molntjänstadministratörer kring informationens säkerhet, både under pågående avtalstid men även efter en eventuell konkurs eller uppköp av aktören? Duranti och Rogers avslutar artikeln med att poängtera vikten av att ställa hårda frågor kring upprätthållandet av autenticitet och trovärdighet hos digitala dokumenthanterings- och lagringssystem.

Upprätthållande av autenticitet hos digital information diskuteras ingående i de olika InterPARES projekten som pågått sedan 1998 (InterPARES uå). Nationellt har säkerhet kring digital information diskuterats mer ingående sedan 1990-talet (Hänström 2007). Ännu tidigare, i slutet av 1980-talet, diskuterades inom Pittsburghprojektet frågor kring långtidslagring av digital information vilken skapas eller används överförd i nätverk mellan datorer (Bearman 1994; School of Information Sciences 2002).

När det gäller publicerad forskning kring blockkedjeteknologi så är det användandet för att säkra transaktioner hos kryptovalutor, främst Bitcoin, som är den vanligaste utgångspunkten för diskussionerna. Blockkedjeteknologin presenteras av Nakamoto 2008 i artikeln *Bitcoin: A Peer-to-Peer Electronic Cash System* och där beskrivs hur blockkedjeteknologin fungerar. Teknologin har uppmärksammats från andra håll än finanssektorn och bland annat pågår i

flera länder projekt kring att använda teknologin vid framförallt land- och fastighetsöverlåtelser (Lantmäteriet 2016, Collindres 2016, Smerkis 2017). Forskning kring blockkedjeteknologin i arkivvetenskapliga samanhang har gjorts av framförallt Hrvoje Stancic inom ramen för InterPARES Trust projekt TRUSTER, vilket är ett forskningsprojekt inom arkivvetenskap och långtidsbevarande (Bralić m.fl. 2017).

I artikeln *Trusting records: is Blockchain technology the answer?* vilken publicerades 2016 beskriver Victoria Lemieux potentialen att upprätthålla autenticitet och trovärdighet hos digitala records. Artikeln innehåller en fallstudie kring ett projekt om fastighetstransaktioner för vilket Lemieux går igenom riskfaktorer och vilka internationella standarder som är applicerbara på de olika momenten i skapandet av en blockkedja eller vid användande av befintlig blockkedja för nya områden. Slutsatsen i artikeln är att blockkedjeteknologi har potential att komma till stor nytta för att upprätthålla autenticitet hos digital information (Lemieux 2016a).

Mattila m.fl. (2016) lägger i artikeln *Product- centric Information Management A Case Study of a Shared Platform with Blockchain Technology* fram ett förslag som bygger på teknologin på en plattform för informationshantering vid produktutveckling där flera parter är inblandade. Området lider av trovärdighetsproblem kopplat till hantering av digital information och blockkedjeteknologi skulle göra hanteringen mer transparent, spår- och verifierbar. Artikeln behandlar både litteratur och en fallstudie från vilken slutsatsen är att kunskap om blockkedjeteknologi och de potentiella lösningar kring informationshantering vid produktutveckling som teknologin utgör är viktig.

En begränsning i teknologin är att det har varit svårt att få olika blockkedjor att interagera med varandra och att det i efterhand är svårt att förändra upplägg av kedjan, något som lyfts fram som orsak till att många projekt avstannat eller lagts ner (Illgner 2017). Därför har till exempel Back m.fl (2014) arbetat med att ta fram en lösning för vilken är en variant av sammankopplande blockkejor som kan koppla ihop block från olika blockkedjor och därmed göra dem mer flexibla. Forskning kring hur blockkedjor skulle kunna hackas och hur kraftfull hårdvara som skulle behövas har diskuterats av bland andra Aggarwal m.fl. (2017) och Bernstein m.fl. (2017) vilka båda ser utvecklingen av kvantdatorer som potentiellt hot mot dagens blockkedjor. De drar samtidigt slutsatsen att nya typer av krypteringar kommer tas fram och ligga till grund för nya blockkedjor vilka därmed kommer vara skyddade mot attacker från kraftfullare datorer än som finns tillgängligt idag.

Våren 2017 skrevs ett examensarbete vid Handelshögskolan av Ulrika Byström och Diana Lundkvist med titeln ”Blockkedjan – En riskreducerare?” En undersökning av blockkedjans effekt på risk inom revisions, finans - och fastighetsbranschen vilket kommer fram till att det finns stora möjligheter för blockkedjetekniken att lösa delar av den osäkerhet som finns inom revisions, finans och fastighetsbranschen vilket är det område undersökningen avgränsas till. Författarna beskriver tekniken i mycket positiva ordalag och kallar den revolutionerande med potential att förändra stora delar av hur finans och fastighetsbranschen fungerar (Byström & Lundkvist 2017).

4 Undersökning

Inom området dokument och arkivhantering har framförallt Victoria Lemieux (2016) och Hrvoje Stančić (2017) skrivit om blockkedjeteknologins potential utifrån olika typer av fallstudier där teknologins potential kopplas till att säkra autenticitet hos digital information. Nedan följer en litteraturstudie av hur de och andra behandlat frågor rörande autenticitet och digital information i olika sammanhang.

4.1 Autenticitet i digital dokument och arkivhantering

I Sverige har upprätthållande av autenticitet hos digital information diskuterats i närmare 25 år och Riksarkivet har tagit emot elektronisk information i olika former i över 40 år. Dessa handlingar är till största delen allmänna vilket medför att de ska bevaras för framtiden av både juridiska skäl och att finnas tillgängliga för forskare (Hänström 2007).

Upprätthållande av autenticitet diskuteras ingående i de olika InterPARES projekten och i InterPARES 1 (2001) definierade autenticitet och autentisk enligt följande:

> “In common usage, the concept of authenticity is defined as “the quality of being authentic, or entitled to acceptance.” 1 The term authentic means “worthy of acceptance or belief as conforming to or based on fact” and is synonymous with the terms genuine and bona fide. Genuine “implies actual character not counterfeited, imitated, or adulterated [and] connotes definite origin from a source.” Bona fide “implies good faith and sincerity of intention.” 2 From these definitions it follows that an authentic record is a record that is what it purports to be and is free from tampering or corruption. “

InterPARES förtydligar skillnaden mellan autenticitet och autentisk och att begreppen kan betyda olika saker beroende på hur de används. Autenticitet hos digitala handlingar betyder att handlingen inte förvanskats eller hamnat i fel samanhang. Autenticitet i detta samanhang betyder således inte att den information som finns lagrad är sann eller en korrekt beskrivning.

InterPARES 1 pågick mellan 1998-2001 och byggde på det tidigare forskningsprojektet The Preservation of the Integrity of Electronic Records. Projektet undersökte förutsättningar kring bevarande av autenticitet hos digitala records vilka inte längre behövdes i den verksamhet de bildats (InterPARES 1 2001). Projektet genomfördes av forskargrupper med olika inriktningar och det som undersökte autenticitet hos digitala records, Authenticity Task Force, genomförde en deduktiv teoretisk studie för att identifiera elektroniska records olika byggstenar och hur de relaterar till informationens autenticitet.

4.2 Diplomatik

Diplomatik handlar om att belägga autenticitet hos dokumenterad information. Disciplinen lanserades under 1680-talet efter de så kallade `diplomatiska krigen` vilka handlade om diskussioner kring autenticitet och värdet i information hos äldre, främst medeltida, dokument. Diplomatik utvecklades så småningom till en egen vetenskap (Duranti 1989). Metodiken gick från början ut på att studera dokuments yttre och inre beståndsdelar som papper, bläck, sigill, det språkliga uttrycket med mera för att fastställa bevisvärdet hos medeltida rättsgrundande dokument som kyrko- och klosterprivilegier (Fritz 2017). Den moderna användningen av disciplinen diplomatik formuleras kring 1989-1992 i sex artiklar av av Luciana Duranti vid University of British Columbia och bygger på de grunder för diplomatik som lades fram i slutet av 1600-talet. För InterPARES 1 byggde det teoretiska perspektivet Archival diplomatics på Durantis artiklar.

Duranti visar i artiklarna hur diplomatik kan användas för att beskriva processer hos organisationer och hur de utfört sin verksamhet (Duranti 1998). Archival diplomatics kombinerar arkivteori med diplomatik kring skapande av information, inre organisatoriska strukturer, och användande i relation till faktiskt innehåll och andra dokument inom samma område (Duranti 2013). Kombinatinen av arkivvetenskapligt tänkande och diplomatisk metodik gör att även teorier kring till exempel record management kan likställas med eller underordnas archival diplomatics (Duranti 2010b). Den moderna användningen har anpassats till att istället för att bedöma till exempel papper, bläck och sigill handla om identifierbara delar och byggstenar i digitala filer. Digitala records består av ett antal delelement vilka relaterar till varandra genom komplexa mönster. De delar som bygger upp ett digitalt record faller in i fyra olika kategorier; Documentary Form, Annotations, Context och Medium (InterPARES 2001).

