Ansvar för personuppgifter i publika blockkedjor

– En teknologi förenlig med GDPR?

Stellan Koch

Juridiska institutionen
Examensarbete 30 hp.
Inriktning: Rättsinformatik
Juristprogrammet (270 hp.)
Höstterminen 2018
Handledare: Johan Axhamn
Examinator: Cecilia Magnusson Sjöberg
Engelsk titel: Responsibility for Personal Data in the Public Blockchain
– A Technology Compatible with the GDPR?

Stockholms universitet

Förord

När uppsatsen som sista moment i min juristexamen nu är klar vill jag passa på att rikta ett stort tack till släkt och nära vänner som visat intresse och omtanke under min utbildning.

Jag vill även särskilt tacka hela min familj för all den oerhörda värme, motivation och det stöd ni kontinuerligt gett mig under utbildningens gång – utan er hade det här inte varit möjligt.

Tack.

Stockholm den 6 januari 2019
Stellan Koch

Ansvar för personuppgifter i publika blockkedjor

– En teknologi förenlig med GDPR?

Stellan Koch

Abstract

While the Internet provides enormous opportunities within development of communications and database systems it also endangers the processing of personal data unlawfully. With traditional database structure in focus the responsibility and accountability of said processed personal data was somewhat clear as the General Data Protection Regulation (GDPR) entered the legal framework of the European Union's member states in May 2018. Blockchain technology being the latest innovation in database structure challenges the applicability of the new regulation by introducing cryptography and a peer-to-peer distributed ledger technology. This thesis is the result of an attempt to analyze the personal data processed in public blockchains, i.e. Bitcoin, and its compliance with certain fundamental data protection rights stipulated in the GDPR such as the right to erasure of personal data.

Furthermore, in relation to fundamental data protection rights violations are also subjects of accountability. While the new distributed ledger technology vastly increases the difficulty to determine a target for accountability the thesis also considers the traditional view on databases on which the GDPR was built upon. Thus, the thesis aims to further explore the relation between participants on the innovative blockchain and fundamental personal data protection rights in the GDPR.

Nyckelord
GDPR, Dataskyddsförordningen, Blockkedjor, Personuppgifter, Personuppgiftsansvar.

Förkortningar

Ds.	Departementsserien
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
EU	Europeiska unionen
Europakonventionen	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna 2012/C 326/02
Funktionsfördraget	Fördraget om Europeiska unionens funktionssätt 2012/C 326/01
IP	Internetprotokoll
kB	Kilobyte
MB	Megabyte
prop.	Proposition
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning
TfR	Tidsskrift for Rettsvitenskap

Innehållsförteckning

1. Inledning

1.1 Bakgrund

De senaste årtiondena har teknologi-, kommunikations- och IT-system utvecklats snabbt. Inte bara har de samhälleliga kraven på informationstillgänglighet och kommunikation ökat utan även utbudet av digitala lösningar och protokoll inom dessa områden. Ur ett rättsligt perspektiv har dels tolkningar för att inrymma sådan ny teknologianvändning gjorts inom redan tillämplig lagstiftning och dels har ny lagstiftning och direktiv stiftats på både nationell och internationell nivå. I grund och botten är ofta kommunikation, information och datasäkerhet gemensamma grundpelare för dessa innovativa teknologiska tjänster. En teknikutveckling som möjliggör yttrandefrihet och informationsspridning innebär dock även risker för integritetskränkningar vilket medför ett krav på lagstiftaren att säkerställa att integritetsskyddande bestämmelser kan tillämpas.[1]

Ett exempel på en snabbutvecklande teknik är området inom *blockkedjor*. De digitala valutornas eller *kryptovalutornas* explosionsartade framväxt som exempelvis Bitcoin har säkert inte undgått många. Det är dock med säkerhet färre som förstår sig på den teknologiska strukturen bakom dessa valutor, närmare bestämt blockkedjeteknologin. En blockkedja eller *blockchain* på engelska är inte nödvändigtvis en kryptovaluta. Fördelarna som blockkedjor medför gör dem dock särskilt lämpade som transaktionssystem och digitala valutor. Blockkedjeprojekt och applikationer finansieras ofta även genom att en överliggande funktionell valuta skapas för blockkedjan som investeringsinstrument, varför kryptovalutor och blockkedjor ofta förväxlas. Ur ett rättsinformatiskt perspektiv är det emellertid själva blockkedjeteknologin bakom dessa projekt och valutor som är särskilt intressant att studera. Blockkedjeteknologin medför att data kan ”kedjas ihop” med hjälp av matematiska formler och på så sätt skapa en lång kedja av data. Övergripande kan nämnas att kedjestrukturen bidrar till att verifiera den information som behandlas. De matematiska standarder som används i blockkedjor förhindrar att tidigare inlagd information ändras då hela kedjan fallerar om någon tidigare länk ändras. Publika blockkedjor löser även med hjälp av en distribuerad databasstruktur problemet med en centraliserad påverkanspunkt. Istället för att databasen nås via en enskild server distribueras hela databasen kontinuerligt till alla i nätverket så att nätverket kan fortsätta vara aktivt

[1] SOU 2016:7 s. 184 f.

och databasen tillgängligt via andra användares upplagor av databasen i det fall en server går ned.

Med hjälp av denna kedjestruktur som tydligt synliggör ändringar av information i kedjan för alla i nätverket möjliggör blockkedjeteknologin verifieringar av digitala original. Blockkedjor som är öppna för allmänheten, publika blockkedjor, är särskilt lämpade för digitala transaktioner sedan alla kan delta i nätverket och det går att verifiera transaktioner utan behov av någon tredje part som säkerställer systemet såsom en bank eller myndighet. Anledningen att blockkedjeteknologin är intressant att studera ur ett juridiskt perspektiv bottnar i att blockkedjor medför en ny struktur över hur information behandlas och distribueras. En djupare och mer teknisk beskrivning av teknologin följer i kommande kapitel.

Medan både utbudet och intresset för blockkedjor växer hos såväl företag som myndigheter finns en mängd frågeställningar och rättsliga oklarheter som teknologin bär med sig. De mest rättsligt relevanta frågorna berör datahanteringen och ansvarsproblematiken. En fundamental skillnad mot vanliga databaser är den distribuerade huvudboken som publika blockkedjor använder och avsaknaden av ändringsmöjlighet för data som blivit tillagd på kedjan. Dessa skillnader ligger till grund för många av de juridiska spörsmål som kommer redogöras för mer ingående i denna uppsats. Istället för att en person eller ett företag har en server och databas finns informationen istället hos alla som är med i ett decentraliserat nätverk. Det är just denna teknologiska strukturändring som skapar tillämpningsfrågor i förhållande till Europeiska unionens (EU) allmänna förordning om behandling av personuppgifter (GDPR).[2]

1.2 Ämnet

Det huvudämne som denna uppsats handlar om är de dataskyddsrättsliga följdproblem som följer av blockkedjestrukturen med en distribuerad huvudbok, särskilt den personuppgiftsansvarigas roll i förhållande till blockkedjor. Målet är att utreda tillämpningen av och förenligheten med GDPR för blockkedjor där varje ny bit av information samtidigt blir distribuerad till flera enheter istället för lagrade på en enhet som traditionella databaser. Uppsatsen ämnar utreda hur GDPR kan tillämpas på den databasstruktur blockkedjor medför som skiljer sig så väsentligt från traditionella databaser. Målsättningen omfattar även en utredning av hur de tekniska behandlingarna av informationen som lagras på kedjan, bl.a. *kryptografiska hash-*

[2] Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), hädanefter GDPR, dataskyddsförordningen eller förordningen.

funktioner (kryptering av klartext till kod), bör betraktas inom ramen för GDPR och personuppgiftsbegreppet. Uppsatsen berör hur regelverket i GDPR avseende *behandling* och *personuppgiftsansvarig* bör tolkas när det kommer till blockkedjor. Behandlingen tar sikte främst på personuppgiftsbehandlingen som GDPR ställer särskilda krav på. En av de centrala delarna i blockkedjor är att mycket information omvandlas till annan typ av kod vid lagring. Uppsatsen ämnar i det avseende undersöka hur den typ av informationsbehandling som sker i publika blockkedjor bör betraktas i förhållande till GDPR. Den andra centrala punkten för blockkedjor är dess decentraliserade karaktär där det inte finns någon central databas utan allt är distribuerat till varje nod i nätverket. I denna typ av databasstruktur där det inte finns någon uttryckligt ansvarig blir begreppet personuppgiftsansvarig särskilt problematiskt. De fundamentala integritetsskyddande bestämmelserna som en personuppgiftsansvarig ska säkerställa riskerar för blockkedjor följaktligen bli svårapplicerade.

För att förstå vissa diskussioner om bl.a. pseudonymisering och hashsummors förhållande till personuppgiftsbegreppet fullt ut kommer den tekniska biten redogöras för ingående i följande kapitel. Teknologin bakom ämnet beskrivs dock i korthet redan i detta inledande kapitlet för att läsaren enklare ska kunna greppa syftet och frågeställningarna. I en traditionell databas sparas normalt informationen på en enhet, som även kan vara tillgänglig för åtkomst på flera håll genom en serveruppkoppling. Vid nytt införande av information sparas det genom servern ned på databasen som sedan finns tillgänglig för andra som har åtkomst till samma server. Det centrala är emellertid hela tiden att information som läggs till eller ändras sker i en och samma databas.

Teknologin bakom den nätverksstruktur som blockkedjor använder innebär emellertid, något förenklat, att istället för att en centraliserad bakomliggande databas används har alla i systemet en fullständig kopia av databasen på sin användarenhet. Vid en ny införing av information sparas det inte ned till en centraliserad databas på en enhet, utan skickas ut till alla användarenheter i systemet (s.k. *peer-to-peer*, P2P). Skillnaden mot en molntjänst blir följaktligen att informationen finns sparad på varje användarenhet istället för att åtkomst sker via uppkoppling mot en eller flera förutbestämda servrar. En sådan distribuerad databas medför följaktligen många juridiska frågeställningar om bl.a. ansvar. Det kan noteras att blockkedjeteknologin inte främst gör sig känd för själva distribueringsmomentet, utan för de tekniska

standarder som används som medför att information i kedjan kan verifieras och sedermera inte bli föremål för ändring eller korruption.[3]

1.3 Syfte och frågeställningar

Uppsatsens syfte är att utreda två huvudsakliga juridiska frågeställningar som användandet av blockkedjeteknologin medför. Först kan nämnas frågor om informationshanteringen och de i GDPR relevanta skyddsbestämmelserna som bl.a. rätten till rättelse, ändring och radering.

- Hur skiljer sig personuppgiftsbehandlingen i publika blockkedjor mot behandlingen i traditionella databaser?
- Hur förhåller sig behandlingen av personuppgifter i publika blockkedjor till dessa integritetsskyddande bestämmelserna i GDPR?
- Kan publika blockkedjor medföra praktiska tillämpningsproblem med de krav GDPR uppställer på integritetsskyddande åtgärder?

Utöver hur teknologin samverkar med de fundamentala integritetsskyddande bestämmelserna behöver ansvarsfrågan för personuppgifternas behandling på blockkedjorna utredas. I GDPR stipuleras ett särskilt ansvar för den som är att anse som personuppgiftsansvarig. Ansvaret grundas i att den personuppgiftsansvarige ofta är den som bestämmer ändamålet och utförandet av uppgiftsbehandlingen. För blockkedjor blir det emellertid problematiskt då det inte finns någon central auktoritet eller ansvarig i den traditionella meningen. Eftersom blockkedjor ändrar lagringsstrukturen så väsentligt mot traditionella databaser behöver följande frågeställningar ställas.

- Går det att för publika blockkedjor med säkerhet säga hur personuppgiftsansvaret i GDPR ska betraktas i förhållande till de olika aktörerna på publika blockkedjor?

1.4 Avgränsning

Blockkedjor och virtuella valutor förväxlas i hög grad då virtuella valutor ofta bygger på blockkedjor. Politiska och regulatoriska diskussioner kring blockkedjor och kryptovalutor och de nationalekonomiska diskussioner som kryptovalutor medför är intressanta. Denna uppsats kommer dock begränsas till att fokusera på rättsliga utmaningar för blockkedjor inom ramen för personuppgifter och datahantering.

[3] För vidare redogörelse av P2P-nätverk se Drescher, D., *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, Berkeley CA, 2017, s. 14 f. och 23 f. [cit. Drescher].

Vidare måste en begränsning av vilken eller vilka blockkedjor som ska analyseras göras. På webbplatsen CoinMarketCap som listar börshandlade kryptovalutor finns i skrivande stund över 1700 stycken listade.[4] Visserligen är många av dessa mindre kryptovalutor versioner av andra större blockkedjor, men det är för tekniskt omfattande att redogöra för varje unik blockkedja. Sedan teknologin är det intressanta att utreda kommer uppsatsen i avsnitt där förklaringar görs eller exempel ges avseende blockkedjor baseras på Bitcoins blockkedjestruktur. Bitcoins blockkedja är den största kända publika blockkedjan och är fokuserad på transaktioner, men strukturen och teknologin går att applicera på andra områden. För att skapa en förståelse för det mest relevanta kan därför, om det underlättar för att förstå användningsområdet, en transaktion istället föreställas en annan typ av dataöverföring som en bild eller ett inlägg i ett register. Andra blockkedjor kan komma att nämnas i de fall det är nödvändigt som jämförande exempel för att skapa sammanhang i diskussionen.

En avgränsning i relation till GDPR görs till att endast behandla några av de mest relevanta frågeställningarna för blockkedjor. Här kan främst nämnas GDPRs tillämpningsområde, definitioner samt frågeställningar kring begrepp som personuppgifter och personuppgiftsansvarig. Särskilt intressant är ansvarsfrågan och bestämmandet av vem som är personuppgiftsansvarig eller personuppgiftsbiträde för blockkedjor varför det kommer fokuseras på. Uppsatsen ämnar inte utreda artikel för artikel av GDPR, utan kommer istället att belysa utvalda artiklar i nämnda kapitel i förhållande till de i uppsatsen relevanta frågeställningarna.

Som nämnt kommer uppsatsen begränsas till att behandla publika blockkedjor. Skillnaden mellan publika och privata blockkedjor kommer dock beskrivas och exemplifieras för att ge förståelse till problematiken som diskuteras. I detta avseende kommer privata blockkedjor beröras i ett jämförande syfte men i förhållande till de rättsliga frågeställningarna hålls fokus på publika blockkedjor.

1.5 Metod och material

Avseende metodval och material kan följande nämnas. Området uppsatsen avser att behandla är relativt nytt. Många rättsordningar har i dagsläget inte domstolsprövat blockkedjeteknologin som väsentligt ändrar strukturen och därmed hur informationen hanteras gentemot vanliga traditionella databaser. Med anledning av att EU:s nya dataskyddsförordning, GDPR, trädde i kraft den 25 maj 2018 har i princip hela EU numera samma bestämmelser avseende person-

[4] CoinMarketCap, *Historical Snapshot – September 09, 2018 | CoinMarketCap*, "www.coinmarketcap.com/historical/20180909/", lydelse 2018-09-09.

uppgiftshantering. Då många rättsordningar följaktligen har samma regelverk på området för personuppgiftshantering, under vilket blockkedjor inte har prövats i särskilt stor utsträckning, är den rättsdogmatiska metoden den mest aktuella metoden att lägga till grund för uppsatsen.

Det motiveras med att den rättsdogmatiska metoden i korthet söker utreda hur regler faktiskt tillämpas på en given situation; vad är gällande rätt på området? Den rättsdogmatiska metoden präglas av ett försök att systematisera och tolka de rättskällor som finns.[5] Genom att studera rättskällor görs ett försök att tolka de bestämmelser som kan tänkas omfatta det aktuella problemet. Rättskällorna i den traditionella meningen är bl.a. lagtext, förarbeten, domstolsavgöranden, doktrin och sedvanerätt m.fl.[6] I brist på avgörande från prejudikatinstanser får avgöranden från lägre instanser ses som vägledande tills vidare. Vidare torde sedvana på området för blockkedjor i detta avseende inte kunna ges någon betydande rättslig tyngd med anledning av att teknologin är så pass ny att den inte ännu har någon rättslig förankring eller stöd.

Uppsatsens ämne spänner över fler rättsordningar än bara den svenska. De källor som kommer att behandlas är således inte begränsade till endast svenska. I synnerhet, sedan GDPR är ett framarbetat direktiv inom EU, kommer rättskällorna även att omfatta artiklar, historia och diskussioner om vad regelverket exakt var tänkt att lösa. Det kan vara värt att nämna att rättsdogmatiken inte är en entydig metod. Grundstenen i rättsdogmatisk metod är rättskälleläran, men i brist på praxis eller lag med förarbeten som explicit nämner de problem blockkedjor medför kommer doktrin och artiklar ha en viktig funktion i denna uppsats för att försöka klargöra tolkningen och systematiseringen av gällande rätt.

Värt att bära med sig gällande doktrin och artiklar är att slutsatser och tolkningar måste dras med stor varsamhet och stor källkritik. Nya teknologier, som blockkedjeteknologin, med stor potential men få färdiga produkter är ofta föremål för kraftiga spekulationer och investeringar. Det är därför inte ovanligt förekommande att artiklar författas med ett underliggande motiv. Ju längre från primära rättskällor desto större kritik bör därför riktas mot innehållet. Den typen av doktrin behöver dock inte kritiseras för endast att vara påverkande med anledning av investeringar utan kan även bidra till rättssäkerhet och förutsebarhet då doktrin som rättskälla inte konkurrerar på samma sätt med demokratiskt förankrade rättskällor som lag och rättsfall.[7]

[5] Jfr Kleineman, J., *Rättsdogmatisk metod*, i Korling, F. & Zamboni, M. (red.), *Juridisk metodlära*, Studentlitteratur, Lund, 2013, s. 26 [cit. Korling & Zamboni (red.)].
[6] Ibid. s. 21.
[7] Ibid. s. 27.

Eftersom ämnet har en så pass landsöverskridande karaktär, framförallt inom EU med anledning av GDPR, kommer den rättsdogmatiska metoden få ett visst EU-rättsligt genomslag då den nationella lagstiftningen på området i princip utgörs av GDPR.[8] Inom EU-rätt finns emellertid nationell doktrin hos alla medlemsländer.[9] Inom området för integritet och personuppgiftsbehandling kan det skilja sig väsentligen mellan länderna. Den rättsdogmatiska metoden kommer därför tillmätas ett brett förhållningssätt för att inkludera EU-rättsliga inslag för att se till de gemensamma personuppgiftsrättsliga frågor GDPR behandlar som kan inverka på området för blockkedjor.

Det som kännetecknar ett sådant extensivt förhållningssätt till att inkludera viss EU-rättslig metod i den s.k. rättsdogmatiska är att fokus skiftas från svenska till EU-rättsliga rättskällor.[10] Olsen hävdar att den rättsdogmatiska metoden bör tolkas snävt och inte inrymmer sådana inslag av dels internationell karaktär eller bredare analyser och *lege feranda*-resonemang utan endast avser utreda gällande rätt.[11] Istället har bl.a. Sandgren påpekat att en sådan extensiv användning av rättsdogmatiken bör betraktas som någon form av analytisk rättsforskning.[12] Jareborg menar dock att man inte inom rättsdogmatiken hindras vidga perspektivet och gå utanför gällande rätt för att söka nya svar och bättre lösningar.[13] Den rättsdogmatiska metoden som används i denna uppsats är därför som Sandgren hade benämnt den rättsanalytisk medan jag väljer att beteckna den som extensiv rättsdogmatisk i linje med Jareborg. Oavsett hur man väljer att beteckna metoden inkluderas ett mer analytiskt och kritiskt perspektiv i uppsatsen än att endast systematisera och klarlägga gällande rätt.

Eftersom uppsatsen skrivs under rättsinformatikens område kommer även den rättsinformatiska metoden underbygga denna uppsats. Metoden innebär bl.a. att tillvägagångssätt att integrera juridiska aspekter i tekniskt orienterade områden studeras.[14] Arbetet präglas av att undersöka systematiken mellan juridik och informationsteknik. Det kan i praktiken handla om konsekvensanalyser och skyldighetsanalyser för viss teknisk implementering av system som kan komma att behandla personuppgifter i bl.a. sökfunktioner online.[15] Genom att studera dessa

[8] Malmgren, S., *Rättslig informationsförsörjning online*, i Magnusson Sjöberg, C. (red.), *Rättsinformatik – juridiken I det digitala informationssamhället*, 2 u., Studentlitteratur, Lund, 2016, s. 460 [cit. Magnusson Sjöberg (red.)].
[9] Reichel, J., *EU-rättslig metod*, i Korling & Zamboni (red.) s. 128 f.
[10] Reichel, J., *EU-rättslig metod*, i Korling & Zamboni (red.) s. 109.
[11] Se Olsen, L., *Rättsvetenskapliga perspektiv*, SvJT 2004 s. 116 f.
[12] Se Sandren, C., *Är rättsdogmatiken dogmatisk?*, TfR 2005 s. 655 f.
[13] Se Jareborg, N., *Rättsdogmatik som vetenskap*, SvJT 2004 s. 5.
[14] Magnusson Sjöberg, C., *Om rättsinformatik*, i Magnusson Sjöberg (red.), s. 27.
[15] Ibid. s. 29.

samband mellan IT och juridik ökar förutsättningarna för att på ett tillfredsställande sätt bedöma möjligheter och risker för tekniska applikationer.[16] Vägledning kan här hämtas från bl.a. utskott och andra arbetsgrupper inom EU. En sådan arbetsgrupp skapar inte nödvändigtvis någon officiellt bindande vägledning men bör ändå kunna tillmätas ett större värde än övrig doktrin på grund av sin status på området i kombination med brist på annan vägledande praxis. Vidare kan nationella myndigheter utfärda vägledning och riktlinjer vilka bör behandlas på liknande sätt. I den strikt rättsdogmatiska metoden bör en sådan myndighetsvägledning kunna tillmätas ett högre värde medan sådan vägledning ur ett mer analytiskt perspektiv fortfarande kan ifrågasättas utan lagförtydligande eller prejudikat från EU-domstolen.

1.6 Disposition

Denna uppsats är disponerad på följande sätt. Utöver detta inledande kapitel kommer kapitel två behandla tekniken bakom blockkedjor; hur de fungerar och vad det rent tekniskt sett är som gör de särskilt användbara. En grundläggande förståelse för teknologin är viktig för att juridiska diskussioner senare inte ska uppfattas som svårförståeliga eller sakna sammanhang. Därefter kommer i kapitel tre de rättsregler som uppsatsen ämnar problematisera att redogöras för; de behandlingsregler samt ansvarsregler för informationen i blockkedjor. Rättsreglerna och aktuella artiklar i GDPR redogörs först för generellt, vilka syften de har och hur tanken är att de ska användas. Därefter diskuteras blockkedjors kompabilitet och samverkan på detta förhållande i kapitel fyra. Till sist förs avslutande diskussioner och resonemang för att sammanfatta vilka slutsatser som kan nås.

[16] Ibid. s. 30.

2. Blockkedjeteknologin

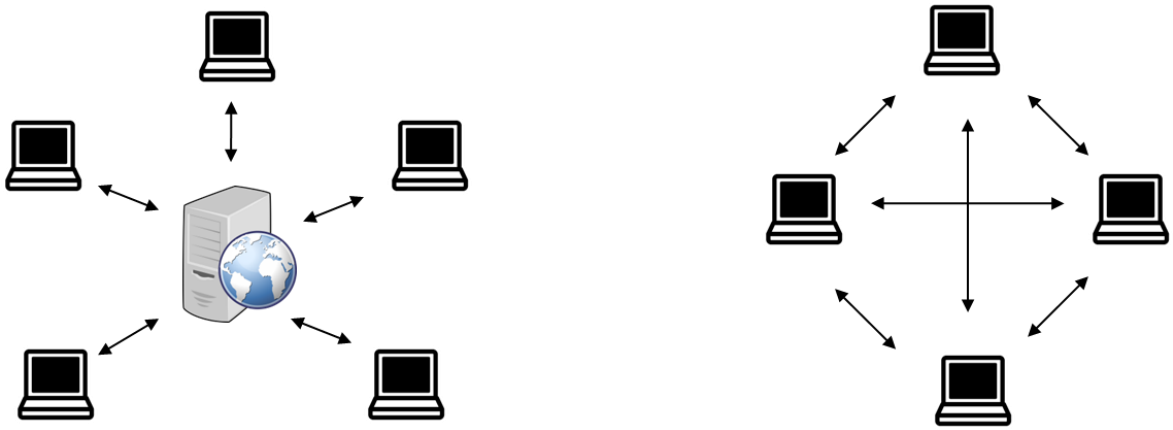
2.1 Övergripande struktur och definitioner

I detta kapitel kommer tekniken bakom blockkedjor att redogöras för. Blockkedjor kan som nämnt i inledningskapitlet ha många olika tekniska utformningar beroende på vilket syfte de ska uppfylla. Det finns dock vissa kritiska delar som utgör huvudkaraktäristiska drag för blockkedjor i allmänhet. I denna grundläggande redogörelse för tekniken kommer därför framförallt vikt läggas vid de fundamentala delarna som bl.a. distributionen av databasen och hur nya data kedjas ihop för att säkerställa blockkedjans integritet.[17]

Inom ramen för datavetenskap och blockkedjeteknologin används både förkortningar och en särskild terminologi som utan tidigare introduktion kan upplevas som svårförstådda. Särskilt då många vedertagna begrepp är på engelska bör dessa förklaras i korthet för att underlätta förståelsen av avsnitt i detta kapitel. En *huvudbok* är ett uttryck för en loggbok över all aktivitet som sker för hela blockkedjan. Huvudboken är ett sätt att spara alla transaktioner i kedjan, som följaktligen blir längre och längre allt eftersom nya inlägg i blockkedjan sker. Varje nytt inlägg i blockkedjan kallas ett *block* och innehåller normalt en tidsstämpel, den typ av data som blockkedjan hanterar (i Bitcoins fall transaktioner som skett de senaste minuterna) och en referens till föregående block.

Vidare distribueras huvudboken *P2P* (peer-to-peer) mellan alla *noder* i nätverket.[18] En nod är en dator eller enhet som kör mjukvaran för blockkedjan och således kan skicka eller erhålla nya uppdateringar direkt från andra noder i nätverket. En transaktionspart behöver dock inte nödvändigtvis själv köra en nod då noder behöver vara uppkopplade dygnet runt. I de flesta fall går användaren istället via andras noder (som tillhandahålls av bl.a. handelsplattformar, tjänster som erbjuder digitala plånböcker, *blockutvinnare* m.fl.) för att kommunicera sin transaktion till nätverket. Det s.k. P2P-nätverket är således en decentraliserad nätverksstruktur som utesluter behovet av en central server eller meddelandepunkt. Istället kommunicerar noderna direkt med andra noder som är online, enl. figur 1.

[17] För en komplett redogörelse för teknologin bakom blockkedjor rekommenderas Drescher, D., *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, Berkeley CA, 2017 i sin helhet.
[18] Nakamoto, S., *Bitocin: A Peer-to-Peer Electronic Cash System*, s. 3, "https://bitcoin.org/bitcoin.pdf", lydelse 2018-10-05 [cit. Nakamoto].



Figur 1. Skillnaden mellan ett centraliserat nätverk (till vänster) och ett decentraliserat P2P-nätverk (till höger). Skulle servern i bilden till vänster krascha kan ingen kommunicera längre medan i bilden till höger kan alla fortsätta kommunicera även om en av deltagarna går offline.

2.2 En distribuerad huvudbok

2.2.1 Ett exempel på hur en huvudbok kan användas

Blockkedjeteknologin har framförallt anammats inom det digitala området för transaktioner och valutor. Tar vi därför Bitcoins huvudbok som exempel består den av samtliga loggar över alla transaktioner någonsin gjorda på Bitcoins blockkedja. För att exemplifiera användningen av en distribuerad huvudbok kan vi ponera fyra vänner som under en resa bokför utlägg som gjorts (och för vems räkning) i en huvudbok som distribueras mellan dem. Innebörden är följaktligen att alla kan se hur mycket var och en ska betala varandra vid en given tidpunkt, utan att tidigare behövt växla faktiska pengar (sedlar eller mynt) vid varje utlägg. Två transaktioner i huvudboken kan således se ut som följande. Den första transaktionen säger att Björn betalat för Annas lunch om hundra kronor. Björn ligger då minus hundra kronor (ska erhålla hundra kronor vid given tid) och Anna plus hundra kronor (ska betala hundra kronor vid given tid) i huvudboken. Den andra transaktionen säger att Anna betalarför Björn bussbiljett om femtio kronor.

Björn ligger nu plus femtio kronor och Anna minus femtio kronor i den uppdaterade versionen av huvudboken. I slutändan ämnar huvudboken i förevarande fall till att säkerställa riktigheten av hur den ekonomiska situationen ser ut parterna emellan, dvs. att Anna nu är skyldig Björn femtio kronor. Så fort en ny transaktion görs, antecknas detta automatiskt på varje

persons kopia av huvudboken; den distribueras. Hade istället huvudboken inte distribuerats utan hållits centralt hos Björn hade han kunnat modifiera tidigare betalningar, lagt till nya påhittade betalningar eller tappat bort den.

2.2.2 Tillit till huvudbokens innehåll

En ovan nämnd lösning fungerar eftersom de fem vännerna litar på varandra att varje inlägg är korrekt. Varje person som har tillgång till huvudboken vet vilka de andra parterna är och att de faktiskt kommer betala tillbaka de belopp de är skyldiga. I en öppen blockkedja som Bitcoins, vilken är publik för alla att ansluta sig till, följer det sig naturligt att negativa belopp inte tillåts i form av skuld. Istället för namn som i exemplet ovan används även anonyma koder som identifiering. Det är med andra ord väldigt svårt att veta vem som står bakom en viss identitet på blockkedjan. Användandet av en distribuerad huvudbok i en öppen blockkedja medför dock många säkerhetsfrågor, särskilt frågan om tillit. Eftersom alla kan tillföra nya transaktioner måste det säkerställas att det faktiskt är rätt innehavare som gjort en transaktion. Det går dock att genom användandet av digitala signaturer verifiera de anonyma användarna i nätverket som autentiska medan sin anonymitet behålls.