Duranti beskriver två grenar av diplomatik; General diplomatics som rör skapande, utformning och hantering av information medan Special diplomatics behandlar enskilda dokument och hur man utifrån information i dem kan dra slutsatser och ge kunskap om utfärdarens verksamhet. Av dessa så har General diplomatics lyfts fram som den mer användbara varianten när det gäller moderna förhållanden och att den information som tas fram med special diplomatics även finns åtkomlig genom andra vägar samtidigt som den metoden kan vara mer tidskrävande (Storch 1998). Utvecklingen mot hur information skapas och bearbetas idag har dock gjort special diplomatics mer aktuellt för att placera in lösryckt digital information i sammanhang vilket ledde till formulerandet av archival diplomatics. Inom InterPARES 1 skapades mallar för tillvägagångssätt vid användande av diplomatik vilka utprovades genom fallstudier (InterPARES 1 2001).

På samma vis som den tidiga diplomatiken tog hjälp av och i sin tur inspirerade andra historiska vetenskaper som filigranologi, paleografi, heraldik och sfragistik så interagerar dagens digitala diplomatik med närliggande grenar av andra vetenskaper som till exempel forensik och systemvetenskap (Fritz 2017, Duranti 2010). Inom diplomatik angrips ett dokument på olika vis. Yttre faktorer som kan hjälpa till att datera eller på annat vis indikera ursprung handlar om format, studier av själva skriften och vilken typ av besegling som använts (Fritz 2017). Dessa metoder överförs när det gäller digital information till att studera mediet informationen ligger på, typsnitt, upplösning och liknande samt hur eventuella signaturer eller krypteringar utförts. Information som ligger på en floppydiskett och består av obsoleta filformat kan misstänkas vara från 1980- början av 1990-talet medan ett modernt filformat som ligger lagrat i en molntjänst kan misstänkas vara relativt ny. Detta kan dock inte avgöras med säkerhet då det alltid går att skapa och lagra digital information på äldre media och format liksom äldre records kan migreras till nyare format. För att säkerställa ursprung och autenticitet hos digital information som inkommer till en arkivinstitution eller är tänkt att användas som bevis i något sammanhang kan olika typer av forensiska undersökningar krävas. IT forensik och närliggande undersökningsmetoder anammar mycket av diplomatikens metoder men kan vara resurskrävande både vad gäller kompetens och ekonomi då det ofta krävas både speciell hårdvara och inköp av mjukvara med tillhörande licenskostnader (Kirshenbaum m.fl. 2010 s 80-82). För att underlätta och minska risken för informationsförvanskning och dyrbara undersökningskostnader diskuteras nu blockkedjeteknologins möjligheter. Precis som Diplomatik användes menar de olika forskare

som ägnat sig åt ämnet att blockkedjeteknologin har potential att kunna hjälpa organisationer att lösa autenticitetsfrågor.

4.3 Hur blockkedjeteknologi fungerar

Grundläggande för att blockkedjor fungerar är möjligheten att kryptera information. Kryptering av information görs i många sammanhang och fungerar genom att en algoritm skapar en hashfunktion som tar slumpmässig data och omvandlar till en hashsumma. Hashsumman kan liknas vid ett fingeravtryck för just den datan. Fingeravtrycket är litet i förhållande till den mängd information det identifierar. Hashsumman är jämförbar med ett fingeravtryck, ett litet mönster som kan identifiera en person. Samma data ger alltså alltid upphov till en likadan hashsumma precis som en persons fingeravtryck alltid ser likadant ut. Får man däremot bara tillgång till fingeravtrycket går det inte att ta reda på vilken data den motsvarar om man inte har tillgång till en hashnyckel, eller en motsvarighet till fingeravtrycksregister (Wint 2015).

Blockkedjor kan se aningen olika ut, men består av tre huvuddelar: En transaktion som noteras och dokumenteras, transaktionens bekräftande samt införandet i en öppen liggare. För transaktioner som till exempel överföring av valuta är det första steget att skapa ett nytt block vilket sker genom att noder kopplar ihop sig med andra noder från tidigare transaktioner. Blocket krypteras och får en hashsumma, ett digitalt fingeravtryck. Hashsumman står tillsammans med eventuell övrig information i blockets ”header”, eller blockhuvudet. Det är blockhuvudet som är beviset för transaktionen och när den bekräftas av ytterligare noder uppdateras blockkedjan med en ny hashsumma för hela blockhuvudet (Lemieux 2016a). I fallet med Bitcoin så bekräftas transaktioner genom att de tidsstämplas. Även tidsstämplingen sker med noder utspridda bland blockkedjans deltagare. Tidsstämpeln krypteras till en hashsumma vilket bekräftar att transaktionen skett före en viss tidpunkt vilket förhindrar risken för till exempel dubbla överföringar. Noderna som utför tidsstämpeln kan göra det vid olika tidpunkt vilket ger en kedja av hashsummor vilka innehåller krypterade varianter av tidigare tidsstämplar (Nakamoto 2009).

Den öppna liggare som används av Bitcoins blockkedja fungerar på så vis att de noder som används avläser tidigare krypteringar och bara accepterar block som består av godkända transaktioner. Noderna godkänner ett block genom att börja bygga upp nästa vilket sker genom att de börjar med att använda tidigare blocks hash. Noderna är anonyma och kan

lämna eller komma in i processen när som helst eftersom de hela tiden kontrollerar och bekräftar bakåt i kedjan. Skulle något inte vara korrekt så vägrar noden fortsätta arbetet med det nya blocket (Nakamoto 2009). Det är slumpmässigheten i det gitter av ingående noder och den algoritm som används för kryptering som bildar blockkedjans signaturschema. I fallet med Bitcoin är det algoritmen secp256k1 vilken resulterar i en hashsumma som består av 256 bit som används (Lemieux 2016a).

4.4 Verksamheter och Projekt som använder blockkedjeteknologi idag

Det pågår ett stort antal verksamheter och projekt runt om i världen där blockkedjeteknologi används och testas för olika ändamål. I december 2017 gjordes en genomgång där ett hundratal företag som arbetade på olika vis med blockkedjeteknologi inom ett 30-tal olika branscher identifierades (Mesropyan 2017). För att ge en bild av läget kring vilka typer av verksamheter som anammat teknologin och kommit längst i utvecklingen av projekt och skarpa applikationer redogörs här kortfattat för några av dessa.

Satoshi Nakamoto är det namn som används av den eller de personer som lanserade blockkedjetekniken i samband med skapandet av kryptovalutan Bitcoin. Under namnet ”Satoshi Nakamoto” publicerades 2008 ett dokument som beskrev blockkedjeteknologin i samband med lanserandet av kryptovalutan Bitcoin (Nakamoto 2008). Liknande upplägg hade dock lanserats tidigare. 1990 lanserade Chaum m.fl. en elektronisk valuta som byggde på kryptering. I slutet av 1990-talet lanserade Szabo ”bit-gold” som byggde på länkning av krypteringar på ett vis som påminner om blockkedjetekniken och deltagarna tävlade om att lösa proof of work-funktioner med ett distribuerat äganderegister (Bitcoin 2017). Det var dock med Nakamotos publicerade artikel 2008 som blockkedjeteknologin lanserades i den form den har idag.

Flera projekt där blockkedjor är en fundamental del handlar om registrering av mark och fastighetsägande. Tidigast ut med ett fungerande system var Georgien där idag flera hundratusen transaktioner har registrerats i samma blockkedja som ligger till grund för kryptovalutan Bitcoin. Även andra före detta Sovjetrepubliker som till exempel Ukraina undersöker möjligheten till ett liknande system i samarbete med företaget BitFury som också låg bakom projektet i Georgien. Som skäl till intresset för tekniken hos före detta Sovjetstater och även andra politiskt instabila nationer nämns korruption som risk för förvanskning av ägandedokumentation och oroligheter vilka riskerarar att fysiskt förstöra register bundna till

papper eller fast hårdvara (Ryder 2017; Smerkis 2017). Liknande resonemang ligger bakom det projekt som håller på att utveckla ett system för fastighetstransaktioner i Honduras (Collindres 2016).

Telecomföretaget Ericsson har lanserat en tjänst som säkrar integriteten hos information baserad på blockkedjeteknologi. Ericssons tjänst Blockchain Data Integrity är utvecklad för att säkerställa att information som hanteras i molntjänster och Internet of Things, IoT, inte ska gå att manipulera. Ericsson motiverar sin satsning på säkerhetstjänster för digital information med att det sker en förändring i attityd inom säkerhetstänkandet. Istället för att fokus som tidigare legat på att hindra obehörig åtkomst av information fokuseras nu mer på att hindra möjligheter till manipulation (Data Centric Security 2017).