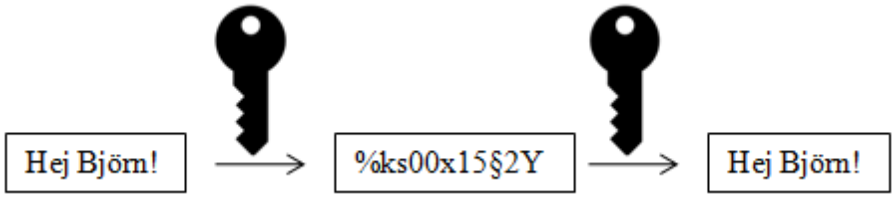
2.3 Digitala signaturer och kryptering

En kritisk del i öppna blockkedjor är verifikationen av en transaktion för att säkerställa att varje transaktion är korrekt och inte förfalskad. Om en ny transaktion stipulerar att A betalar B en viss summa är det av synnerlig vikt att veta att det är A som utfört denna transaktion och inte B som försöker tillskansa sig summan genom att förfalska transaktionen. Detta löser blockkedjor genom användandet av digitala signaturer. Digitala signaturer kan användas för att dels just signera en transaktion som sedan andra kan verifiera var signerad just av rätt person. Digitala signaturer är en kombination av kryptering och jämförelse av hashsummor.[19]

2.3.1 Symmetrisk kryptering

Inom tidig kryptografi användes ofta en så kallad *symmetrisk kryptering*. Om Anna skickar Björn ett meddelande använder hon vid en symmetrisk kryptering en algoritm som omvandlar texten till en oläslig kodsumma. Samma algoritm eller *nyckel* som används för att kryptera meddelandet används sedan för att läsa det, enl. figur 2.[20]

[19] Ds. 1998:14 s. 18 f.
[20] Jfr Drescher s. 96.



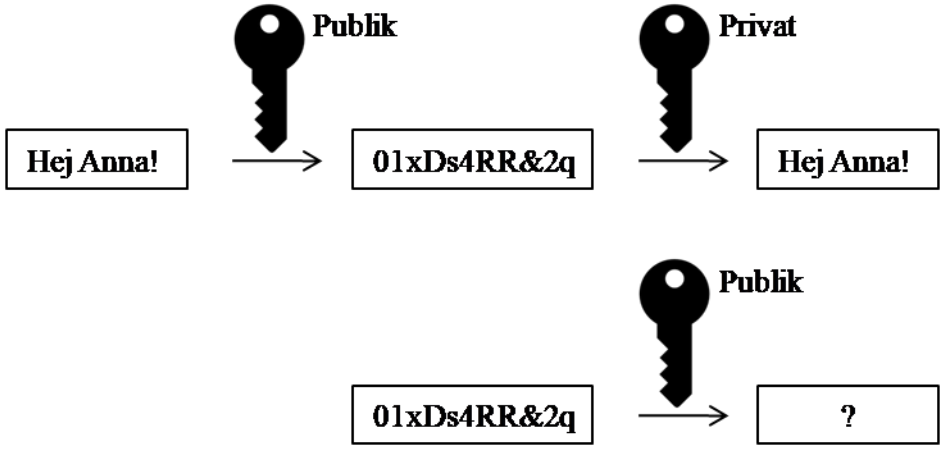
Figur 2. I en symmetrisk kryptering används samma algoritm eller nyckel för krypteringen som dekrypteringen.

En symmetrisk kryptering ter sig dock synnerligen dålig för digitala signaturer sedan det ofta är verifieringen av avsändaren som är det centrala och inte krypteringen av själva meddelandet.[21]

2.3.2 Asymmetrisk kryptering

Inom blockkedjor används istället en asymmetrisk krypteringsprocess som går till som följande. Privata och publika nycklar skapas för varje ny identitet på blockkedjan. Den publika nyckeln annonseras till nätverket för allas kännedom, medan den privata nyckeln hålls känd endast av användaren själv. Olika protokoll för att skapa digitala signaturer finns tillgängliga men det mest centrala i förfarandet är att den privata och den publika nyckeln är matematiskt länkade men omöjliga att derivera baklänges, s.k. envägskryptering. En privat nyckel för Anna är med andra ord länkad till hennes publika nyckel, utan möjlighet för någon att med hjälp av hennes publika nyckel omvänt generera hennes privata nyckel. För många blockkedjor används elliptiska kurvor som matematisk formel för att generera nyckelparet som används vid signering.[22] För Bitcoins blockkedja används Elliptic Curve Digital Signature Algorithm (ECDSA).[23] Vid användandet av en asymmetrisk kryptering för själva meddelandeinnehållet blir förfarandet till skillnad från en symmetrisk kryptering att två nycklar används.[24] Avsändaren använder då mottagarens publika nyckel för kryptering, medan mottagaren använder sin privata för att läsa meddelandet, enligt figur 3.

[21] Ds. 1998:14 s. 19.
[22] Jfr ibid. s. 21.
[23] Se vidare Wang, D., *Secure Implementation of ECDSA Signatures in Bitcoin*, s. 20 ff. "http://www.nicolascourtois.com/bitcoin/thesis_Di_Wang.pdf", lydelse 2018-10-14.
[24] Jfr Ds. 1998:14 s. 19 f.



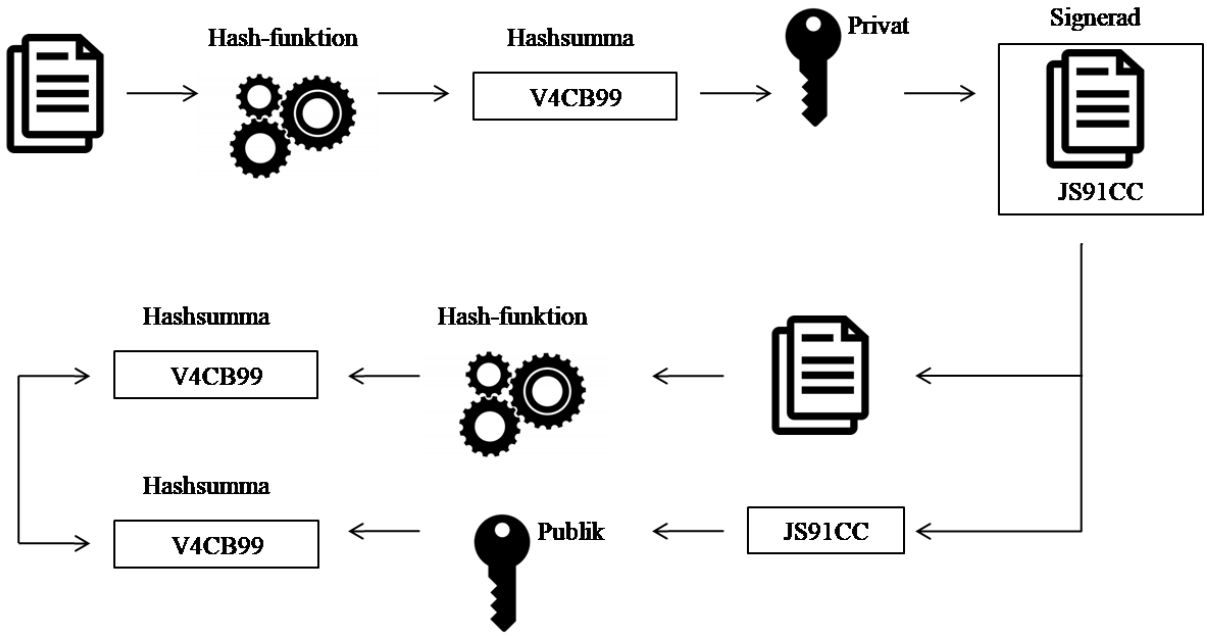
Figur 3. I en asymmetrisk kryptering av ett meddelande används mottagarens publika nyckel av avsändaren vid krypteringen. Endast mottagaren kan sedan använda sin privata nyckel för att dekryptera meddelandet.

2.3.3 Signering av transaktioner

I blockkedjor finns egentligen inget behov av att kryptera själva meddelandet i sig till en viss användare då tanken är att alla ska kunna läsa transaktionerna. Däremot är en viktig beståndsdel verifikationen att rätt person utförde transaktionen. I figur 3 ser vi att Anna kan vara säker på att meddelandet inte modifierats från dess att det skickades. Då de publika nycklarna annonseras till alla i nätverket för att kunna skicka krypterade meddelanden till Anna vet hon inte om det faktiskt var Björn eller inte som skickade meddelandet. Digitala signaturer i blockkedjor fokuserar istället med andra ord i detta avseende främst på att lösa identitetsverifikationen av avsändaren snarare än att kryptera meddelanden.

Förfarandet blir istället enligt följande. Meddelandet eller transaktionsinformationen om belopp och mottagare m.m. krypteras inte i sig. Avsändaren Björn skickar sitt meddelande genom en hash-funktion vilket genererar en hashsumma (en hashsumma är produkten av att ett meddelande körs genom en hash-funktion, vilket förklaras mer i detalj i följande avsnitt). Hashsumman tillsammans med Björns privata nyckel skapar en digital signatur som skickas tillsammans med originalmeddelandet Björn tänkt skicka. Mottagaren, övriga i blockkedjan eller Anna i detta fall, kör meddelandet genom samma hash-funktion som Björn använde vilket ger henne en hashsumma. Anna använder även Björns publika nyckel som finns publicerad med den digitala signaturen för att få fram ytterligare en hashsumma. Om meddelandets hashsumma är det samma som signaturen tillsammans med den publika nyckelns genererade hashsumma är identiteten på avsändaren verifierad som Björn, enl. figur 4.[25]

[25] Jfr även ibid. s. 23 och Drescher s. 103 ff.



Figur 4. *En asymmetrisk kryptering för att skapa en digital signatur. Transaktionen Björn gör i detta fall är inte krypterad utan består av transaktionen i ren text samt den digitala signaturen som tillägg. Steg 1 görs av Björn medan steg 2 och 3 görs av mottagaren. Om hashsumman i steg 2 och 3 överensstämmer är Björns identitet som avsändare av transaktionen verifierad.*

2.4 Block

Vi vet vid detta lag att det går att genom asymmetrisk kryptering digitalt signera data eller transaktioner vilket medför att avsändarens identitet kan verifieras även i ett anonymt nätverk. Följaktligen kan nätverket lita på att transaktionen i fråga är riktig och bör inkluderas i ett block eller att transaktionen är korrupt och inte bör ingå i ett block. En verifierad transaktion som sedermera inkluderas i ett block får egenskapen att den är låst och oåterkallelig. Nätverket inom blockkedjor är programmerat och bryr sig således endast om att transaktionen är legitim inom ramen för den digitala signaturen, och tar således inte höjd för bakomliggande faktorer till transaktionen som hot eller att fel mottagare angetts.

2.4.1 Block av ihopklumpad data

När vi nu känner till hur identiteter och nya inlägg på blockkedjan kan verifieras behöver själva strukturen hur kedjan är formad förklaras ytterligare. På ordet blockkedja hör vi att det är en länkad kedja bestående av block av data. I varje block finns, beroende på blockkedja, ett visst antal interaktioner ofta baserat på tid och datastorlek. Bitcoins blockkedjas protokoll är programmerat för att skapa sex nya block varje timme där varje block inte får överstiga en

viss datastorlek som nätverket bestämt, för närvarande 1 Megabyte (MB).[26] Vid en uppsjö av transaktioner på en gång kan därför transaktioner på vissa blockkedjor, såsom Bitcoins, ta lång tid om en transaktion inte får plats i nästkommande block. Hur bra en blockkedja lyckas överkomma sådana begränsningar brukar benämnas *skalbarhet*. En anledning till att begränsa storleken på block och tillkomsten av nya block kan vara för att minska risken för spamattacker som potentiellt skulle kunna förstoppa nätverket. Blockkedjor inom specifika användningsområden kan därför ha sin egen definition på när ett nytt block ska skapas och hur stort varje block får vara. En privat blockkedja för fastighetsregister kanske inte nödvändigtvis har samma hastighetskrav som valutor och transaktioner utan istället uppdaterar någon enstaka gång per dag.

2.4.2 Verifiering av medel vid transaktioner

Som nämnt tidigare är ett grundläggande krav för blockkedjor som bl.a. Bitcoin att användare måste inneha tillräckligt belopp för att kunna spendera då negativa belopp emellertid inte accepteras. Innehavet av belopp för att kunna spendera bekräftas genom att i varje transaktion referera tidigare transaktioner, inkommande och utgående.[27] Om Anna vill skicka 55 Bitcoin till Björn måste hennes transaktion i princip innehålla referenser till alla hennes föregående inkommande transaktioner, så kallade *inputs*, för att se att hon är god för beloppet. Bitcoins protokoll är vidare strukturerat på det sätt att en input måste användas i sin helhet vid en transaktion. Har Anna följaktligen endast en tidigare input där hon blivit tillskickad 75 Bitcoin och nu vill skicka 55 till Björn refererar hon till den tidigare inkommande transaktionen. Den utgående transaktionen, eller s.k. *output* blir 55 till Björn och 20 tillbaka till henne själv. Den tidigare transaktionen har då använts i sin helhet och Anna har nu en ny input om 20 att referera till för nästa transaktion.

2.4.3 Vad för information finns i ett block?

Eftersom publika blockkedjor är just publika där alla kan se transaktioner som sker finns det program och webbsidor som möjliggör att se exakt vilka transaktioner som är inkluderade i varje block i kedjan. Tar vi block nummer 545180 i Bitcoins blockkedja som exempel kan det

[26] Se Nakamoto s. 4. Se även Bitcoin.org, *Block Size Limit, "*https://bitcoin.org/en/glossary/block-size-limit", lydelse 2018-10-14 samt Drescher s. 66 f.
[27] Se Nakamoto. s. 2. Se även Okupski, K., *Bitcoin Developer Reference: Working Paper*, 2016, s. 35, "https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf ", lydelse 2018-10-05 [cit. Okupski].

konstateras att detta block består av 207 stycken transaktioner till en storlek om 143 Kilobyte (kB) och blev genererat klockan 15:23:36 den 10e oktober 2018.[28]

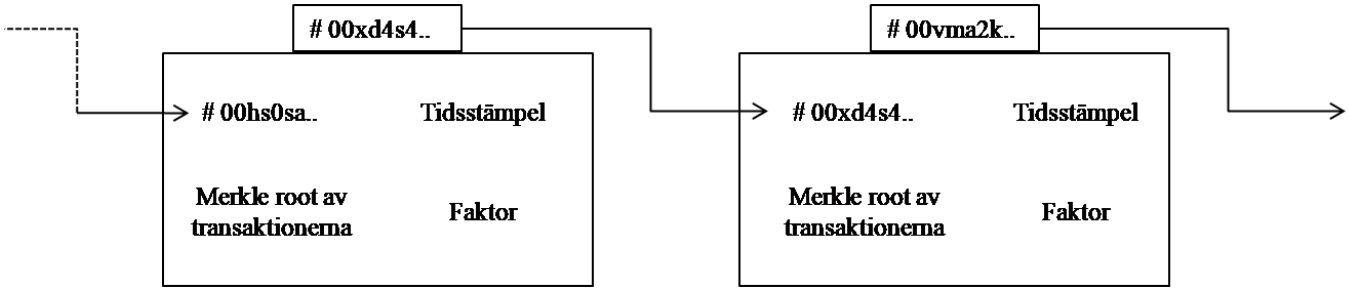
Det finns emellertid mer information i varje block än så. Varje blocks sidhuvud eller s.k. *header* innehåller viss metadata; vilken version av mjukvaran som används, en referens till föregående blocks hashsumma, transaktionerna i blocket, tidsstämpel och ett slumpmässigt värde (även kallat *salt*).[29] Denna information, körd två gånger genom en hash-funktion blir det nuvarande blockets hashsumma, som sedan kan användas av nästa block som referens. Just hashsumman är särskilt viktig för att skapa själva kedjan som förhindrar dubbla transaktioner eller s.k. *double spendings*.[30] Inte förrän transaktionen är inlagt i ett block som blivit länkat i kedjan är föregående input för varje transaktion att betrakta som använd. En som handlar i ond tro skulle annars kunna använda samma input till två outputs. Det är här blocken kommer in och säkrar ordningen på transaktionerna i kedjan, så att det går att veta vilka transaktioner som skett före andra, för att på så vis ignorera redan använda inputs.

2.5 Upprättande av kedjan

Alla aktiva blockutvinnare (s.k. *block-miners*) på blockkedjenätverket kan själva välja att skapa ett nytt block av temporära transaktioner som skickats från noder i nätverket men som ännu inte är inlagda i ett block, s.k. *väntandes transaktioner*. Flera blockutvinnare komponerar här sina egna förslag till vilka väntande transaktioner som ska bilda nästa block i kedjan. I detta stadium är det endast fråga om förslag till nästa block och här kommer funktionen av det slumpmässiga värde in som finns i varje block-header. För att accepteras som nästa bekräftade block måste skaparen av blocket ändra det slumpmässiga numret om och om igen till dess att blockets hashsumma understiger ett särskilt värde som bestäms dynamiskt av blockkedjans programvara beroende på hur stor belastning det är på nätverket och hur många som försöker komponera nya block. Eftersom en ändring av endast en siffra skapar en väsentligt annorlunda hashsumma kräver det mycket datorkraft eller s.k. *Proof-of-Work* för att lyckas skapa ett nytt block som matchar nätverkets krav. Denna process benämns ofta som *mining* då den som

[28] Blockchain.com, *Block #545180*, ”www.blockchain.com/btc/block/000000000000000000001084d6d26cd688036887daaa505afbf83ad677c9b67fc6”, lydelse 2018-10-09.
[29] Se Okupski, s. 5.
[30] Se ibid. s. 35. För vidare redogörelse av problematiken och lösningen kring *double spendings* se Drescher s. 49 ff.

lyckas gissa rätt gynnat blockkedjan och erhåller en viss monetär belöning i form av kontrollerad inflation och syftar till att säkerställa integriteten för blockkedjan.[31]



Figur 5. *Ett exempel på en blockkedja. Varje block-header innehåller föregående blocks hashsumma, tidsstämpel, en Merkle root av blockets transaktioner samt en slumpmässig faktor som gissas fram. Försöker någon ändra ett enda tecken i ett föregående block medför det att hashsumman för det blocket ändras väsentligen vilket medför att nästa block i kedjan inte längre stämmer. I exemplet kan noteras att kedjan för tillfället har # 00 som inledande målvärde för att accepteras som nästa block. Den slumpmässiga faktorn prövas därför gång på gång till dess att hashsumman börjar på # 00.*

Sannolikheten att flera block samtidigt når under målvärdet för att bli nästa validerade block är väldigt liten, men finns dock emellertid. Det är därför inom publika blockkedjor den längsta kedjan anses som den legitima.[32] Har två olika block samtidigt genererat en hashsumma som är under målvärdet kommer de båda distribueras till nätverket som kan välja vilken de vill använda för att beräkna nästa block. Hinner någon skapa nästföljande block med hjälp av den ena av de två samtidigt skapade blocken är det nu den längsta kedjan och anses den korrekta. Nätverket sparar således de båda blocken i väntan på att se vilket som kommer användas till nästkommande block.[33] Inom vissa blockkedjor som Bitcoins kan det därför konstateras att ju äldre ett block är desto ”säkrare” är de transaktionerna, eftersom det nyaste blocket för en person kan ändras i det fall någon annan lyckas skapa fler block i rad baserat på ett annat block som det nyaste blocket.

2.5.1 Samarbetsparadoxen för blockutvinnare

Eftersom det krävs enorm mängd datorkraft för att räkna ut dessa pussel som krävs för att få skapa nästa block finns så kallade *mining pools* som är samling av flera noder som arbetar

[31] Se Berentsen, A & Schär, F, *A Short Introduction to the World of Cryptocurrencies*, s. 5 f., “files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf”, lydelse 2018-10-12. Jfr även Drescher s. 89 ff.
[32] Se Nakamoto s. 3 f. Se även Okupski s. 35 f.
[33] Se Nakamoto s. 3.

tillsammans. Det är en sorts organisering för att dela på chansen att få lägga in nästa block, och således dela på den belöning det medför. Den längsta kedja en enskild mining pool uppnått är sex block i rad, vilket dock är väldigt ovanligt. I skrivande stund är således block som är sex steg eller fler tillbaka att anse som definitivt säkra, men då det fortfarande är så pass ovanligt att en enskild entitet lyckas generera sex block i rad kan färre än så anses relativt säkra redan efter någon eller några bekräftelser. Det är emellertid något problematiskt att som enskild entitet ta total dominans av bestämmandet för nya block. Det skulle krävas mer än 50 procent av samtlig datorkraft på blockkedjans nätverk för att med sannolikhet kontrollera följden. En nod har dock sällan något incitament av att ingå i en så pass stor mining pool eftersom om 50 procent uppnås skulle blockkedjan anses vara centralt dominerad och följaktligen opålitlig. Samtidigt som samarbete ökar chansen att någon i samarbetet gissar rätt och belöningen delas dem emellan påverkar det dynamiken över förtroendegraden för blockkedjan, en sorts paradox.

2.6 Användandet av hash-funktioner

Hittills har kryptografiska algoritmer eller hash-funktioner endast förklarats i korthet och dess användningsområde kan vara något svårförståelig. För Bitcoins blockkedja används i huvudsak SHA-256 (Secure Hash Algorithm) som är en algoritm som omvandlar text och siffror till en bestämd 256-bitars längd.[34] Det är en envägsfunktion vilket betyder att det inte går att dekryptera utan hashsumman som är resultatet används istället som ett jämförande medel.[35] Exempelvis kan lösenord som körs genom SHA-256 sparas som hashsumma. Vid senare inloggning körs det lösenord användaren skriver in genom samma algoritm, omvandlas till hashsumma och jämförs med den sparade hashsumman som finns. På detta sätt kan data som annars hade varit känslig, så som lösenord, sparas och jämföras utan att faktiskt sparas i ren text. Den matematiska förklaringen till hur SHA-256 fungerar är tämligen komplicerad.[36] Emellertid är det intressant att förstå att olika blockkedjor kan ha olika kryptografiska algoritmer beroende på hur de är utformade och vilket behov de används för. För Bitcoins blockkedja används SHA-256 i kombination med ett slumpmässigt värde för att det tar datorkraft och tid att generera varje hashsumma vilket bidrar till en ökad säkerhet då det tar lång tid att försöka ändra blockkedjan. Det finns blockkedjor som kan påvisa snabbare transaktionstider med

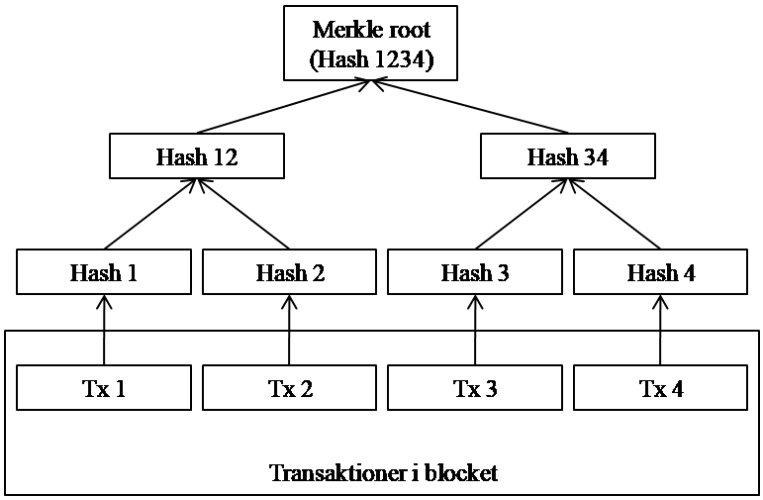
[34] Se ibid. Jfr även Federal Information Processing Standards Publication, *Secure Hash Standard (SHS)*, s. 3, ”nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf”, lydelse 2018-10-14 [cit. *Secure Hash Standard (SHS)*].
[35] Se Ds. 1998:14 s. 21 ff. Se även Merkle, R.C., *Secrecy, Authentication, and Public Key Systems,* Technical Report No. 1979-1, s. 11 ff., “www.merkle.com/papers/Thesis1979.pdf”, lydelse 2018-10-14 [cit. Merkle].
[36] Se *Secure Hash Standard (SHS)* s. 21 ff.

snabbare kryptografisk algoritm som ändå kan klassas som säkra.[37] En mindre krävande kryptografisk algoritm kan i vissa fall anses lättare att knäcka genom s.k. *bruteforce-attack* där attackeraren provar olika inmatningar om och om tills rätt hashsumma matchas. Det ska dock nämnas att de blockkedjor som inte är beroende av slumpmässiga värden som ett begränsande medel inte nödvändigtvis har samma behov av styrka i krypteringen.[38] Av denna anledning används flera olika kryptografiska algoritmer för respektive blockkedja, där ju längre hashsumma desto svårare att gissa sig fram till rätt ingångsvärde. De vanligaste kryptografiska algoritmerna har därför ofta inte kortare hashsumma än 128, 256 eller 512 bitar, där en 512-bitars hashsumma följaktligen tar längre tid att processa än en 128 eller 256 bitar lång hashsumma.

2.6.1 Kondensering av data genom hash-funktioner

Ett bra exempel på hur SHA-256 eller andra kryptografiska algoritmer verkar i blocken av data på blockkedjor är hur de används för att indexera transaktioner i blocken. Som nämnt finns i varje block-header metadata om alla transaktioner i blocket vilket utgör en del i blockets hashsumma. Detta är emellertid endast ett kondensat eller digitalt fingeravtryck av de transaktioner som är inkluderade i blocket, en s.k. *Merkle root*.[39] Det som benämns *root* i ett Merkleträd är den högsta gemensamma hashsumman för transaktionerna enligt figur 6. Eftersom de kryptografiska algoritmerna alltid genererar samma hashsummor för exakt samma ingångsvärden kan vi med hjälp av den slutgiltiga hashsumman bekräfta vilka transaktioner som ingår, utan att i blockets header behöva lista samtliga transaktioner. Användningen av ett Merkleträd är således egentligen ett sätt att spara datautrymme i blockkedjan, som ett koncentrerat fingeravtryck av flera transaktioner.[40]

[37] LeMahieu, C., *Nano: A Feeless Distributed Cryptocurrency Network*, s.1 ff., "nano.org/en/whitepaper", lydelse 2018-10-09.
[38] Ibid. s. 5.
[39] Se Merkle s. 41 ff.
[40] För vidare användningsområde och redogörelse för kondensering av data se Drescher s. 88 f.



Figur 6. *Ett exempel på ett Merkleträd. Transaktionerna i blocket hashas två och två tills endast en hashsumma finns kvar. Kondensatet av alla transaktioner är unikt för just dessa transaktioner. Ändras någon transaktion eller innehåll i transaktionerna stämmer inte längre den slutgiltiga hashsumman, även kallad Merkle root.*

2.6.2 Ett exempel på användning av hash-funktioner

Hash-funktioner kan användas för alla typer av digital data. Bilder, ljud och video är även de digital kod som kan köras genom en hash-funktion för att generera ett digitalt fingeravtryck som sedan kan användas för att exempelvis säkerställa äktheten av ett original.[41] Ett projekt under Center of Innovative Finance vid University of Basel lanserade i april 2018 en tjänst för diplomverifiering där studenters betyg och diplom lagras på en blockkedja till skillnad från de traditionella system för betygsutdrag som sker från universitetens databas.[42] Blockkedjan säkerställer för både arbetsgivare, universitet och studenterna själva att diplomen är korrekta och inte har ändrats. Vid examen kan universitetet lägga till ett block på blockkedjan innehållandes en students diplom som hashsumma. En arbetsgivare som av en student blivit tillskickad en pdf-fil med examensbeviset kan sedan köra dokumentet genom samma SHA3-256 hashfunktion och följaktligen på blockkedjan verifiera dess autenticitet om hashsumman stämmer överens med den på blockkedjan inlagda. Arbetsgivaren kan då veta att den arbetssökande studenten inte har ändrat i det digitala dokumentet.

[41] Jfr figur 4.
[42] Schär, F., *Certificates based on Blockchain Technology*, "cif.unibas.ch/fileadmin/user_upload/cif/press_release_EN.pdf", lydelse 2018-10-10.

2.7 Skilda förutsättningar för privata och publika blockkedjor

När vi nu vet de tekniska förutsättningarna för hur blockkedjor, främst publika, fungerar kan nämnas att de skiljer sig från privata blockkedjor på flera väsentliga områden. Medan blockkedjestrukturen med block och kryptografiska hash-funktioner emellertid är densamma finns exempelvis möjligheten att ändra information i en privat kedja som inte på samma sätt finns i en publik kedja. Från den tekniska redogörelsen bör bäras med att kedjestrukturen möjliggör att transaktioner eller överföringar av data inordnas i ett kronologiskt register som vi, utan att ha tillit till andra i systemet, kan enas om.[43] I en privat blockkedja finns inte detsamma behov. Behovet av privata blockkedjor har å andra sidan ofta ifrågasatts då en traditionell databas ofta är både snabbare och lättare integrerad om det ändå rör sig om ett privat transaktionssystem. I en semi-privat blockkedja där exempelvis alla kan ha insyn men inte medverka går det att på förhand bestämma vilka som ska få medverka och på vilka villkor.

Vidare kan privata och semi-privata blockkedjor lättare enas om en manipuleringspolicy av blockkedjan. Till skillnad från de publika blockkedjorna behövs inte nödvändigtvis samma konsensus för att ändra blockkedjan. Som vi noterat tidigare behövs att varje block ”räknas om” i det fall ett tidigare block ändras. I en privat kedja kan detta låta göras i lugn och ro utan att någon tävling mot andra blockutvinnare som vill räkna ut nästa block pågår. Följden blir att privat hanterade blockkedjor kan ändra data i blockkedjan eftersom det inte finns samma skyddsmekanism mot förändringar som i de publika kedjorna. De publika blockkedjorna har på så vis den största utmaningen sedan information som en gång lagrats endast med stor svårighet kan ändras.

En annan skillnad mellan de privata projekten och de publika blockkedjorna är att publika blockkedjor ofta handlar om allmänna transaktioner medan de privata kedjorna ofta kan hantera mer ”känslig data” som register, upphovsrätter eller transaktioner banker emellan. Ett exempel är det blockkedjeprojekt som Lantmäteriet utvecklar som potentiellt skulle kunna ändra hur vi genomför fastighetstransaktioner.[44] Det nämns i rapporten att projektet tänks omfatta en privat blockkedja och en publik där personer kan interagera, men att själva fastighetsregistret ändå bestäms av myndigheter som är de enda som kan lägga in de nya transaktioner-

[43] Okupski s. 35.
[44] Lantmäteriet, *Framtidens husköp i blockkedjan,* ”www.lantmateriet.se/contentassets/ee30ed78dcdb4dd698cf454001369cf8/blockkedjan-framtidens-huskop.pdf”, lydelse 2018-10-11.

na i kedjan.[45] Det finns således poäng med att kedjan är publik för insyn och verifikation, medan vem som helst inte kan påverka listans funktionalitet och själv lägga in nya block.