Inom affärsvärlden så är projektet Hyperledger som initierats av Linux Foundation drivande kring användande av blockkedjeteknologi för säkra och effektiva transaktioner av olika slag (Hyperledger 2016). Everledger är ett brittiskt företag som har som affärsidé att genom att dokumentera värdefulla föremål, i deras fall till största delen diamanter, och använda block-kedjeteknologi för att säkra proveniens och ägande i syfte att försvåra försäljning av stöldgods (Everledger 2017). Diamanter är även fokus för DeBeers satsning på blockkedjeteknologi för att säkra proveniensen för sina produkter (Cleaver 2017). Företaget RSK lanserade i december 2017 planerna på en tjänst för smarta kontrakt som bygger på samma blockkedja som används för Bitcoin med det uttalade syftet att utveckla ekosystemet kring Bitcoin (RSK 2017). Ett exempel på hur en ny verksamhet kan kopplas till en redan befintlig blockkedja utan att påverka den.

Flera större projekt kring applikationer av blockkedjeteknologi pågår runt om i världen. I Kanada planeras digitala identitetslösningar baserade på blockkedjeteknologi (Alexander 2017). Dataföretaget IBM tillkännagav i augusti 2017 att de tillsammans med ett antal större amerikanska livsmedelsproducenter och försäljare startat ett projekt för att med hjälp av blockkedjeteknologi säkra dokumentation kring produktions- och försäljningsled för livsmedel. Det projektet är en påbyggnad och utveckling av ett lyckat pilotprojekt där IBM tillsammans med Wallmart använt blockkedjor för att spåra mango i USA och fläsk i Kina (IBM 2017). Även i Sverige finns ett liknande projekt kring spårbarhet hos livsmedel där bland andra Axfoundation, SKL Kommentus och Kairos Future är inblandade (Kairos Future 2017b). I november 2017 gjorde NASDAQ en pressrelease där man tillkännagav att man höll

på att leverera ett elektroniskt röstningssystem byggt på blockkedjeteknologi till börsen i Sydafrika (NASDAQ 2017).

4.5 Blockedjeteknologi inom dokument och arkivhantering

Sedan ett par år har det publicerats artiklar kring blockkedjeteknologins potential inom det arkivvetenskapliga området men den största delen av vad som publiceras är kopplat till kryptovalutor, oftast med Bitcoin som utgångs-punkt. Att en majoritet av det som skrivs om blockkedjor handlar om kryptovalutor förklaras med att det var med Bitcoin som blockkedjeteknologin lanserades och det tog tid innan andra discipliner började undersöka teknologins potential. Den första större undersökning jag hittat kring hur blockkedjeteknologi skulle kunna hjälpa till att upprätthålla trovärdighet hos digitala records är Victoria Lemieuxs *Trusting Records: Is Blockchain Technology the Answer?* från 2016. I artikeln appliceras flera standarder inom records management och digitalt bevarande, främst Association of Records Managers & Administrators, ARMA, Generally Accepted Recordkeeping Principles, GARP, ISO 15,489, ISO 14,721 och ISO 16,363. Tillsammans med en fallstudie handlar undersökningen om registrering av markägande och fastighetstransaktioner i Honduras. Resultaten pekar mot att blockkedjeteknologi kan användas för att leva upp till de standarder som finns formulerade inom området idag av ISO och ARMA och således att teknologin kan användas för att upprätthålla integritet hos records (Lemieux 2016a).

Bralić, Kuleš, Stančić, (2017) lanserar i sin artikel *A Model for Long-term Preservation of Digital Signature Validity: TrustChain* ett förslag kring hur blockkedjeteknologi kan användas för att säkra digitala signaturer över lång tid. Artikeln tar upp och diskuterar problematiken kring dagens digitala signaturer vilka visserligen i korttidsperspektiv är säkra och enkla att använda men när de går ut lämnar informationen öppen för manipulation. Mattila, Seppelä och Holmström (2016) lägger i artikeln *Product- centric Information Management: A Case Study of a Shared Platform with Blockchain Technology* fram idéer kring hur blockkedjeteknologin kan användas för att upprätthålla trovärdighet i digital information som skickas mellan organisationer och användare. Deras undersökning går ut på att hitta applikationer för teknologin som förenklar samarbete vid produktutveckling där information behöver vara säker mot förvanskning samtidigt som det kan finnas juridiska skäl att dokumentera vem som gjort vad och när. Författarna ser stor potential med teknologin vilken kan komma att ligga till grund för informationsutbyte och säker dokumentation inom

många olika områden. I artikeln lyfts även fram frågor kring hur information som ägs av någon enskild deltagare ska behandlas och problem med interaktion mellan olika blockkedjor.

4.5.1 Hot mot blockkedjeteknologi

När det gäller potentiella hot mot blockkedjeteknologi i form av medvetna försök att manipulera dem så anses det idag inte finnas någon teknik som kan klara av det. Nakamoto (2009) beskriver att eftersom blockkedjan har en kronologisk historik som kontrolleras av distribuerade anonyma noder vilka inte bygger vidare på icke verifierade block så minimieras risken för både medveten manipulation och att till exempel dubbla transaktioner kan ske av misstag. För att manipulera ett block krävs att man kan kontrollera en större mängd noder än hela övriga systemet har tillgång till, något som inte anses gå att göra i en helt distribuerad blockkedja eftersom att det skulle kräva större datakraft än vad som finns tillgängligt idag. En samlad attack av manipulerade noder måste förutom att manipulera informationen i ett block även manipulera alla senare block i blockkedjan för att ärliga noder ska kunna fortsätta bygga kedjan (Lemieux 2016a).

Det förutspås i en artikel av Aggarwal m.fl (2017) att kvantdatorer inom tio år kan komma att klara av att bryta det underliggande signaturschemat för äldre blockkedjor, till exempel det som idag ligger till grund för Bitcoin och bygger på algoritmen secp256k1 vilken börjar bli föråldrad. Författarna menar dock att även om det med hjälp av kvantdatorer kommer kunna gå att hacka den teknik som används idag så är branschen väl medveten om hoten samtidigt som även säkerheten i blockkedjor ökar och nya algoritmer för kryptering ger än mer avancerade nycklar. Författarna förespråkar Momentum, en algoritm framlagd av Larimer (2014) som klarar större attacker mot de hashar som blockkedjetekniken använder för kryptering. Aggarwal m.fl.(2017) påpekar även att framtidens block i blockkedjorna kommer krypteras av kvantdatorer vilket bör göra dem ännu säkrare. Även Bernstein m.fl. (2017) diskuterar kvantdatorers potentiella hot mot kryptering och kommer fram till att dagens blockkedjor riskerar kunna hackas med framtida teknik. De lanserar i artikeln en ny algoritm som är snabbare och upprätthåller säkerheten även mot framtida snabba kvantdatorer samtidigt som även de förordar Momentum.

Lemieux (2016a) poängterar i samband med fallstudien av fastighetsregister i Honduras att det är av avgörande vikt att rätt information från början hamnar i blocken. Detta förutsätter säker och stabil digital infrastruktur. Lemieux (2016a) gör en systematisk listning över ett

antal identifierade brister och potentiella hot utifrån det exempel kring blockkedjeteknologins användande för land och fastighetstransaktioner som planeras i Honduras. De olika hoten mot autenticiteten i blocken ges tre olika grader av sannolikhet: Low, Medium och High med referens till de olika ISO och ARMA standarder som är applicerbara för projektet. Upprätthållande av autenticitet och integritet är huvudsyftet med att använda blockkedjeteknologi och för att detta ska uppfyllas måste det finnas möjlighet att kontrollera när, var, hur och av vem information hamnat i kedjan. Det första hotet som diskuteras handlar om vem som egentligen kontrollerar en blockkedja. I fallet med Bitcoins blockkedja har det förekomit att noder koncentrerats till små grupper av användare när nya block skapats vilket lett till frågor kring hur decentraliserad den blockkedjan egentligen är. Risken att någon skulle kunna ta kontroll över de noder som validerar transaktioner anses som ”Low-medium” (Lemieux 2016a).

Trovärdigheten hos informationen som finns i blocken kan inte påverkas av tekniken utan de som skapar den måste se till att den är korrekt men Lemieux (2016a) klassar risken för att felaktig information låses i block som ”High”. I fallet med fastighetstransaktioner i Honduras poängteras att alla transaktioner och registreringar även måste valideras av den myndighet som har hand om dem men i helt öppna decentraliserade kedjor finns risk för att felaktig information medvetet eller omedvetet läggs i kedjan. Transaktionskedjor som inte börjar i en blockkedja utan har pågått en tid i ett annat system kan bli omöjliga att verifiera i blockkedjan, särskilt om det förekommer tidigare krypteringar vilka inte är kompatibla med de som används i blockkedjan. En förändring av algoritmen för kryptering kan göra verifiering svår eller omöjlig. Desto fler krypteringar som gjorts i en blockkedja desto större blir risken att hashar ”krockar” och därmed blir identiteten inte unik och går därmed inte att validera. För att hashar skulle krocka eller att krypteringen ska kunna hackas anses risken som Low-medium”.