2.8 Sammanfattning av blockkedjeteknologin

Innan vi går vidare och ser på de rättsliga utmaningarna för blockkedjeteknologin förs här en kort sammanfattning. Sammanfattningen är tänkt att summera materialet i detta kapitel för att de viktigaste momenten i teknologin kan bäras vidare i tanken till den juridiska argumentationen. Initialt kan nämnas den distribuerade huvudboken som sprids mellan alla användarenheter på blockkedjan. Varje individ har alltså insyn i den kompletta loggboken över alla transaktioner som skett. På detta sätt är databasen distribuerad till skillnad från traditionella databaser som är centraliserade. Digitala transaktioner kräver vidare digitala signaturer. Detta sker genom asymmetrisk kryptering vilket genererar en privat nyckel och en publik nyckel. Den publika nyckeln används av andra i nätverket när någon vill skicka dig en transaktion, medan den privata används av dig själv för att signera dina egna utgående transaktioner. En transaktion kan således bekräftas som legitim om transaktionens hashsumma överensstämmer med din publika nyckel och signaturs hashsumma.

Väl i själva blockkedjan har vi block som består av ihopklumpade transaktioner som skett den senaste tiden. Varje block har en referens till föregående block vilket skapar den kronologiska följden i systemet. För att ett nytt block ska kunna accepteras av nätverket som nästa giltiga block krävs det datorkraft för att lyckas generera en hashsumma som understiger det målvärde nätverket dynamiskt bestämt. Det krävs generellt sett mycket datorkraft för att generera ett nytt block. När flera block skapats på rad försvåras möjligheten att ändra ett tidigare block, sedan en dator då behöver räkna om samtliga block efter det i vilken ändringen skedde. En sådan uträkning tar tid, under vilken ett ytterligare nytt block säkerligen skapats som nu gäller som den korrekta kedjan eftersom den längsta alltid anses vara den rätta. Det är på detta sätt som blockkedjor skapar sitt förtroende då det är ytterst svårt och kostsamt att försöka manipulera kedjan.

En ytterligare viktig komponent är de kryptografiska algoritmerna som används för att skapa digitala fingeravtryck av data. All data kan köras genom en kryptografisk algoritm som genererar en bestämd längd bokstäver och siffror som fungerar som ett fingeravtryck för den ursprungliga datan. Slutligen kan även nämnas att blockkedjor kan ha olika former beroende på ändamål. Huruvida en blockkedja är publik eller privat kan drastiskt förändra möjligheten att

[45] Ibid. s. 7 och s. 12 ff.

bestämma och ändra i blockkedjans innehåll. En privat blockkedja bestämmer själv vilka som ska ha inflytande över nya block och innehåll, medan publika ofta har en stark konsensusregel i takt med att nya block tävlas för att läggas till vilket förhindrar enskilda parter från att manipulera innehållet.

3. GDPR

3.1 Inledande om den nya dataskyddsförordningen

Den nya dataskyddsförordningen ersätter det äldre EU-direktivet 95/46/EG, dataskyddsdirektivet, som föranledde den svenska personuppgiftslagen (1998:204, PuL).[46] Den nya dataskyddsförordningen blev tillämplig från den 25 maj 2018. Förordningen syftar till att ge ett enhetligt skydd för enskildas grundläggande rättigheter och friheter inom EU i takt med att integritetsfrågor blir allt viktigare och vanligt förekommande. Den personliga integritetens vikt framgår tydligt av artikel 1 samt skäl 1 och 2 i förordningen som hänvisar till både EU-stadgans artikel 8.1 och Funktionsfördragets artikel 16.1 som båda föreskriver en rätt till skydd för personuppgifter. Även Europakonventionen som gäller som lag i Sverige omfattar i artikel 8 rätten till skydd för privatliv.[47] Integritet är emellertid ett begrepp som får anses vara svårt att fullständigt täcka med en beskrivning.[48] Det får istället förstås som ett uttryck med ett brett omfång som ändras över tid i takt med att informationstillgängligheten ökar. För svensk del infördes 2010 i regeringsformen (1974:152) 2 kap. 6 § 2 st. för var och en gentemot det allmänna ett skydd mot betydande intrång i den personliga integriteten.[49]

Den nya dataskyddsförordningen är en förordning och således direkt tillämplig och rättsligt bindande för medlemsstaterna. Det föregående dataskyddsdirektivet gav i egenskap av direktiv inte samma enhetlighet som den nu gällande förordningen förväntas skapa.[50] Genom att EU väljer att inskränka medlemsstaternas möjlighet att själva utforma bestämmelserna förstås att man vill uppnå ett ännu mer enhetligt regelverk än vad dataskyddsdirektivet tidigare har föranlett.[51] Medan den nya dataskyddsförordningen i stort bygger på det föregående dataskyddsdirektivet kan rättigheter och ökad kontroll över sina personuppgifter pekas ut som de mest väsentliga förändringarna.[52] Det handlar om bl.a. införandet av konsekvensanalyser för om en viss behandling kommer att leda till högre risk för enskildas rättigheter, en tydligare rätt till radering av personuppgifter och krav på inbyggt dataskydd.[53]

[46] Artikel 94 och 99 GDPR.
[47] Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[48] SOU 2008:3 s. 244 f. Se även SOU 2016:7 s. 65 f.
[49] Lag om ändring i regeringsformen (2010:1408).
[50] Skäl (9) GDPR.
[51] Skäl (13) GDPR.
[52] Se prop. 2017/18:105 s. 19 f.
[53] Ibid.

I detta kapitel utreds närmare det materiella tillämpningsområdet för GDPR, begrepp som personuppgifter och personuppgiftsansvarig samt databehandling inom ramen för vad som kan vara relevant för blockkedjor. Kapitlet syftar till att utreda materiellt viktiga bestämmelser och begrepp för att sedan kunna analysera dess kompabilitet med blockkedjor. Analys och slutsatser över kompabiliteten mellan det de utredda bestämmelserna förs således inte i detta kapitel utan i kapitel 4.

3.2 Allmänt om tillämpningsområde och definitioner

3.2.1 Kort om det materiella tillämpningsområdet

I artikel 2 i dataskyddsförordningen uppställs det materiella tillämpningsområdet för förordningen. I första punkten nämns att förordningen ska tillämpas på behandling av personuppgifter som företas helt eller delvis på automatisk väg samt annan behandling än automatisk av personuppgifter som ingår eller kommer ingå i ett register. Det är många begrepp i denna artikel som måste redas ut för att kunna bestämma tillämpningsområdet. Det ska vara fråga om en *behandling* och att behandlingen ska avse *personuppgifter*. Det ska även vara fråga om en behandling som företas helt eller delvis på *automatisk väg* eller *annan behandling än automatisk* om personuppgifterna *ingår eller kommer ingå* i ett *register*. Förordningens artikel 4 försöker definiera många av dessa begrepp. Det är dock inte helt klart exakt vad som exempelvis är en personuppgift eller vad som ska ses som en behandling i varje enskilt fall. Dessa definitioner behöver därför utredas mer ingående. Tillämpningsområdet torde dock vara, så länge nyckelordet personuppgift aktualiseras, väldigt stort och det är få användningsområden som inte täcks in av begreppet *behandling*.[54]

Ett undantag finns i artikel 2.c för behandling som sker som ett led i verksamhet av ren privat natur eller som har samband med hushållet. Denna undantagsbestämmelse är viktig att belysa då det finns många situationer i vardagen där personuppgifter behandlas men som betraktas vara av privat natur och således undantas från förordningen. Exempel kan tänkas vara privata kontaktlistor, mejllistor eller dagböcker som nämns i skäl 18 till förordningen. Värt att ha i åtanke är att även situationer av ekonomisk karaktär kan omfattas inom den privata undantagsregeln. Exempelvis är utlägg för en middag som antecknas med personuppgifter motiverade av ekonomiska skäl, men gör dem inte nödvändigtvis kommersiellt präglade och kan således fortfarande falla in under undantagsbestämmelsen för privat verksamhet.

[54] Klamberg, M., Magnusson Sjöberg, C. & Öman, S., *Skydd av personlig integritet och informationsfrihet*, i Magnusson Sjöberg (red.), s. 176.

3.2.1 Utökat territoriellt tillämpningsområde

Utöver det materiellt tillämpbara området måste även det territoriella tillämpningsområdet beaktas. Här är dataskyddsförordningen tämligen otvetydig i sin formulering men det kan i praktiken fortfarande vara svårt att med säkerhet i alla fall klargöra huruvida förordningen är territoriellt tillämpbar. I artikel 3.1 i förordningen nämns inledningsvis att förordningen ska tillämpas på behandling av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig som är etablerad i unionen. Här tas vidare ingen hänsyn till om själva behandlingen sker inom EU eller inte, så länge det sker inom ramen för en verksamhet som bedrivs av någon som är etablerad inom EU.

En utökning från det föregående dataskyddsdirektivet är att förordningen enligt artikel 3.2 även ska tillämpas på behandling av personuppgifter som avser personer som befinner sig i EU även om den utförs av en personuppgiftsansvarig som inte är etablerad i unionen om behandlingen knyter an till varor eller tjänster som bjuds ut till personer inom EU eller om behandlingen har anknytning till övervakning av beteende som sker inom EU.[55] Den här utökningen är en väldigt breddande kompetens som har blivit ifrågasatt. Det betyder nämligen i praktiken att EU-förordningen träffar även behandling av uppgifter som sker i en stat utanför EU om det finns någon verksamhetskoppling till unionen. Framförallt kan tjänster på nätet och digitala varor vara svårtolkade huruvida dem utbjuds till personer registrerade i unionen eller inte samt hur gränsdragningen för var ett beteende sker. Exempelvis kan ett klick på min dator å ena sidan tyckas vara ett beteende som sker hos mig inom unionen. Beteendet kan å andra sidan tolkas på så sätt att det endast får betydelse då jag är uppkopplad mot en server i ett annat land där klicket får sammanhang och faktisk betydelse.

3.3 Personuppgifter

Vad som är en personuppgift definieras i artikel 4 i GDPR. Här nämns att en personuppgift är alla upplysningar som avser en identifierad eller identifierbar fysisk person varvid en identifierbar fysisk person avser någon som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som namn, personnummer m.m. eller en eller flera faktorer som är specifika för den fysiska personens identitet. Identitet kan även som nämns i definitionen vara den fysiska personens ekonomiska identitet, vilket kan komma vara särskilt relevant för publika blockkedjor i följande diskussion.

[55] Jfr prop. 2017/18:105 s. 19.

Särskilt intressant är de indirekta identifikationsgrunderna. I artikel 4 nämns alltså inte enbart direkta identifierare som namn, personnummer, lokaliseringsuppgift eller onlineidentifikationer utan även andra indirekta identifierare. Här kan nämnas som exempel dynamiska IP-adresser (Internetprotokoll).[56] EU-domstolen meddelade i mål C-582/14 Breyer v. Bundesrepublik Deutschland att en dynamisk IP-adress är att anse som en indirekt personuppgift enligt det föregående dataskyddsdirektivet som har samma lydelse avseende indirekta personuppgifter. Detta eftersom den dynamiska IP-adressen tillsammans med internetleverantörens ytterligare uppgifter om beställaren, som för tillfället förfogar över den dynamiska IP-adressen, gör det möjligt att identifiera den registrerade. Målets dom är en utökning från mål C-70/10 Scarlet Extended SA. v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) vilket endast tog sikte på statiska IP-adresser där domstolen ansåg att dessa utgör skyddade personuppgifter eftersom de gör det möjligt att exakt identifiera internetanvändarna.

3.3.1 Systemidentifikationsnummer som personuppgift

Varför är då IP-adresser särskilt intressant att utreda i denna del? IP-adresser är numeriskt uppbyggda och skiljer sig således från namnuppgifter. Dock är personnummer även de numeriska till karaktären. Personnummer är emellertid statligt reglerade och tilldelade medan IP-adresser är reglerade och tilldelade genom internetorganisationer. Det måste således förstås att ursprunget inte har någon betydelse, om det är statligt registeruppförande eller ett ideellt infrastrukturellt register. Som nämndes i mål C-528/14 är dock en IP-adress att anse som personuppgift med indirekt karaktär sedan den tillsammans med leverantörens uppgifter kan identifiera användaren. En användares IP-adress kan alltså ingå i ett system och där utgöra en indirekt personuppgift i det fall ytterligare uppgifter gör det möjligt att hänföra den till en fysisk person. Vad händer då i ett anonymt system som inte kräver registrering eller som helt enkelt inte sparar användarinformation? Jämförelsen med IP-adresser blir då inte lika relevant eftersom IP-adresser tilldelas genom reglerade internetorganisationer och leverantörer som sparar information om den registrerade. Ponera istället att vi har ett publikt system där varje anonym identitet får ett identifikationsnummer tilldelat till sig. Utan ett krav på registrering bör det dock på samma sätt rimligen vara fråga om en indirekt personuppgift om det anonyma identifikationsnumret tillsammans med ytterligare upplysningar gör det möjligt att identifiera personen bakom numret.

[56] Klamberg, M., Magnusson Sjöberg, C. & Öman, S., *Skydd av personlig integritet och informationsfrihet*, i Magnusson Sjöberg (red.), s. 177.

3.3.2 Indirekta personuppgifter grundat på beteende och efterforskning

Frågan är då om ett beteende kan utlösa en indirekt personuppgift? Om vi vet att ett företag alltid företar en utbetalning av löner vid en viss tidpunkt månatligen kan vi i ett publikt betalningsnätverk efterforska betalningsströmningarna. Ganska snart genom transaktionsgranskning och korshänvisning kan vi börja sammankoppla dessa till synes anonyma identifikationsnummers riktiga ägare. I andra fall kan vi ponera att användarna själva går ut med att man gjort en viss transaktion eller att man är ägare av ett visst nummer. Tar vi traditionella banker som håller liknande transaktioner osynliga för allmänheten röjs på innehavaren av ett konto så fort en faktura eller inbetalningskort utställs. Även det faktum att kännedom om att en viss person står bakom ett nummer kommit till stånd på olaglig grund, exempelvis genom dataintrång eller i strid mot sekretessavtal, bör inte spela någon roll i denna bedömning. Det vore en väldigt juridiskt snårig lösning som knappast skulle fungera i praktiken om endast information som blivit känd på laglig väg var personuppgiftsgrundande i den bemärkelsen.

3.3.3 Indirekta personuppgifter till följd av tredjepartsregistrering

Vidare bör nämnas tillfällen där tjänster eller en tredjepart registrerar uppgifter vid användandet av ett anonymt betalningssystem som Bitcoin. Om det i en tredjepartstjänst registreras personuppgifter för en produktleverans får en koppling anse ha gjorts till det tidigare anonyma identitetsnumret i betalningssystemet. I ett sådant fall måste det anonyma identifikationsnumret utgöra en personuppgift likt en IP-uppgift. Frågan är dock om identifikationsnumret i alla lägen då är att betrakta som personuppgift. Det går exempelvis i detta fall att indirekt efterforska vem som står bakom numret med hjälp av den tredjepartstjänsten där användaren registrerat sin adress för en leverans. Det går dock emellertid endast för den tredjepartstjänsten som innehar denna koppling. Frågan är om det är av relevans för att uppgiften ska anses vara en indirekt personuppgift i förordningens mening. Det får i det närmaste antas att så är fallet med hänvisning till den slutsats som EU-domstolen gör i de båda målen gällande IP-adresser ovan.[57] Likt omständigheterna i de båda fallen har en specifik leverantör informationen om vem som IP-adressen är kopplad till. Ingen annan har den informationen, ändå är IP-adressen att se som personuppgift för andra i sin behandling. Med detta resonemang borde slutsatsen bli att ett identifikationsnummer i ett anonymt system som inte kräver registrering måste anses som indirekt personuppgift i det fall att identifikationsnumret använts i ett annat sammanhang

[57] Mål C-582/14 Breyer v. Bundesrepublik Deutschland och C-70/10 Scarlet Extended SA. v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

varvid identiteten röjts. Dock är det utan vägledning svårt att avgöra hur allmänt känt ett innehav av sådan uppgift behöver vara.