En brist med tekniken är att blockkedjor består av just kedjor vilket gör att det inte på ett enkelt sätt går att interagera mellan olika blockkedjor. Detta uppmärksammades av Amalia Illgner i en artikel i New Scientist i november 2017. Hon pekar på problemet med att det inte går att interagera mellan olika blockkedjor som förklaring till att många projekt inom området misslyckats (Illgner 2017). Ett exempel på problemet är att olika kryptovalutor som alla bygger på blockkedjeteknik inte på ett enkelt sätt kan växlas mot varandra. En lösning på problemet med att blockkedjor inte kunnat interagera med varandra är utvecklandet av

”pegged sidechains” vilka skapar övergångar mellan blockkedjor. Dessa sidokedjor är trots att de skapar interaktion mellan andra kedjor egna enheter och om kryptering skulle bli felaktig eller medvetet manipuleras så kan den inte sprida sig till blockkedjorna (Back m.fl. 2014).

4.5.2 Juridik och blockkedjeteknologi

Terminologi kring blockkedjeteknologi ur juridiska perspektiv diskuteras av Walsh (2017), främst utifrån amerikansk lagstiftning, där det framkommer viss brist på gemensam terminologi och begreppsförvirring till stor del orsakad av teknologins snabba framväxt. På svenska diskuteras blockkedjeteknologi ur ett juridiskt perspektiv av Jennie Gunnarsson (2017) vid Lunds Universitet i *Blockkedjeteknik och avtalsrätt - särskilt om skydd för svagare part vid användning av smarta kontrakt*. Slutsatsen är positiv till att blockkedjetekniken kan komma att bli en viktig del i så kallade smarta kontrakt men poängterar att rättsläget kring avtal som sluts med hjälp av tekniken inte är helt klart. Regelverk och lagstiftning inom olika områden behöver justeras och förtydligas och det behövs även tydligare modeller för användandet innan tekniken kan få stort genomslag (Gunnarsson 2017).

Den juridiska oklarheten kring transaktioner med hjälp av blockkedjor utan ansvarig huvud-organisation gjorde att Electronic Frontier Foundation slutade ta emot donationer i form av Bitcoin 2011 (Cohn 2011), något som senare ändrades igen när regelverk blev tydligare och de tar återigen emot donationer i form av Bitcoin (Electronic Frontier Foundation 2017). Även idag finns oklarheter kring det juridska när det gäller teknologin. För svenska förhållanden menar Gunnarsson (2017) att regelverket måste justeras för att kunna appliceras på avtal som sluts med hjälp av applikationer som bygger på blockkedjeteknologi. I en öppen decentraliserad blockkedja kan det finnas frågetecken kring var avtalet egentligen slutits vilket gör att det finns osäkerhet kring vilken lagstiftning som gäller. Terminologin kring blockkedjor är inte standardiserad vilket gör att det finns en begreppsförvirring. Bristen på internationella definitioner på begrepp och standarder rörande teknologin utgör en risk för de som använder den samtidigt som utvecklingen av blockkedjeteknologin riskerar att hämmas (Walsh 2017).

Lemieux (2016a) ser potential hos blockkedjor att kunna säkra juridiska bevis och lyfter fram det som ett av skälen till intresset från Honduras. Landet har haft stora problem med trovärdigheten i den dokumentation kring landägande som funnits och fler exempel finns där oklarheterna resulterat i allvarliga konsekvenser och långdragna rättsfall. Det är även för att

bevara det juridiska bevisvärdet som blockkedjeteknologi används vid fastighetstransaktioner i Georgien och liknande projekt i andra politiskt instabila länder (Ryder 2017; Smerkis 2017).

4.5.3 Informationsteknik

Inom ämnet informationsteknik skrev Kim Andersson våren 2017 ett arbete där författaren främst diskuterar hur tekniken används av olika kryptovalutor och vilka valutor som riskerar hamna på efterkälke då det finns motstånd mot att använda de utvecklade blockkedjetekniker som finns. Andersson nämner även det potentiella hot mot tekniken som en mer allmän tillgång till kvantdatorer skulle kunna föra med sig (Andersson 2017). Även Wall och Malm (2016) diskuterar hantering av valutor och finansiella instrument ur ett informationstekniskt perspektiv och hur ett decentraliserat system byggt på blockkedjor skulle kunna bli både säkrare och effektivare än system som används idag. En förutsättning är dock att det finns en bred sammarbetsvilja och att teknologin införs gradvis.

4.5.4 Skillnader mellan blockkedjor och traditionella record management system

Blockkedjor skiljer sig på flera vis från andra record management system. Blockkedjor medverkar till en maktförskjutning av dokumenthantering och registerhållning samtidigt som den blir mer decentraliserad. Trovärdigheten garanteras av de som deltar i systemet i stället för av en organisation, det är alltså inte de som skapat informationen som står för upprätthållandet av autenticiteten utan de som på något vis är medlemmar av det system som upprätthåller blockkedjan (Lemieux 2016b).

I en rapport från McKinsey & Company i februari 2017 slås fast att blockkedjeteknologin har potential att både hantera och skydda information och därmed göra effektivitetsvinster jämfört med traditionella system för records management. Rapporten är dock tydlig med att teknologin fortfarande är i utvecklingsstatide och behöver tid att mogna vilket den bäst gör genom att implementeras i fler projekt och utvecklingsarbeten (Cheng m.fl. 2017).

4.6 Blockkedjeteknologi och Långtidsbevarande

Det svenska företaget Enigio erbjuder produkter som e-arkiv och långtidsbevarande av digital information. På sin hemsida skriver de om vikten av att implementera ny teknologi som blockkedjor i dokumenthanteringen för att utveckla e-arkiv och säkra integriteten hos lösningar för långtidsbevarande. Företaget har patenterat för ”time:stamp” en produkt som ger

digitala records en tidsstämpel vilken genom blockkedjeteknologi bevaras och inte går att förvanska.

Det standarder som reglerar långtidsbevarande av digital information är ISO 14721 och ISO 16363 (Lemieux 2016a). För att upprätthålla autenticitet hos digitala certifikat finns standarderna ISO/IEC 18014 och European Telecommunications Standards Institute, ETSI, 319 422 vilka går ut på att information tids stämplas, något som gjorts sedan slutet på 1980-talet. Dokumentationen måste dock ges en ny tidsstämpel med jämna mellanrum. De digitala signaturer som idag används för att signera elektroniska dokument fungerar bra i ett kortare perspektiv. Problem uppstår dock när de olika certifikaten bakom signaturen löper ut eller om företag som står bakom dem går i konkurs eller genomgår större förändringar. Det finns två aspekter på digitala signaturer. Dels upprätthåller de informationens integritet, alltså att informationen är densamma som då den signerades. Den digitala signeringen gör även att det går att se vem som signerat och när, vilket ger informationen värde både juridiskt och som historisk källa. Integriteten kan kontrolleras genom att räkna ut hashsumman för att bekräfta att den digitala filen inte ändrats. Digitala certifikat för signering löper ut efter några år och måste förnyas, dessutom är de beroende av det företag eller organisation som utfärdat dem. Förnyas inte den digitala signaturen så går det inte att bekräfta vem som står bakom informationen eller när den är skapad, vilket leder till förlorat bevisvärde och kan till och med göra information oanvändbar (Bralić m.fl. 2017).

Inom ramen för projektet “Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model)” redogör Bralić m.fl. (2017) i *artikeln A model for long-term preservation of digital signature validity: TrustChain* för en metod de benämner TrustChain, vilken skulle kunna vara en lösning på problemet med certifikat som löper ut men även för andra aspekter på långtidsbevarande. TrustChain är en blockkedja som är tillgänglig och nedladdningsbar för alla som är intresserade, men det är bara TrustChain medlemmar som kan lägga till information i blockkedjan. TRUSTER är i sin tur ett delprojekt inom InterPARES trust. TrustChain är ännu i prototypstadiet, men författarna anser att de kommit tillräckligt långt för att dra slutsatsen att blockkedjeteknologin som ligger till grund för det fungerar och är en lösning på att upprätthålla autenticiteten hos digitala signaturer förutsatt att de inlemmas i systemet innan de digitala certifikaten löpt ut, det går således inte att applicera TrustChain på records med utgångna certifikat (Bralić m.fl. 2017).

5 Svenska blockkedjeprojekt och kunskap bland arkivarierna

Här redovisas inhämtad data från personlig kontakt via epost med personer som på olika vis är eller har varit inblandade i projekt som undersöker blockkedjeteknologins potential och möjligheter. Även enkätundersökningen kring kännedom om blockkedjeteknologi bland arkivarier och närliggande yrkesgrupper beskrivs och redovisas. Redogörelsen är inte komplett vare sig kring de projekt och verksamheter som pågår eller representativ för kunskap om blockkedjeteknologi bland landets alla arkivarier, men ger ändå en bild av hur verksamhet kring blockkedjor ser ut och kännedomen om teknologin bland arkivarier i Sverige.

5.1 Blockkedjeprojekt i Sverige

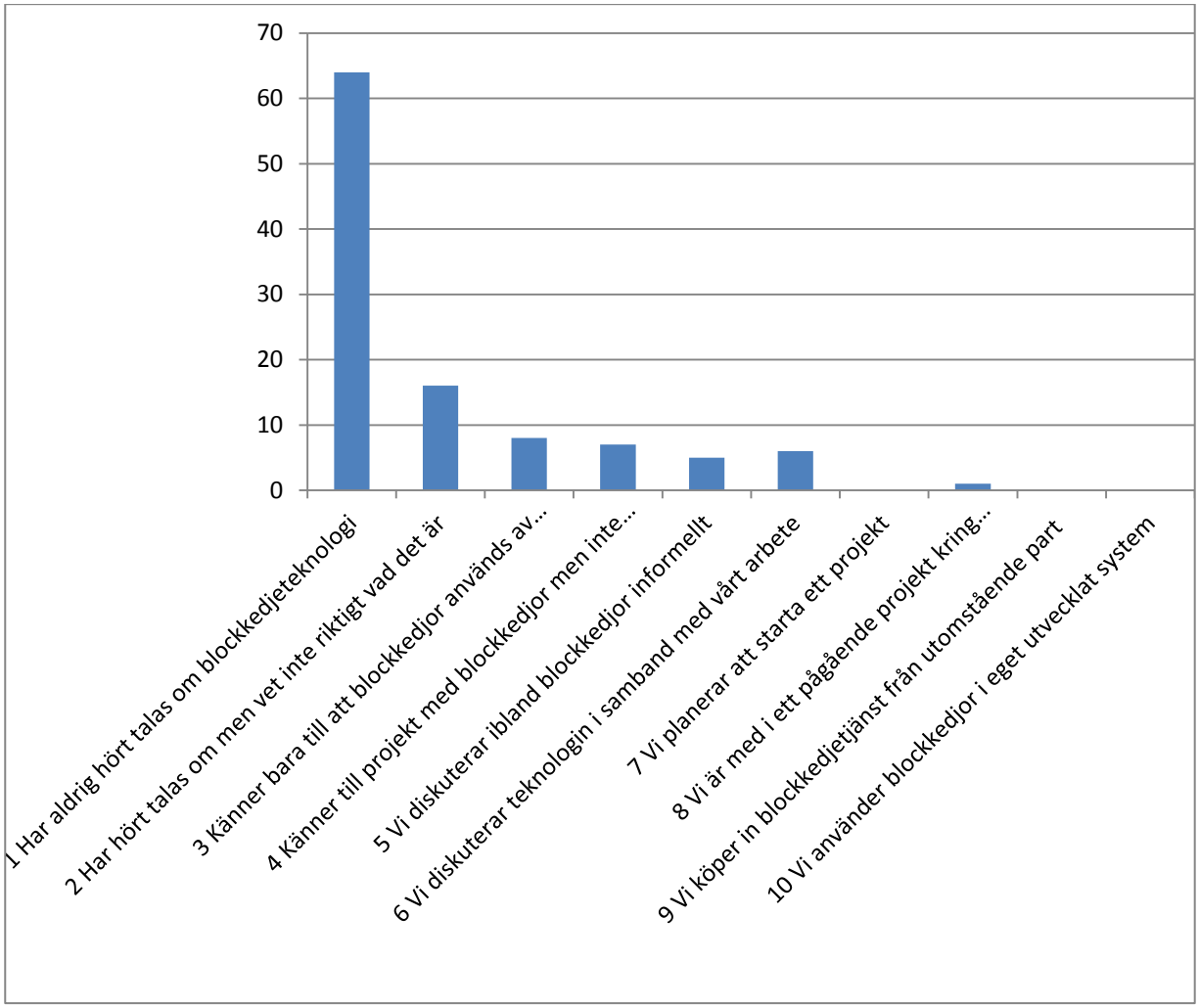
I Sverige är det företaget Enigio som kommit längst i användandet av blockkedjeteknologi i samband med dokument och arkivhantering. Enigio är genom sina grundares engagemang en av huvudaktörerna i InterPARES TRUSTER projekt och en representant för företaget berättar via mail att de är en trolig leverantör av den tekniska lösningen vilken eventuellt kommer bygga helt eller delvis på blockkedjeteknologi. Enigios representant förklarar även att de använder blockkedjeteknologi för att skapa löpande verifieringar med sin tjänst Time:beat vilken bygger på blockkedjeteknologi och är grunden till flera produkter som sparar och validerar till exempel e-post, hemsidor och fotografier. Denna tjänst kan kombineras med företagets e-arkivlösning. E-arkivlösningen i sig bygger i dagsläget inte på blockkedjeteknologi men företaget erbjuder en tjänst som utför löpande verifieringar av e-arkivet vilka sparas i en blockkedja. Företagets blockkedjelösning används även av Syrian Archive, en organisation som arbetar med att dokumentera krigsförbrytelser under kriget i Syrien (Ottsjö 2017).

Det svenska bokföringsföretaget Wint började 2015 utveckla blockkedjor för att kunna garantera att digital bokföring inte ska gå att ändra i efterhand (Wint 2015). Den 27 november 2017 fick jag i kontakt med en utvecklare hos Wint dock höra att projektet ännu inte tagits förbi prototypstadiet. Även i Sverige är fastighetstransaktioner i fokus, bland annat i det projekt kring blockkedjeteknologi som pågår i Lantmäteriets regi men även företaget Enigio vill använda blockkedjeliknande teknologi för upprättandet av löpande skuldebrev. Löpande skuldebrev upprättas i samband med bodstadslån och företagsinteckningar och det finns lagkrav kring att det ska gå att skilja kopia från originalet (Ottsjö 2017). Lantmäteriets projekt kring användande av blockkedjor vid fastighetstransaktioner har pågått sedan 2016 men i

skrivande stund så har ännu inga skarpa applikationer utvecklats. Projektet är ännu i utvecklingsstadiet och den avslutande fasen uppges via email med Lantmäteriets digitaliseringschef den 27/11 2017 samt grundaren och VDn för konsultbolaget Kairos Future 22/11-2017 avslutas våren 2018. Konsultbolaget Kairos Future ligger även bakom initierandet av ett pågående projekt tillsammans med SKL Kommentus, Axfoundation och Martin & Servera kring att med hjälp av blockkedjeteknologi kunna dokumentera produktionsförhållanden för livsmedel och vägen från produktion till konsument (Kairos Future 2017b).

5.2 Kunskap Bland Arkivarierna

För att få en bild av hur utbredd kunskapen om blockkedjeteknologi och dess potential är bland arkivarier och närliggande yrkesgrupper i Sverige genomfördes en enkätundersökning. Resultatet av enkäten redovisas här nedan:



Resultat från enkätundersökning i Facebookgruppen Arkivarier i Sverige utförd i november 2017. Y-axeln visar procent och X-axeln de olika svarsalternativen. Totalt svarade 107 personer.

Undersökningen visar att en majoritet av de svarande aldrig hört talas om blockkedjor, 64 av 107 personer valde alternativ nummer ett: ”Har aldrig hört talas om blockkedjeteknologi”. 16 personer angav alternativ två, att de hört talas om men inte vet vad blockkedjor är. Ytterligare 15 personer valde något av alternativ 3 och 4, att de hört talas om blockkedjor i samband med kryptovalutor eller andra projekt men inte reflekterat över användning för egen del. Elva personer uppgav alternativ 5 eller 6, att de ibland diskuterar blockkedjor informellt eller i samband med arbetet. En svarande angav alternativ 8, att de är med i ett pågående

projekt kring blockkedjeteknologi. Undersökningen omfattar ett begränsat antal svaranden och urvalet av svaranden är inte helt kontrollerbart men efter att ha kontrollerat svarandes profiler på Facebook visade sig den absoluta majoriteten kunna bekräftas vara yrkesversamma inom arkivområdet.

Undersökningens resultat indikerar att blockkedjeteknologi i stort sett inte alls är något som diskuteras eller planeras för bland arkivarier i Sverige. Den enda svarande som valt alternativ 8, vi är med i ett pågående projekt kring blockkedjeteknologi, arbetar på Lantmäteriet.