3.3.4 Anonyma protokoll och behandling som rimligen kan förväntas

Samtidigt som förordningen i vissa fall är förståelig om vad en indirekt personuppgift kan anses vara finns många frågetecken kvar. Av resonemanget ovan följer även att till synes oidentifierbara identitetsnummer från andra protokoll än IP, vilka protokoll inte är allmänt kända, ändå bör betraktas som personuppgifter om någon har information registrerad om vem som står bakom identitetsnumret. Ett sådant resonemang kan tänkas gå långt bortom de gränser förordningen tänkt omfatta i det fall den personuppgiftsansvarige behandlar uppgifter som inte kan förväntas utgöra indirekta personuppgifter. Tankeexemplet kan dock komma att misslyckas uppfylla skäl 26 i förordningens krav på att hjälpmedlet för att identifiera den aktuella personen *rimligen ska kunna komma att användas*.[58] Som generaladvokaten nämner ska så inte vara fallet om det exempelvis skulle kräva orimliga resurser i form av tid och kostnad och att risken för identifiering i praktiken är försumbar.[59] Här nämner generaladvokaten explicit det faktum att det i princip alltid kan föreställas ett scenario där tredje man har tillgång till relevanta uppgifter för att en användare ska kunna identifieras. Det skulle i ett sådant fall vara omöjligt att göra skillnad på olika hjälpmedel för indirekt personuppgifter.

3.4 Personuppgiftsansvarig

3.4.1 Allmänt personuppgiftsansvar

Med den nya dataskyddsförordningen infördes genom artikel 4 en ny roll, s.k. *personuppgiftsansvarig* eller *controller* på engelska som ersätter den äldre motsvarigheten *registeransvarig* i dataskyddsdirektivet.[60] Den personuppgiftsansvarige avser en fysisk eller juridisk person som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige är genom artikel 5.2 ansvarig för att grundläggande principer vid behandling i punkt 1 i samma artikel efterlevs. Det kan handla om bl.a. laglighet i 5.1.a där den personuppgiftsansvarige måste säkerställa att behandlingen sker på ett lagligt sätt eller korrekthet i 5.1.d där den ansvarige måste korrigera eller radera felaktiga personuppgifter utan dröjsmål.[61] Det är ofta ganska tydligt för en användare att få veta vem eller vilket företag som är personuppgiftsansvarig, särskilt som artikel 13 i förord-

[58] Jfr även p. 42-49 i mål C-582/14 Breyer v. Bundesrepublik Deutschland.
[59] Ibid. p. 46. Se även p. 67-70 i generaladvokatens förslag till avgörande i samma mål, C-582/14 Breyer v. Bundesrepublik Deutschland.
[60] Jfr artikel 2(d) i dataskyddsdirektivet.
[61] Jfr även här främst artiklarna 16-18 GDPR.

ningen stipulerar krav på information som ska tillhandahållas den registrerade. Det kan dock finnas situationer där personuppgiftsbehandlingen utformats på ett sätt som inte står i enlighet med GDPR. Eftersom rollen som personuppgiftsansvarig medför ansvar och en rad skyldigheter är det följaktligen viktigt att tidigt utreda vem som är personuppgiftsansvarig i det enskilda fallet. Vid prövning måste domstolen fastställa vem, om GDPR anses tillämpligt, som är personuppgiftsansvarig.

3.4.2 Begränsning av ansvarsöverlåtelse

En viktig del i förståelsen kring den personuppgiftsansvariges ansvar är att behandlingen i sig kan överlåtas till ett *personuppgiftsbiträde*. Ansvaret för behandlingen kan dock inte överlåtas. Ett företag kan alltså överlåta personuppgiftsbehandlingen till en tredje part. Om ett företag givit instruktioner till ett personuppgiftsbiträde angivande vad och hur behandlingen ska ske är det rimligen även huvudmannen, företaget, som bär ansvaret för behandlingen. Den personuppgiftsansvariges allmänna skyldigheter framgår av bl.a. artikel 24 medan artikel 25 i förordningen stipulerar bl.a. ett krav på inbyggt dataskydd som standard eller på engelska *privacy by design*.[62] Beteckningen personuppgiftsansvarig användes redan i den svenska implementeringen av dataskyddsdirektivet genom PuL. Utöver den bokstavliga ändringen från registeransvarig till personuppgiftsansvarig, vilket skulle indikera ett något utvidgat omfång, är innebörden av rollen emellertid densamma; att huvudansvaret för att personuppgiftsbehandlingen går rätt till.[63] Även om beteckningen registeransvarig för tankarna till att omfatta endast register har personuppgiftsansvaret även i det tidigare dataskyddsdirektivet ansetts vara vidsträckt för behandling av personuppgifter.[64]

3.4.3 Gemensamma personuppgiftsansvariga

En annan viktig aspekt är att artikel 26 i GDPR tillåter flera gemensamma personuppgiftsansvariga. Artikeln och även skäl 79 föreskriver även att det krävs ett tydligt fastställande av vem som bär vilket ansvar enligt förordningen i det fall flera personuppgiftsansvariga gemensamt bestämmer ändamål och medel för behandlingen. Artikel 26 medför ett krav att i det fall fler parter är gemensamt personuppgiftsansvariga ett avtal dem emellan ska upprättas där det tydligt framgår vem som ansvarar för vad. Ett sådant arrangemang måste även göras tillgäng-

[62] Se avsnitt 3.7.3 angående dataskydd som standard.
[63] Klamberg, M., Magnusson Sjöberg, C. & Öman, S., *Skydd av personlig integritet och informationsfrihet*, i Magnusson Sjöberg (red.), s. 178.
[64] Jfr HFD 2012 ref. 21 där Högsta förvaltningsdomstolen fann att Försäkringskassans ansvar inte endast omfattade den interna personuppgiftsbehandlingen utan även för den kommunikationen innan uppgifterna nått kassans interna system.

ligt för den registrerade enligt artikel 26.2. Vidare finns i 26.3 ett solidariskt ansvar för parterna i förhållande till den registrerade.

Ett scenario som kan vara svårt att förutse utgången i skulle kunna vara ett system som behandlar personuppgifter där flera de facto är personuppgiftsansvariga utan att ett avtal sinsemellan upprättats. En registrerad skulle då teoretiskt sätt kunna utöva sina rättigheter mot var och en som fastställs som personuppgiftsansvarig. I komplexa system med valmöjligheter är det inte omöjligt att varje användare skulle kunna ses som personuppgiftsansvarig i viss mån där själva protokollet skulle vara personuppgiftsbiträde då den endast möjliggör infrastrukturen för behandlingen utan att nödvändigtvis vara beslutsfattaren.[65] Här kan ges vid handen att den nya dataskyddsförordningens föreställning om personuppgiftsansvariga är att de traditionellt inte är svårligen bestämda. Med framväxten av allt mer decentraliserade system har förordningen i detta avseende inte tagit höjd för tekniskt ”icke-linjära” behandlingsmodeller. Det betyder inte nödvändigtvis att det inte går att fastställa vem eller vilka som är personuppgiftsansvariga, men det kräver en mycket omfattande analys av de tekniska bitarna i systemet och exakt hur och på vilka villkor personuppgiftsbehandlingen går till.

3.5 Personuppgiftsbiträden

3.5.1 Förhållandet till personuppgiftsansvarig

I tillägg till den personuppgiftsansvariga finns även i den nya dataskyddsförordningen rollen som *personuppgiftsbiträde* eller *processor* på engelska. I artikel 4 definieras ett personuppgiftsbiträde som den som biträder den personuppgiftsansvariga i utförandet av behandlingen. Artikel 29-arbetsgruppen för skydd av personuppgifter (föregångaren till Europeiska dataskyddsstyrelsen) meddelade även i ett yttrande att två krav föreligger för att ett förhållande ska finnas mellan en personuppgiftsansvarig och ett biträde. Det första är att det är fråga om två enskilda entiteter medan det andra är att biträdet agerar på uppdrag av den ansvarige.[66] Samma person, juridisk eller fysisk, kan således inte både ha rollen som personuppgiftsansvarig och personuppgiftsbiträde avseende en enskild behandling. Det är dock möjligt för samma person att ha olika roller i förhållande till olika behandlingar.

Personuppgiftsbiträdet agerar på uppdrag av den personuppgiftsansvarige men kan dock ändå genom artikel 82-83 i den nya dataskyddsförordningen stå ansvarig i förhållande till den regi-

[65] Jfr Garrod, L., *Who is the Data Controller and Processor on your blockchain*, “hackernoon.com/who-is-the-data-controller-and-processor-on-your-blockchain-79dbe6b107d8”, lydelse 2018-11-23.
[66] Artikel 29-arbetsgruppen för skydd av personuppgifter, *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, s. 25.

strerade vilket kan leda till böter eller ersättningsanspråk. Detta självständiga ansvar är en utvidgning av 45 och 48 §§ PuL som endast gällde personuppgiftsansvariga. Det finns i artikel 28.1 krav på att personuppgiftsbiträden endast ska anlitas om de kan ge tillräckliga garantier att lämpliga tekniska och organisatoriska åtgärder genomförs så att behandlingen uppfyller kraven i förordningen. Det är ett relativt strikt krav vilket betyder att den personuppgiftsansvarige rimligen kan komma att behöva bevisa att sådana garantier lämnats. En sådan garanti kan bl.a. vara enligt 28.5 att personuppgiftsbiträdet har anslutit sig till en godkänd uppförandekod i enlighet med artikel 40 eller en godkänd certifieringsmekanism enligt artikel 42. I sådant fall ska en tillräcklig garanti anses ha lämnats.

3.5.2 Avtalskrav och risk för rollöverskridande behandling

Ett strikt krav som uppställs för att ett personuppgiftsbiträde ska få tillträda och behandla personuppgifter på uppdrag av den personuppgiftsansvarige är emellertid att ett avtal eller annars bindande rättsakt enligt artikel 28.3 finns som ska föreskriva en rad omständigheter. Avtalet ska vara skriftligt enligt 28.9 vilket omfattar elektroniskt upprättade avtal. I det fall ett personuppgiftsbiträde överträder sina befogenheter i förhållande till de instruktioner personuppgiftsbiträdet fått från den personuppgiftsansvarige ska denne anses vara personuppgiftsansvarig i förhållande till den behandlingen enligt 28.10. Utan avtal riskerar följaktligen en som tror sig agera som personuppgiftsbiträde inträda i rollen som personuppgiftsansvarig då begreppet personuppgiftsbiträde kräver att någon är personuppgiftsansvarig i förordningens mening.

3.6 Registrering av personuppgiftsbehandling

Utöver den tillsyn som tillsynsmyndigheterna i respektive medlemsland utövar har både personuppgiftsansvariga och personuppgiftsbiträden krav på registerföring av personuppgiftsbehandling enligt artikel 30.1 respektive 30.2 i förordningen. I skäl 82 till förordningen nämns att både personuppgiftsansvariga och personuppgiftsbiträden bör dokumentera samtlig behandling. I det äldre dataskyddsdirektivet föreskrevs inget direkt krav som den nya förordningen stipulerar, men det fanns dock ett indirekt sådant krav vilket byggde på att personuppgiftsbiträden var skyldiga att rapportera all behandling som sker till den personuppgiftsansvariga. Tillsammans med personuppgiftsansvarigas rapporteringsplikt vid incidenter och samarbetskrav i förhållande till tillsynsmyndigheten krävde detta i praktiken att register fördes över all behandling.

I den nu aktuella lydelsen i förordningen ska bl.a. dokumenteras kontaktuppgifter, ändamål för behandlingen och om möjligt en beskrivning av vilka tekniska och organisatoriska säker-

hetsåtgärders som tas för behandlingen. För att inte ett sådant registerförande ska bli allt för omfattande för mindre företag innehåller den nya dataskyddsförordningen genom artikel 30.5 en begränsning där företag med färre än 250 anställda inte behöver företa sådan dokumentering. Emellertid kan avsedd dokumentation ändå behöva föras om det bl.a. är sannolikt att behandlingen kommer medföra en risk för att registrerades rättigheter kränks eller att behandlingen inte är tillfällig. Det får dock inte anses ovanligt att personuppgiftsbiträdesavtal innehåller klausuler som medför en skyldighet för personuppgiftsbiträdet att dokumentera och rapportera vilken behandling som utförs i det fall biträdet har färre än 250 anställda.

3.7 Dataskydd vid behandling och dataskydd som standard

De tekniska krav som den nya dataskyddsförordningen ställer på behandling är ambitiösa men kan i vissa fall tyckas framstå som abstrakta. Här åsyftas inte i huvudsak principer om datasäkerheten kring skydd mot obehörig tillgång eller skydd mot förlust av sådana data som i artikel 5 utan främst de tekniska standarder som ska säkerställa att den registrerades rättigheter inte kränks såsom uppgiftsminimering och pseudonymisering i artikel 25. Den aktuella artikeln stadgar bl.a. att personuppgiftsansvariga ska genomföra lämpliga tekniska åtgärder vari pseudonymisering anges särskilt samt uppgiftsminimering. Genom uppgiftsminimering begränsas den data som behandlas vilket bidrar till en reducerad risk för kränkningar av individers rättigheter kring personuppgifter. Endast de absolut nödvändiga uppgifterna för ändamålet samlas in. En sådan design kan tänkas enklast applicerbar främst i egna system eller applikationer. I öppna formulär där individer ges möjlighet att själva ange information torde en uppgiftsminimering bli svårare. Däremot kan gallring av personuppgifter och lagringsminimering där irrelevant personuppgifter raderas eller avidentifieras användas som ett effektivt medel vid sådana insamlingar.

3.7.1 Pseudonymisering

När det kommer till pseudonymisering, efter grekiskans *”falskt namn”*, som nuddats vid tidigare handlar det i huvudsak om att man omvandlar den registrerade och dennes personuppgifter till annat namn, kod eller siffror. I artikel 4 ges definitionen av pseudonymisering som att man behandlar uppgifterna på ett sådant sätt att de inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. Här kan nämnas användbara lösningar som exempelvis kundnummer istället för personuppgifter. En mer långtgående pseudonymisering kan även innehålla en kryptering där den personuppgiftsansvariga eller biträdet sparar krypte-

ringsnyckeln för att vid behov kunna vidta åtgärder.[67] I systemet finns således inte längre direkta personuppgifter som behandlas. Nämnvärt är dock att pseudonymer är att betrakta som indirekta personuppgifter sedan de går att med hjälp av pseudonymiseringsformeln eller *nyckeln* att hänföra ett pseudonym till dess ursprungsinformation.[68] Vidare kan det även vara möjligt att särskilja en individ ur en grupp individer med hjälp av pseudonymiserade uppgifter. Pseudonymisering är alltså inte ett medel för total avidentifiering vilket är en mycket viktig distinktion som behöver göras.