6 Diskussion

ARMAs Principle of Integrity ställer krav kring autenticitet och trovärdighet och att det ska vara möjligt att bekräfta proveniensen hos information. Ett records integritet är kopplat till möjligheten att bevisa dess autenticitet och att det är oförvanskat. Kan detta inte visas är integriteten förlorad. Information ska enligt principen alltså redan när den skapas hanteras på ett vis som garanterar dess integritet över tid. Även långt innan ARMA formulerade sina principer så pågick diskussioner kring hur autenticitet hos digital information skulle kunna upprätthållas. InterPARES och dess föregångare forskningsprojektet The Preservation of the Integrity of Electronic Records samt tidigare projekt som till exempel Pittsburgh projektet formulerade liknande problemställningar vilka fortfarande till stor del saknar lösningar och gemensamma standarder.

Det finns en mängd utmaningar kring att avläsa digital information från olika lagringsmedia och kunna sätta informationen i rätt sammanhang. En av utmaningarna är att kunna verifiera att informationen på olika lagringsmedia är korrekt och inte har förvanskats på något vis, medvetet eller omedvetet. En annan utmaning är att bekräfta sammanhanget, att informationen återfinns i samma kontext den skapats eller använts i. För information som skapats och förvaltats i enlighet med ARMAs Principle of Integrity så undviks dessa problem och skulle informationen dessutom finnas i en verifierbar blockkedja så förenklas avgörandet kring dess autenticitet och därmed bevisvärde avsevärt (Principle of Integrity 2017; Lemieux 2016a).

Att upprätthålla autenticitet hos digitala records kan vara en utmaning och ännu större blir svårigheten om information av någon anledning måste återskapas efter att ha blivit manipulerad eller raderad. Att återge information dess autenticitet och trovärdighet ställer högre krav kring både resurser och kompetens, vilka kan bli både kostsamma och tidskrävande. En metod eller teknologi som förhindrar att information förändras eller raderas utan att det syns genom att förändringar registreras tillsammans med informationen skulle lösa stora delar av den problematik arkivväsendet står inför när det gäller dokument och arkivhantering i digitala miljöer.

För att återskapa information från olika typer av hårdvara finns disciplinen IT-forensik och närliggande metoder vilka används inom både brottsutredningar och för att återskapa och tillgängliggöra material som lämnats till arkivinstitutioner (Kirschenbaum m.fl. 2010). För att

komma åt och återskapa information som skapats, bearbetats och lagrats i molntjänster fungerar inte samma metoder och det är idag väldigt svårt att se om något har raderats eller överskrivits (Chung m.fl. 2017). Detta förhållande har uppmärksammats och diskuteras av flera forskare de senaste tio åren men IT-forensik och närliggande discipliner är kostsamma och kräver både hög kompetens hos utövarna men även tillgång till programvara och i många fall även speciell hårdvara vilket kan vara förenat med stora kostnader för både inköp och användarlicenser (Kirschenbaum m.fl. 2010 s 81-82; John 2012).

Information som raderats från en hårdvara går för det mesta att återskapa. Det kan vara betydligt svårare att återskapa information som skrivits över med ny information. Även om information går att återskapa efter att ha raderats eller överskrivits så återstår problem med att återskapa proveniensen. Information som återskapats på en hårddisk kan härledas till hårddiskens ägare eller den person som haft tillgång till den vid ett visst tillfälle. Betydligt svårare är att se vem som skapat och hanterat information i en större organisation som har en gemensam molnbaserad informationshanteringslösning. För att information ska ha ett bevisvärde, oavsett om den behövt återskapas eller inte, så bör moderna varianter av diplomatik och diplomatiskt tänkande appliceras vid värdering av informationen.

Som lösning på problem kring att säkra autenticitet hos molnbaserad information lanserade telekomföretaget Ericsson tjänster under namnet Data Centric Security. Tjänsterna syftar till att säkra information från förvanskning och är exempel på en förändring i attityd till informationssäkerhet. Från att tidigare haft fokus på att hindra obehörig åtkomst läggs allt mer arbete på att säkra information från medveten eller omedveten förvanskning. Ericssons produkt bygger på blockkedjeteknologi därför att teknologin dokumenterar händelser utan att det går att gå tillbaka och ändra i händelsekedjan (Data Centric Security 2017).

Det finns avgörande skillnader mellan de projekt som undersöker möjligheterna med blockkedjor och det är dels de som handlar om finansiella instrument och valutor respektive de projekt som har ambitionen att använda teknologin för att spara information om fysiska föremål eller aktiviteter. I Sverige kan detta exemplifieras med de pågående projekten kring fastighetstransaktioner vilka har till syfte att säkra en kedja av transaktioner och avtal där flera parter förutom köpare och säljare är inblandade. Denna typ av användning skiljer sig från hur blockkedjeteknologin är tänkt att användas vid dokumentation av produktionsförhållanden för livsmedel och hur livsmedel ska kunna spåras från producent till konsument. En ytterligare något annorlunda variant exemplifieras med företaget Everledger som dokumenterar

ägandehistoriken för diamanter och andra värdefulla och stöldbegärliga föremål, både för att försvåra försäljning av stulna föremål och för att ha ge rätt underlag till försäkringsbolag.

Företag som Enigio och Ericsson har fungerande produkter som bygger på blockkedjeteknologi och används för syften som ligger nära sådant som arkivarier i allt större utsträckning arbetar med. Även om företagen säljer sina produkter och gärna behåller kontroll över dem så finns åtminstone i Enigios fall möjlighet att koppla loss kontrollen över blocken från dem genom en överföring av de nycklar som behövs (Enigio 2017). Att Bitcoin och andra kryptovalutor som bygger på blockkedjeteknologi funnits i närmare tio år utan att själva blockkedjorna manipulerats är i sig ett bevis på att teknologin fungerar väl för vissa typer av transaktioner. Det är till stor del tack vare att kryptovalutor visat att teknologin fungerar som det inom finanssektorn finns stor tilltro till den. Försöken kring att använda blockkedjor vid fastighetstransaktioner har mynnat ut i fungerande verksamheter där Georgien är det exempel verksamheten pågått längst, sedan våren 2017. Lantmäteriets och Kairos Futures pågående projekt kring fastighetstranaktioner i Sverige kommer med sin tredje och avslutande rapport våren 2018.

Kännedom och kunskap om blockkedjeteknologi och dess potentiella användningsområden ökar och forskning pågår inom flera olika discipliner och branscher viket sannolikt kommer göra medvetenheten om teknologin allt större de kommande åren. Även om kunskapen om blockkedjor bland arkivarier i Sverige tycks vara låg så finns i landet ändå kompetens som får anses vara världsledande inom teknologins användande för att säkra autenticitet hos digitala records genom företaget Enigios representanters medverkan i InterPARES trust. De analyser som gjorts för att undersöka blockkedjeteknologins kompabilitet med etablerade standarder för upprätthållande av autenticitet av framförallt Lemieux (2016a) visar att det redan idag går att uppfylla de flesta av kriterierna. Juridiskt sett kan regelverk behöva ses över för att den hantering som information utsätts för och metoder för validering inte ska riskera orsaka oförutsedda problem. Särskilt viktigt är det eftersom det inte alltid är självklart vilket lands lagar som gäller vid hanteringen och att det ännu inte finns någon enhetligt definierad terminologi inom området (Walsh 2017; Gunnarsson 2017).

7 Slutsatser

Utifrån den ovan förda diskussionen och de givna exemplen på pågående projekt och verksamheter som bygger på blockkedjeteknologi så är det gemensamma målet att säkra proveniens, autenticitet och trovärdighet hos information, antingen den är i forma av ekonomiska transaktioner, kontrakt, signaturer, registreringar eller dokumentation av fysiska produkter.

De uppställda frågeställningarna i inledningen till detta arbete var: 1. Vilka problem kring digital informationsautenticitet diskuteras inom arkivvetenskapen? 2. Hur skulle blockkedjeteknologi kunna lösa de problem som diskuteras? 3. Vilka potentiella för- och nackdelar finns kring blockkedjeteknologin?

Problematik kring autenticitet hos digital information har diskuterats ingående i de olika InterPARES projekten liksom av flera andra forskare och arkivarier. Medvetenheten om de problem som finns kring bevarande av digital information i allmänhet och att upprätthålla autenticitet i synnerhet är väl kända inom dokument och arkivhanteringsområdet. Av publicerade vetenskapliga artiklar så har det sedan 2016 kommit flera stycken som diskuterar blockkedjeteknologin och dess potential. Teknologin lanserades för snart tio år sedan men det är först under senare år som den fått någon större uppmärksamhet utanför användning av kryptovalutor. De projekt inom olika discipliner som idag pågår visar att många ser potential hos teknologin för att lösa problem inom många områden. Inom dokument och arkivområdet så ligger företaget Enigio långt fram och har idag fungerande produkt som bygger på teknologin. De personer som utvecklat Enigios blockkedjebaserade teknik är medaktörer i InterPARES trust och mycket tyder på att deras produkt kommer bli en del av den modell som planeras av projektet.

Potentiella hot och begränsningar hos teknologin har diskuterats och förslag på lösningar kring till exempel på hur olika kedjor skulle kunna interagera med varandra har föreslagits och produkter för detta är under utveckling. Vid en jämförelse med internationella standarder från ISO och ARMA för upprätthållande av autenticitet och trovärdighet hos information så framkommer vissa risker men i de flesta fall så utgör blockkedjeteknologin i sig inte något hinder för tillämpning av de standarder som finns idag. I stället är det frågetecken kring tillfället när information låses i ett block eftersom felaktig information kan förekomma vilket är något som ställer krav på organisationen kring hur information skapas och hanteras, något

som i sin tur regleras av ARMAs GARP. Den potentiella utvecklingen av snabbare och effektivare hårdvara i form av kvantdatorer diskuteras inom flera olika vetenskapliga discipliner och medvetenheten kring de potentiella hot de kan komma att utgöra är stor. Lösningar handlar om att även om kvantdatorer kommer bli vanligare och kunna användas för att hacka de underliggande krypteringar som används i dagens blockkedjor så går utvecklingen mot att ta fram allt mer avancerade algoritmer för kryptering. Blir kvantdatorer vanligare så kommer antagligen även kryptering ske med dem vilket skulle ge avsevärt mer avancerade krypteringar.

De risker som finns handlar om att säkra att det är korrekt information som sparas i blockkedjan och att åtkomsten garanteras, problem som känns igen från alla delar av arkiv och informationshanteringens område.

Slutsatserna av denna undersökning är således att blockkedjeteknologi har potential att lösa många av de problem som diskuteras kring bevarande av autenticitet hos digital information. Denna undersökning har visat att kännedomen om blockkedjeteknologin bland arkivarier i Sverige tycks vara tämligen låg samtidigt som det i Sverige finns expertis som får anses vara världsledande när det gäller tillämpning av blockkedjeteknologi inom dokument och arkivhanteringsområdet. InterPARES trust och forskningsprojekt TRUSTER kommer avslutas under 2018 och om slutprodukten kommer innehålla blockkedjeteknologi kommer stora delar av dokument och arkivhanteringsbranschen att behöva sätta sig in i hur det fungerar.

Önskvärt vore ett större engagemang från arkivsektorn för att identifiera potentiella problem och begränsningar blockkedjeteknologin skulle kunna tänkas medföra vid informationshantering och lagring på både kort och lång sikt. De många olika typer av projekt som pågår inom vitt skilda discipliner och det ökande antalet produkter som finns och bygger på teknologin gör att kunskaper om hur blockkedjor fungerar och hur man agerar när man ställs inför dem antagligen kommer bli en nödvändighet för de som behöver säkra integritet, autenticitet och proveniens hos digital information.

8 Käll- och Litteraturförteckning

Ada, Sharman, Gupta (2009) Theories Used in Information Security Research: Survey and Agenda. Handbook of Research on Social and Organizational Liabilities in Information Security.

Aggarwal m.fl. (2017) Quantum attacks on Bitcoin, and how to protect against them https://arxiv.org/pdf/1710.10377.pdf [Hämtad 17-12-21]

Alexander, D, (2017) https://www.bloomberg.com/news/articles/2017-11-14/forget-iris-scans-canadians-to-use-blockchain-for-digital-ids [Hämtat 2017-11-19]

Andersson, K, (2017) Blockkedjeteknik, https://publications.theseus.fi/bitstream/handle/10024/132514/BlockkedjeteknikFinal.pdf?sequence=1&isAllowed=y [Hämtad 2018-01-01].

Arving, C, (2012) *Tre exempel på hur man kan beskriva sin kvalitativa dataanalys* Digitalt exemplar tillgängligt hos författaren.

Back m.fl. (2014) Enabling Blockchain Innovations with Pegged Sidechains https://www.blockstream.com/sidechains.pdf [Hämtad 2018-01-01].

Beall, A, (2017) Bitcoin mining uses more energy than Ecuador – but there's a fix https://www.newscientist.com/article/2151823-bitcoin-mining-uses-more-energy-than-ecuador-but-theres-a-fix/?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook#link_time=1510066022 [Hämtad 2017-11-16].

Bearman, D. (1994). Electronic Evidence, Strategies for Managing Records in Contemporary Organizations. Pittsburgh, Archives & Museum Informatics. https://pdfs.semanticscholar.org/a600/0229f82c47921a565e37ce6ef3f9f17d111c.pdf [Hämtad 2018-01-01]

Bernstein m.fl (2017) Post-quantum RSA https://eprint.iacr.org/2017/351.pdf [2018-01-01].

Bralić, Kuleš, Stančić, (2017) A Model for Long-term Preservation of Digital Signature Validity: TrustChain https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain [Hämtad 2017-11-21].

Byström & Lundkvist (2017) Blockkedjan – En riskreducerare? En undersökning av blockkedjans effekt på risk inom revisions - , finans - och fastighetsbranschen. http://www.diva-portal.org/smash/get/diva2:1119384/FULLTEXT01.pdf [2018-01-01].

Cheng, S, Daub, M, Domeyer, A, Lundquist, M, (2017) *Using blockchain to improve data management in the public* sectorhttps://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Using%20blockchain%20to%20improve%20data%20management%20in%20the%20public%20sector/Using-blockchain-to-improve-data-management-in-the-public-sector.ashx [Hämtad 2017-12-27].

Chung, Park, Lee (2017) Digital forensic approaches for Amazon Alexa ecosystem. Digital Investigation 22 (2017).

Cleaver, Bruce, (2017) Expectations changing change expectations: diamond traceability https://www.debeersgroup.com/en/news/views/expectations-changing-changing-expectations--diamond-traceabilit.html [Hämtad 2017-12-14].

Cohn, C, (2011) EFF and Bitcoin https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin [Hämtad 2017-11-16].

Collindres, Regan, Pantres (2016) Using Blockchain to Secure Honduran Land Titles https://s3.amazonaws.com/ipri2016/casestudy_collindres.pdf [Hämtad 2017-11-19].

Duranti & Thibodeau, (2006) The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES https://link-springer-com.till.biblextern.sh.se/content/pdf/10.1007%2Fs10502-006-9021-7.pdf [Hämtad 2018-01-01].

Duranti, L, (1989) Diplomatics: New uses for an old science. Archivaria 28 (summer 1989) https://archivaria.ca/index.php/archivaria/article/viewFile/11567/12513 [Hämtad 2017-12-09].

Duranti (2009) From digital diplomatics to digital records forensics. http://www.interpares.org/display_file.cfm?doc=ip3_canada_dissemination_jar_duranti_archivaria_68_2009.pdf [2018-01-01].

Duranti, (2010) A Framework For Digital Heritage Forensics http://mith.umd.edu/forensics/wp-content/uploads/2010/05/4n6umd_duranti.pdf [Hämtad 2017-10-24].

Duranti, (2010b) Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. http://www.emeraldinsight.com.till.biblextern.sh.se/doi/pdfplus/10.1108/09565691011039852 [Hämtad 2017-12-11].

Duranti & Rogers, (2012) Trust in digital records: An increasingly cloudy legal are, *Computer law & security review* 28 (2012) 522 e 531.

Duranti (2013) *From classic diplomatics to digital diplomatics*. Föreläsningsmaterial. http://www.arkivrad.no/sites/arkivrad/files/user/Dokumenter/Medlemsmoter/foredrag_pa_hioa_duranti-oslo_digital_diplomatics_26092013_0.pdf [Hämtad 2017-12-11].

Factor, M, m.fl. (2009) Authenticity and Provenance in Long Term Digital Preservation: Modeling and Implementation in Preservation Aware Storage https://www.usenix.org/legacy/event/tapp09/tech/full_papers/factor/factor.pdf [Hämtad 2017-12-09].

Fritz, B, (2017) Diplomatik, Nationalencyklopedin. http://www.ne.se/uppslagsverk/encyklopedi/lång/diplomatik [Hämtad 2017-12-08].

Gunnarsson, J, (2017) Blockkedjeteknik och avtalsrätt - särskilt om skydd för svagare part vid användning av smarta kontrakt. http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8909063&fileOId=8917016 [Hämtad 2018-01-01].

Hoffman (2017) Blockchain for Recordkeeping: Help or Hype? Vol 2. https://www.researchgate.net/profile/Victoria_Lemieux/publication/309414363_Blockchain_for_Recordkeeping_Help_or_Hype/links/580f539408ae009606bb62f6.pdf [Hämtad 2017-11-21].

Hänström, Kenneth (2007) Autenticitet I en digital värld: långsiktigt bevarande av allmänna handlingar. HU-MAN IT 9.1(2007): 67-109. https://humanit.hb.se/article/viewFile/112/566 [Hämtad 2017-12-05].