3.7.2 Anonymisering

Till skillnad från pseudonymisering, vilka uppgifter omfattas av GDPR som indirekt personuppgift på grundval av att det med indirekta eller kompletterande uppgifter går att identifiera en viss individ, omfattas inte anonyma uppgifter. De faller utanför ramen för personuppgifter som tidigare nämndes är nyckelordet för att det ska vara fråga om en personuppgiftsbehandling under GDPR.[69] Personuppgifter som insamlats eller behandlats kan anonymiseras genom att kopplingen mellan data och individen helt raderas. Det ska inte vid anonymisering gå att återskapa ursprungsuppgifterna eller på något sätt sammankoppla data tillbaka till den registrerade. Användningsområdet för anonymiserade uppgifter är följaktligen klart begränsat i förhållande till personuppgifter, men kan vara av intresse för områden som bl.a. beteendeforskning, marknadsföringsforskning eller statistik.

3.7.3 Dataskydd som standard

Innebörden av dataskydd som standard är att den personuppgiftsansvarige vid bestämmandet av vilka medel behandlingen ska utföras med implementerar vissa lämpliga tekniska åtgärder redan i ett tidigt skede. Pseudonymisering och uppgiftsminimering eller gallring är två exempel på dataskydd som standard som kan begränsa risken för att den registrerades rättigheter kränks. I artikel 25 nämns att man vid dataskydd som standard ska beakta många parametrar. Det får därför anses svårt att generellt ge något entydigt svar om vilken grad av dataskydd som bör implementeras. I skäl 78 till GDPR nämns att även producenter av tjänster och applikationer som kan komma att behandla personuppgifter bör beakta rätten till dataskydd vid framtagningen av dessa tjänster och applikationer. Dataskydd som standard sträcker sig därför längre än den personuppgiftsansvariga sedan programvarorna ofta designas av utvecklare som i sin design bör implementera personuppgiftsskyddande möjligheter. Det är kanske även i det

[67] Se avsnitt 2.3.2 angående bl.a. symmetrisk kryptering som använder samma nyckel vid kryptering som vid dekryptering. Se även Artikel 29-arbetsgruppen, *Yttrande 05/2014 om avidentifieringsmetoder*, s. 20 f.
[68] Se skäl (26) GDPR.
[69] Se avsnitt 3.2.1 och 3.3.

skedet som uttrycket får störst relevans. I skäl 83 till förordningen nämns bl.a. att behandlingen kan krypteras för att öka säkerheten och hindra behandling som strider mot förordningen.

Likt avsnitt 3.7.1 används vid krypteringar och omvandling olika typer av metoder.[70] Den normala praktiska användningen för kryptering får antas vara en kryptering med möjlighet till dekryptering. Då en sådan användning medför att en koppling tillbaks till ursprungsdatan via dekrypteringsnyckeln är möjlig och är det således fråga om indirekta personuppgifter som behandlas. Det går emellertid att använda envägsalgoritmer där den krypterade datan inte går att dekryptera tillbaka för att få fram ursprungsdatan (såsom bl.a. kryptografiska hash-funktioner). Ett sådant förfarande medför dock nackdelen att informationen endast kan användas i behandlingen som ett jämförande medel som bl.a. lösenordsverifiering eller bekräftelse på att en viss information finns i systemet m.m. Det finns då ingen given nyckel som kan omvandla tillbaka värdet till ursprungsinformationen utan det enda sättet vore att gissa sig fram (s.k. *bruteforce-attack*) till ursprungsinformationen.[71] Frågan är i det skedet om graden av kryptering spelar roll vid fastställandet av om den till synes anonyma koden är att anse som personuppgift och omfattas av GDPR eller som anonym och falla utanför. Enligt ett tillsynsärende från Datainspektionen ansågs att hashsummor till följd av envägsfunktioner ska utgöra personuppgifter. Datainspektionen ansåg att det går att baklängesidentifiera ursprungsinformationen genom en jämförelse av gissade hashsummor som körs genom samma funktion.[72] Datainspektionen beaktar dock att användningen av hash-funktioner försvårar sådan identifiering.

3.8 Radering av personuppgifter

När det kommer till den registrerades rättigheter inom ramen för GDPR kan särskilt nämnas rätten till ändring eller radering av personuppgifter vid behandling i artiklarna 16 respektive 17. Artiklarna uttrycker en generell rättighet att på begäran få sina personuppgifter som rör en själv ändrade eller raderade utan onödigt dröjsmål. Rätten till radering eller även kallad *rätten att bli bortglömd* i artikel 17 ställer i punkt 1 upp vissa scenarion när sådan rätt gäller. Den första grunden i artikel 17.1.a tar sikte på situationer där personuppgifterna inte längre är nödvändiga för ändamålet för behandlingen. I ett önskvärt scenario ska den personuppgiftsansvarige dock inte lagra personuppgifter längre än nödvändigt för de ändamål de samlats in för.

[70] Jfr bl.a. avsnitt 2.3.1 och 2.3.2.
[71] Jfr dock avsnitt 2.6 angående s.k. *bruteforce-attacker* där rätt ursprungsdata gissas fram. Se även Felten, E., *Does Hashing Make Data "Anonymous"?*, Federal Trade Commission, 2012, "www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous", lydelse 2018-12-05.
[72] Se Datainspektionens beslut 2015-06-22, dnr 2729-2014, s. 8.

Vidare tar artikel 17.1.b och 17.1.c sikte på återkallelse av samtycke eller invändning mot behandlingen i sig. Återkallelse av samtycke torde vara tämligen vanligt förekommande grund för radering då samtyckesklausuler används i stor utsträckning pga. deras effektivitet för insamlaren. Inte sällan är en användare snabb med att acceptera villkoren för att exempelvis besöka en hemsida eller använda en tjänst varvid användaren då samtyckt till villkoren genom att exempelvis fortsätta besöka hemsidan eller använda tjänsten. En sådan återkallelse av samtycke bör vara framgångsrik i de allra flesta fall. Ser vi vidare till invändning mot behandlingen i 17.1.c invänder den registrerade mot behandlingen i sig. I det scenariot måste enligt artikeln den registrerades invändning väga tyngre än de berättigande skälen för behandlingen, såvida det inte är fråga om behandling eller profilering i direktmarknadsföringssyfte varvid ett sådant krav saknas.[73]

För radering av information som den personuppgiftsansvarige gjort publik gäller enligt 17.2 att den personuppgiftsansvariga, i det fall radering är aktuellt enligt 17.1, ska underrätta andra personuppgiftsansvariga som behandlar personuppgifterna denna gjorde publika. En rimlighetsavvägning görs i förhållande till tillgänglig teknik och kostnad för genomförandet. I de fall en behandling faller utanför en sådan åtgärd kan istället den registrerade riskera behöva kontakta de andra personuppgiftsansvariga för radering. De andra personuppgiftsansvariga behöver även i förhållande till sin behandling grunda den på någon i förordningen tillåten grund. Rätten att bli bortglömd gäller i detta avseende även information på säkerhetskopior eller s.k. *backups* som gjorts.[74] En sådan radering kan både vara svår och kostsam då backupkopior ofta lagras som en fast spegelbild som först behöver återskapas för att kunna redigeras. Det kan därför behöva fastställas i avtalet mellan personuppgiftsansvariga, personuppgiftsbiträden och leverantörer hur sådana mekanismer ska säkras.[75]

[73] Se skäl (70) GDPR.
[74] Se Artikel 29-arbetsgruppen för skydd av personuppgifter, *Yttrande 5/2012 om datormoln (cloud computing)*, s. 12.
[75] Ibid. s. 21.

4. När blockkedjan möter GDPR

4.1 Den stora knuten för blockkedjans regelefterlevnad

När det talas om vilka utmaningar blockkedjor har för att möta kraven under GDPR är den kanske största just angående personuppgifter som inte går att radera på grund av blockkedjans tekniska design. För att kunna problematisera den frågan behöver vi se närmare på de två bestämmelserna; hur personuppgiftsbehandling och rätten att bli bortglömd ska aktualiseras för blockkedjor. Efter att förståelse för hur bestämmelserna kan komma att tillämpas för blockkedjor kan ansvarsfrågan diskuteras.

4.1.1 Personuppgiftsbehandlingen

För att rätten att bli bortglömd ska kunna diskuteras är ett kriterium att det faktiskt rör sig om personuppgifter som behandlas. Vi behöver därför se till vilken typ av uppgifter som behandlas inom blockkedjor och följaktligen hur sådana uppgifter ska betraktas under GDPR. I kapitel 2 redogjordes för tekniken bakom blockkedjor och vilken information som behandlas i dem medan kapitel 3 tog sikte på GDPR och dess relevanta bestämmelser i allmänhet. Jag går därför här igenom de potentiella personuppgifterna som kan tänkas förekomma i en normal blockkedjetransaktion som får analyseras i ljuset av vad som sagts i kapitel 3.

Det första momentet en användare stöter på är att man får en identitet på blockkedjan. Dels skapas två nycklar; den publika och den privata. Vi kan för enkelhetens skull tänka oss den publika nyckeln som ett bankkontonummer eller identitetsnummer men utan bakomliggande registrering av personuppgifter. Den privata nyckeln kan vi betrakta som en pinkod för att signera utgående transaktioner med. Eftersom ett grundläggande moment för blockkedjor är anonymitet kan vi inte likställa uppgifterna direkt med exempelvis ett traditionellt bankkontonummer som vi vet är att anse som personuppgift då numret tillsammans med bankens uppgifter om innehavare identifierar personen.[76] Istället får beteende och metadata ligga till grund som indirekt koppling. Som nämnt i diskussionen angående indirekta kopplingar till följd av beteende finns det många scenarion där en individ kan röja sin blockkedjeidentitet. Det kan handla om att det registreras vid en betalning eller att det blir allmänt känt. Vidare finns studier som visar på att metadata är en mycket effektiv metod för att efterforska identiteter från

[76] Jfr liknande resonemang i avsnitt 3.3 angående IP-adresser.

anonymiserade uppgifter.[77] En sådan metadataanalys måste även få anses uppfylla det rimlighetskrav som generaladvokaten nämnde i Breyer v. Bundesrepublik Deutschland.[78] Av denna anledning måste en sådan anonym identitet som en publik nyckel inom blockkedjor kunna anses som en personuppgift.[79] Den slutsatsen medför att vid varje transaktion på blockkedjan riskeras en personuppgift behandlas vilket är intressant i två aspekter för den fortsatta diskussionen om blockkedjors kompabilitet med GDPR. Dels kan följaktligen rätten att bli bortglömd komma att diskuteras då en sådan rätt grundas på att det rör sig om personuppgifter som registrerats. Dels kan även rollerna diskuteras mer ingående eftersom vi vet att vid en personuppgiftsbehandling, som det nu är fråga om, måste en personuppgiftsansvarig finnas. Vad nu sagt om analys av metadata behöver dock inte nödvändigtvis resultera i att en specifik identitet går att fastställa, troligen är det istället i de flest fall tvärt om, i synnerhet om en användare gjort väldigt få transaktioner (vilket begränsar en analys av metadata eller försämrar dess resultat). Möjligheten medför dock att det kan röra sig om personuppgifter vilket räcker i detta avseende.

Eftersom bestämmelser i GDPR som medför en skyldighet eller rättighet grundar sig på enskilda fall räcker det dock inte att stanna vid den första upptäckta personuppgiften inom blockkedjor. I varje transaktion finns utöver avsändare och mottagare även andra transaktionsdata. Här spelar blockkedjans syfte och utformning stor roll beroende på hur formatet ser ut. I vissa protokoll kan endast nummer skickas, ofta hos valutor, medan i andra skickas text och bilder.[80] Oavsett vilken typ av data som blockkedjan behandlar är det i många fall fråga om en möjlighet för personuppgifter att inkluderas. Det kan i detta avseende nämnas att vad nu sagt gäller kompletta noder på nätverken. Vissa komprimerade noder, s.k. *lightweight nodes* använder endast blockens block-header i vilken transaktionerna endast återfinns som ett hashkondensat eller Merkle root.[81] Med bakgrunden av hur ett Merkle träd fungerar kan en sådan nod användas i situationer där inte prestanda eller hårdvara finns för att köra en fullständig nod. I en sådan isolerat begränsad behandling återfinns endast hashsumman av transaktionerna. Frågan är därför om en hashsumma kan tänkas utgöra personuppgifter. I ett yttrande från Artikel 29-arbetsgruppen ska användandet av en hash-funktion likställas med

[77] Se Perez, B., Musolesi, M. & Stringhini, G., *You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information* s. 8 f., "www.ucl.ac.uk/~ucfamus/papers/icwsm18.pdf", lydelse 2018-12-10.
[78] Jfr avsnitt 3.3.4.
[79] Se avsnitt 3.3.2 – 3.3.4.
[80] Jfr decentraliserade nyhetssidor som byggs på blockkedjor för att säkerställa bl.a. säkerheten av nyhetsflödet.
[81] Se avsnitt 2.5 och 2.6.1. En komprimerad nod kan användas för att bekräfta huruvida en transaktion förekommit eller inte men ser inte all transaktionsdata utan endast hashsummorna av transaktionerna.

pseudonymisering.[82] I avsnitt 3.7.1 fastställdes vidare att pseudonym ska anses utgöra personuppgifter, varför det även i komprimerade noder kan vara fråga om en personuppgiftsbehandling.

4.1.2 Rätten till radering

Vi kan efter ovan analys utgå från att personuppgifter riskeras behandlas i en eller annan form i publika blockkedjor. Som många i debatten nämner samt som framgår i en rapport från ett initiativ av Europeiska kommissionen betecknas det stora orosmomentet för blockkedjor i förhållande till GDPR som bristen på ändrings- och raderingsmöjligheter.[83] Det grundas i en kombination mellan att all transaktionsdata distribueras till alla i nätverket och att blockkedjans integritet fastställs genom det tekniska kravet på att kunna gå tillbaka historiskt och härleda alla transaktioner som skett på kedjan. I teorin kan dock både radering och ändring för publika blockkedjor vara möjliga. Det skulle i så fall handla om att en ändring av ett tidigare block görs vilket får till följd att varje efterföljande block måste räknas om med datorkraft.[84] Ser man till andra praktiska möjligheter för att kunna efterleva kraven GDPR ställer på radering och ändring kommer även andra komplexa frågeställningar in i bilden som motiv. Den som i teorin skulle kunna ändra en blockkedja måste vara motiverad till att göra det då datorkraften som krävs för de flesta blockkedjor är en stor ekonomisk kostnad. Eftersom ju äldre block i kedjan man vill ändra desto mer datorkraft krävs för att räkna om efterföljande blocks nya hashsumma är det inte heller möjligt att, på den nu nämnda teoretiska lösning, i praktiken lyckas sedan blockutvinnare redan i dagsläget tävlar för att hinna skapa *ett* nytt block. Den som vill ändra ett långt tidigare blocks innehåll måste således processera om alla efterföljande block på samma tid som en blockutvinnare endast behöver beräkna det nästkommande blocket för att bilda längsta kedjan.

Den oro som riktas över att publika blockkedjor inte är förenlig med det krav på radering i artikel 17 i GDPR är följaktligen praktiskt motiverad vilket enligt min mening måste vara det rätta förhållningssättet till denna problematik. En allt för teoretisk diskussion kring eventuella lösningar riskerar att bli tandlös i förhållande till den faktiska användningen, särskilt som publika blockkedjor i stort kan användas anonymt i samband med att ansvarsfrågor fortfarande inte på ett tillfredsställande sätt är utredda. Resonerar man kring vilka punkter på block-

[82] Artikel 29-arbetsgruppen, *Yttrande 05/2014 om avidentifieringsmetoder*, s. 20 f.
[83] Lyons, T., *Blockchain Innovation in Europe*, European Union Blockchain Observatory and Forum, s. 16, "https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf", lydelse 2019-01-02.
[84] Se avsnitt 2.5.

kedjan som skulle vara möjliga att tydligare reglera kommer man emellertid förr eller senare nå slutsatsen att det blir fråga om en funktionell begränsning av blockkedjan och praktiskt omotiverade åtgärder som behöver vidtas.