Illgner, A, (2017) *How do you link the world's blockchains? With another blockchain* https://www.newscientist.com/article/mg23631534-600-how-do-you-link-the-worlds-blockchains-with-another-blockchain/?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook#link_time=1511374021 [Hämtad 2017-11-22].

John, J, L, (2012) Digital Forensics and Preservation. http://www.dpconline.org/docs/technology-watch-reports/810-dpctw12-03-pdf/file [Hämtad 2018-01-01].

Kirschenbaum m fl (2010) - Digital Forensics and Born-Digital Content in Cultural Heritage Collections. https://drum.lib.umd.edu/bitstream/handle/1903/14722/whitepaper_borndigital.pdf?sequence=1 [Hämtad 2018-01-01].

Korhonen, Lindström, (2016) *Litteraturstudie* https://www.vasa.abo.fi/users/geklund/Hemsida%20dokument%202016-17/Litteraturstudie%205.9%2016.pdf [Hämtad 2017-11-23].

Larimer, D, (2014) *Momentum – A memory-hard proof-of-work via finding birthday collisions* http://www.hashcash.org/papers/momentum.pdf [Hämtad 2018-01-01].

Lemieux, V, (2016a) Trusting records: is Blockchain technology the answer?, *Records Management Journal*, Vol. 26 Issue: 2, pp.110-139, https://doi.org/10.1108/RMJ-12-2015-0042 [Hämtad 2018-01-01].

Lemieux, V, (2016b) *Blockchain for Recordkeeping.* Föreläsningsmaterial. https://www.w3.org/2016/04/blockchain-workshop/slides/Lemieux-Blockchain_for_Recordkeeping.pdf [Hämtad 2018-01-01].

Marjomaa, Josefin, (2017) *Såhär fungerar en kvantdator* https://www.svt.se/nyheter/lokalt/vast/sahar-fungerar-en-kvantdator [Hämtad 2017-11-29].

Mattila, Juri Seppälä, Timo Holmström, Jan, (2016) *Product- centric Information Management A Case Study of a Shared Platform with Blockchain Technology* https://escholarship.org/content/qt65s5s4b2/qt65s5s4b2.pdf [Hämtad 2017-12-01].

Mesropyan, E, (2017) *30 Non-Financial Use Cases of Blockchain Technology [Infographic]* https://letstalkpayments.com/30-non-financial-use-cases-of-blockchain-technology-infographic/ [Hämtad 2017-12-29].

Nakamoto, S, (2008) Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf [Hämtad 2018-01-01].

Ottsjö, P, (2017) Svensk blockkedja säkrar bevis på krigsbrott, *Ny Teknik*, https://www.nyteknik.se/digitalisering/svensk-blockkedja-sakrar-bevis-pa-krigsbrott-6872068 [Hämtad 2017-12- 21]

Pickard, A, (2013) Research Methods in Information, second edition. London.

Ryder, Bratt, (2017) Goverments may be big backers of the blockchain The Economist https://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers [Hämtad 2017-11-29].

Shrier, Wu, Pentland, (2016) Blockchain & Infrastructure (Identity, Data Security) https://www.getsmarter.com/career-advice/wp-content/uploads/2017/07/mit_blockchain_and_infrastructure_report.pdf [Hämtad 2017-11-21].

Smerkis, Vlad, (2017) Georgia Records 100,000 Land Titles on Bitcoin Blockchain: BitFury The Cointelegraph https://cointelegraph.com/news/georgia-records-100000-land-titles-on-bitcoin-blockchain-bitfury [Hämtad 2017-11- 29].

Storch, S, (1998) Diplomatics: Modern archival method or medieval artifact. The American Archivist Vol. 61 sid 365-383. http://americanarchivist.org/doi/pdf/10.17723/aarc.61.2.h0358316qn85p2lm [Hämtad 2017-12-11].

Wall, E, Malm, G, (2016) *Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository* http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8885750&fileOId=8885765 [Hämtad 2017-12-29].

Walsh, A, (2017) The Path of The Blockchain Lexicon (And the Law) https://www.bu.edu/rbfl/files/2017/09/p729.pdf [Hämtad 2018-01-01].

Wendt, M, R, (2013) Jean Mabillon - Biographische Notizen http://x0b.de/mabillon/mabillon-einfuehrung.html [Hämtad 2017-12-04].

Yli-Huumo, Ko, Choi, Park, Smolander, (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5047482/ [Hämtad 2017-12-07].

Källor utan angiven författare.

Algoritmer, (2009)
http://www.csc.kth.se/utbildning/kth/kurser/DD1341/inda10/algorithms/algoritmer/
Bitcoin, (2017) https://en.bitcoin.it/wiki/Bitcoin#cite_note-25[Hämtad 2017-11-17].

Blockchain Data Integrity, (2017) https://www.ericsson.com/hyperscale/cloud-infrastructure/data-centric-security/data-integrity-assurance Tillgänglig 24/11-2017.
Data Centric Security, (2017) https://www.ericsson.com/en/security/data-centric-security [Hämtad 2017-11-24].

eARD (2013) Begreppslista. Digital version tillgänglig hos författaren.

Electronic Frontier Foundation (2017) https://supporters.eff.org/donate [Hämtad 2017-11-16].

Everledger (2017) www.everledger.io [Hämtad 2017-11-21].

GARP (2017) Generally Accepted Recordkeeping Principles® ©2017 ARMA International, www.arma.org/principles [Hämtad 2017-12-14].

Hash och hashing, (2010)
https://web.archive.org/web/20100302074904/http://www.nada.kth.se/dataterm/fos-lista.html#f168 [Hämtad 2017-11-20].

Hyperledger (2016) https://hyperledger.org/about/charter [Hämtad 2017-11-21].

IBM, (2017) IBM Announces Major Blockchain Collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide
http://www-03.ibm.com/press/us/en/pressrelease/53013.wss [Hämtad 2017-11-22].

InterPARES 1(2001) The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project http://www.interpares.org/book/interpares_book_d_part1.pdf [Hämtad 2017-12-05].

Kairos Future, (2017a) The Land Registry in the blockchain - testbed
https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf [Hämtad 2017-11-22].

Kairos Future (2017b) Blockchain use cases for food traceability and control
https://cdn2.hubspot.net/hubfs/3279625/Publications/Publication%20ENG%20Blockchain%20for%20food%20traceability%20and%20control%202017.pdf [Hämtad 2017-12-15].

Lantmäteriet (2016) Framtidens husköp i blockkedjan Ett utvecklingsprojekt med Lantmäteriet, Telia Company, Chromaway och Kairos Future
https://www.lantmateriet.se/contentassets/6874bc3048ab42d6955e0f5dd9a84dcf/blockkedjan-framtidens-huskop.pdf [Hämtad 2018-01-01].

NASDAQ, (2017) Nasdaq to Deliver Blockchain e-Voting Solution to Strate http://ir.nasdaq.com/releasedetail.cfm?releaseid=1049610 [Hämtad 2017-11-27].

Nod (2017) https://it-ord.idg.se/ord/nod/ [Hämtad 10-12-17].

Principle of Integrity (2017) http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles/integrity [Hämtad 2017-12-07].

Provenance (2017) https://www2.archivists.org/glossary/terms/p/provenance [Hämtad 2017-12-11].

Riksarkivet (uå), Projekt e-arkiv och e-diarium, eARD gör det enklare att följa sina ärenden https://riksarkivet.se/Media/pdf-filer/Projekt/eARD_informationstext.pdf

RSK (2017) https://www.rsk.co/ [Hämtad 2017-12-06].

School of Information Sciences, (2002), Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project http://www.archimuse.com/papers/nhprc/ Återskapad hemsida 2002. [Hämtad 2018-01-01].

TAM- Arkiv, (2014) Arkivhandbok http://www.tam-arkiv.se/sites/default/files/documents/tam_arkivstod/Arkivhandbok_ver_1_0.pdf [Hämtad 2017-12-04].

Vestal Virgins of Rome (2017) http://www.historyandwomen.com/2010/05/vestal-virgins-of-rome.html [Hämtad 2017-12-01].

Wint, (2015) Så garanterar vi att ingen ändrar i bokföringen i efterhand. http://www.mynewsdesk.com/se/wint/blog_posts/saa-garanterar-vi-att-ingen-aendrar-i-bokfoeringen-i-efterhand-41516 [Hämtad 2017-11-22].

Personlig kommunikation

Digitaliseringschef vid Lantmäteriet, kontakt via e-post 22/11, 24/11 och 27/11 2017.
CEO Kairos Future, kontakt via e-post 22/11 2017.
COO Enigio, kontakt via e-post 19/12 och 20/12 2017.
Utvecklare hos Wint, kontakt via e-post 27/11 2017.