Ser vi först till den funktionella begränsningen åsyftas främst designen av blockkedjan. Samtidigt som det är förståeligt att exempelvis barnpornografi inte lagligen ska kunna distribueras på en blockkedja kan det vara svårt att behålla blockkedjans funktionalitet om man begränsar vilken typ av data som kan accepteras. Det är inte nödvändigtvis ett problem för en blockkedja som är designad att endast acceptera siffror men en blockkedja som registrerar upphovsrättsligt material som texter, bilder m.m. kan det vara svårt att begränsa innehållet utan att funktionaliteten för blockkedjan begränsas eller blir oanvändbar inför risken att inte kunna följa kraven inom GDPR. Dock bör nämnas att även en blockkedja som Bitcoins med ett redan begränsat utrymme för ”fri text” i transaktionen riskerar behandla annat lagstridit innehåll än endast personuppgifter.[85] Det finns därför anledning att i detta avseende bredda diskussionen för lagstiftning än att endast ta sikte på personuppgifter, även on personuppgifter må vara en viktig del att behandla. Jämför man med exempelvis en potentiellt illegal blockkedja som skulle distribuera olagligt material skulle en användares kopia kunna betraktas som ett illegalt innehav, vilket i förlängningen betyder att blockkedjan i sig skulle vara olaglig och således funktionellt begränsad.[86] Det är inte på samma sätt olagligt att inneha personuppgifter om någon, särskilt om transaktion i privat regi kan komma att betraktas som strikt privat och falla utanför det materiella tillämpningsområdet i artikel 2.2.c. Jag landar därför i slutsatsen att det inte går att skapa förenlighet mellan blockkedjor och GDPR avseende sådant ”legalt” innehav utan en inskränkande lagstiftning eller utökning över situationer av privat natur inom vilken personuppgifter faller innanför det materiella tillämpningsområdet för GDPR.[87]

Den andra punkten som redan nämnts kort är de praktiskt omotiverade åtgärderna. Finns konsensus mellan blockkedjans användare kan man teoretiskt vänta med att mynta nästa block till förmån för att rensa kedjan på de specifika personuppgifterna och låta hashsummorna beräknas om för alla block. När detta sedan skett kan blockkedjan fortsätta i vanlig ordning. En sådan lösning betyder dock oundvikligen att kedjans funktion pausas under en längre tid. I en

[85] Matzutt, R., Hiller, J., Henze M., Ziegeldorf J.H., Müllman, D., Hohlfeld, O. & Wehrle, K., *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin*, International Financial Cryptography Association, s. 6 f., “https://fc18.ifca.ai/preproceedings/6.pdf”, lydelse 2019-01-04.
[86] Denna frågeställning har varit främst aktuell gällande de rykten om att fragment av barnpornografiskt material ska ha distribuerats på Bitcoins blockkedja i det fritextutrymme som tillåts vid sidan av transaktionsdatan.
[87] Med legalt syftas här främst på blockkedjor som innehåller data som inte i sig är olagligt att inneha en kopia av.

blockkedja designad för vardagliga överföringar av värde vore det förödande att inte kunna utföra en transaktion på flera dagar eller veckor om det är väldigt gamla block som ska ändras. Vidare finns det ingen aktör som kan identifieras som naturligt motiverad att spendera datorkraft på ett sådant utförande. Tvärt om har blockutvinnarna incitament att driva kedjan framåt då de får en belöning för att göra. Även användarna är motiverade att kedjan drivs framåt så deras transaktioner blir genomförda och verifierade på kedjan. Till detta tillkommer även spörsmål som hur ofta sådant yrkande om personuppgiftsradering ska kunna göras och vem det ska framföras till. Sedan majoritet även krävs för att vidta en sådan åtgärd blir en trolig följd att minoriteten som inte vill vidta åtgärden kopierar blockkedjan och dess tidigare block och driver den avknoppade blockkedjan själva. Problemet är således inte löst denna väg heller då informationen finns kvar i den avknoppade kedjan. Raderingsproblemet för publika blockkedjor ser sålunda ut att fortsatt bekräftas som ett av de största kompabilitetsproblemen för publika blockkedjors regelefterlevnad av GDPR.

4.2 Potentiell rollfördelning och ansvar för blockkedjan

Utgår vi nu från att personuppgiftsbehandling på publika blockkedjor strider eller i vart fall riskerar strida mot raderingskravet i artikel 17 har både privata aktörer, lagstiftare och dömande organ att försöka bilda sig en uppfattning om vem som ska ställas till svars. När det kommer till blockkedjor har vi dels en modern distribuerad datastruktur med flera aktörer och dels bestämmelser som de facto måste tillämpas om personuppgiftsbehandlingen omfattas av tillämpningsområdet. I en rättsstat får det inte förekomma att domstolen väljer att inte döma pga. ovisshet i tillämpningen. Förhandsbesked från EU-domstolen kan dock begäras som vägledning, något som dock ännu inte skett avseende blockkedjor. Däremot har den franska dataskyddsmyndigheten CNIL som första tillsynsmyndighet kommit med ett yttrande och riktlinjer över ansvar på blockkedjor.[88] Vilken rättslig tyngd denna vägledning bör tillmätas är ännu svårt att säga då det är den första på området samt att den förhåller sig tämligen vag i riktlinjerna. Rapporten kommer därför att diskuteras som referens i analysen över vilken ansvarsroll olika aktörer kan tänkas inta och om det är en rimlig vägledning för vad följderna kan förväntas bli.

För de redogjorda ansvarsbestämmelserna i GDPR finns alltid en rollanknytning. Det gäller främst personuppgiftsansvariga och även personuppgiftsbiträden. Vid ett tankeexempel av ett

[88] Commission Nationale Informatique & Libertés (CNIL), *Blockchain and the GDPR: Solution for a responsible use of the blockchain in the context of personal data*, "https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf", lydelse 2019-01-02 [cit. CNILs vägledning].

mål i domstol rörande blockkedjor behöver domstolen fastslå vem som ska anses inta vilken roll för att senare kunna gå vidare till ansvarsfrågan och påföljd. Det kan även ha betydelse för vem den registrerade som finner sina personuppgifter på blockkedjan ska rikta anspråk till. Varje aktör eller funktion på blockkedjan måste därför analyseras avseende vilken roll den kan tänkas ha inom ramen för GDPR. I detta kapitel diskuteras dessa roller och även vad effekterna blir av de tänkbara utgångarna.

4.2.1 Det bestämmande inflytandets vikt

Innan vi går in och ser på hur de olika individuella funktionerna på blockkedjan kan betraktas i ljuset av GDPR behöver det bestämmande inflytandet i blockkedjor diskuteras. Det är en viktig del sedan blockkedjor har olika strukturer och karaktärer varvid det bestämmande inflytandet kan se väsentligen annorlunda ut. Det bestämmande inflytandet kan därför vara en vägledare i jakten på vem eller vilka som ska anses vara personuppgiftsansvariga eller personuppgiftsbiträden.

I avsnitt 3.4.1 såg vi att den personuppgiftsansvarige enligt artikel 4 i förordningen är den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för personuppgiftsbehandlingen. Datainspektionen har i ett beslut meddelat att det bestämmande inflytandet avgörs av de faktiska omständigheterna i varje enskilt fall.[89] Här har Datainspektionen även lutat sig på yttrande från Artikel 29-arbetsgruppens yttrande som menar på att bestämmandet av ändamål och medel avser rätten att bestämma ”varför” och ”hur” behandlingen ska genomföras.[90] Bestämmanderätten kan dock delegeras i viss mån. Bestämmanderätten om ändamålet med behandlingen tillkommer alltid den personuppgiftsansvarige medan frågan om medel kan överföras till ett personuppgiftsbiträde så länge den personuppgiftsansvarige fortfarande kan utöva bestämmanderätt över medlen.[91]

Bestämmanderätten kan härröra ur uttrycklig behörighet, underförstådd behörighet eller faktisk behörighet.[92] Medan den uttryckliga behörigheten grundas i lagtext uttryckt behörighet och underförstådd behörighet grundas på praxis och presumtion är den faktiska behörigheten den mest relevanta i förhållande till publika blockkedjor men även sannolikt svårast att till-

[89] Se Datainspektionens beslut 2010-07-02, dnr 686-10.
[90] Artikel 29-arbetsgruppen, *Yttrande 1/2010*, s. 13. Datainspektionens position har även godtagits av Förvaltningsrätten i Stockholm i dom 2013-10-14 mål nr 9987-12. Jfr Öman, S. & Lindblom, H., *Personuppgiftslagen: en kommentar*, 4 u., Norstedts Juridik, 2011, s. 93.
[91] Se, Lundqvist, D., Gustafsson, F., Tomas da Costa, E., Bogsjö Österberg, H., Jarkell, E. & Sahibli, T., *GDPR – några tillämpningsfrågor*, s. 9, Kahn Pedersen, ”kahnpedersen.se/wp-content/uploads/2017/10/KahnPedersen_GDPR_web.pdf”, lydelse 2018-12-06.
[92] Ibid. s. 10. Se även Artikel 29-arbetsgruppen, *Yttrande 1/2010 s. 10-13.*

lämpa. Avtal mellan parterna kan vara en faktisk behörighetsgrund. För privata blockkedjor har administratören för kedjan med största sannolikhet den faktiska behörigheten och är att anse som personuppgiftsansvarig medan blockutvinnare och noder på den privata kedjan är att anse som personuppgiftsbiträden.[93] Som nämnt tidigare i uppsatsen skiljer sig dock privata blockkedjor väsentligen mot publika sedan privata blockkedjor kan kontrolleras och administreras centralt på ett sätt som publika kedjor inte kan.

4.2.2 Skaparna och utvecklarna

I alla typer av blockkedjor finns någonstans en eller flera utvecklare som designar protokollet för blockkedjan. I publika blockkedjor rör det sig ofta om en utvecklargrupp som i och för sig inte nödvändigtvis är en egen entitet men som i vissa fall formar organisationer och bidrar med majoriteten av förslag till utveckling av protokollet. Protokollutvecklarna är ofta oavlönade eller får donationer från investerare som tror på projekten. Något avtal om produktion eller utveckling finns ofta inte och det är inte heller ovanligt att utvecklarna själva ackumulerar den digitala valuta man utvecklar för att vid en lyckad framväxt ta del av värdeökningen. Utvecklarna eller gruppen av utvecklare ansvarar ofta för olika delar av blockkedjan. Det kan även handla om tillägg som publiceras på till blockkedjan relaterade online-forum som senare läggs in i blockkedjans arkitektur.

Det centrala för att kunna bedöma blockkedjeutvecklarnas ansvar under GDPR är att se till deras grad av behörighet. De initiala utvecklarna, i vilket uttryck jag även inkluderar projektledare, som i någon form är med i bestämmandet av utformningen har inte någon uttrycklig behörighet i lag. Det är även svårt att utläsa någon sorts underförstådd behörighet att bestämma ändamål och medel med behandlingen. Det får istället bli den faktiska behörigheten som prövas. I det tidigaste av skeden när blockkedjan ska utvecklas finns en idé bakom vad som ska åstadkommas. Om det är fråga om en ny kryptovaluta eller annan blockkedja måste det ändå finnas ett ändamål med kedjan. Det är därför frestande att dra slutsatsen att det är den som kom på idén för blockkedjan och dess initiala utvecklare som bestämmer ändamålen och medlen för den behandling som sker. En sådan slutsats är inte nödvändigtvis felaktig i detta initiala skede när blockkedjan inte ännu nått en publik utanför utvecklarkretsen.

I ett senare skede när intresse skapats för blockkedjan och användare vill ansluta blir det mer problematiskt i takt med att den faktiska behörigheten att bestämma ändamål och medel

[93] Se Kaufmann, J., *Blockchain meets Data Privacy – Blockchain and the Data Controller*, Legal Revolutionary, 120, s. 127, "legal-revolution.com/images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf", lydelse 2018-12-06 [cit. Kaufmann].

minskar. Ju populärare blockkedjan blir desto fler åsikter om protokollutformning och optimering dyker upp. Sedan koden bakom blockkedjorna publiceras som öppen källkod där alla har insikt är det lätt för en protokolländring att genomföras. Inte sällan konkurrerar således flera protokollversioner om att bli den som de flesta använder, alla med sin egen version av originalkedjan.[94] I detta skede har följaktligen fler och nya utvecklare anslutit sig och presenterar deras versioner av protokollet. Frågan är således hur bestämmanderätten över ändamål och medel ska tillskrivas i en sådan utveckling. Ett vanligt scenario är självklart att de ursprungliga utvecklarna fortfarande kör sin linje och har stöd från användarna för den. Det är inte omöjligt att stöd från användare som använder en viss version torde kunna ses som att ett faktiskt inflytande över bestämmanderätten för ändamål och behandling utövas. Ser man till det krasst är det ju de facto den eller de utvecklarna som lagt fram just den versionen som bestämt ändamålet och medlen för behandlingen, obeaktat vilken typ av information som senare kan komma att introduceras i blockkedjan. Det skulle dock föra diskussionen vidare i om det i så fall skulle kunna vara fråga om ett gemensamt ansvar som personuppgiftsansvariga mellan utvecklarna.

Frågan består dock om bestämmanderätten över ändamål och medel är tillräcklig som grund för avgörandet av huruvida någon är att anse som personuppgiftsansvarig. Visserligen har utvecklarna bestämt hur användarna *kan* kommunicera, dvs. vilket typ av format på informationen som accepteras av protokollet. Efter att en protokollversion har utvecklats är det dock de facto användarna i publika blockkedjor väljer vilken blockkedja de ska använda och vilken information de vill inkludera i sin transaktion på blockkedjan. Till utvecklarnas försvar kan därför argumenteras att en produkt har utvecklats som endast agerar som en plattform för användning som ligger utanför deras kontroll. Till skillnad mot molntjänster lagrar inte utvecklarna själva någon information eller har någon nödvändig server för att protokollet ska fungera. Istället har andra noder tagit över distributionen av information. Inte heller har utvecklarna någon uttrycklig möjlighet genom avtal eller lag att påverka behandlingen som sker i nätverket efter att protokollet lanserats och installerats av noderna.

Skulle en parallell dras här kan man tänka sig att utvecklarna av Internet inte rimligen kan hållas ansvariga för all trafik som sänds med hjälp av det protokollet. En sådan slutsats känns allt för långt hållen. Emellertid kan dock den nya dataskyddsförordningen tillåta en sådan tolkning, vilket skulle medföra enorma konsekvenser för utvecklare och grundare för de större

[94] Jfr modifierade kopior av Bitcoins blockkedja s.k. *forks* på engelska så som bl.a. Bitcoin Cash, Bitcoin SV, Bitcoin Diamond, Bitcoin Gold m.fl.

blockkedjorna. En sådan syn kan dock enligt mig kontras på främst två punkter. Den första är att det är en praktisk svårighet att fastställa vem som ska tillmätas ansvar då protokollutvecklingen ofta sker genom anonyma tillskott av kod över tid. Det är ovisst huruvida det är ursprungsversionen eller delar som ändrats som är det mest väsentliga i bedömningen. Den andra punkten, som torde vara än mer relevant, är att definitionen av en personuppgiftsansvarig i artikel 4 lexikaliskt är den som bestämmer, dvs. en nutidsbild av bestämmanderätten för de ändamål och behandling som sker. Så fort protokollet börjar köras av noder har denne också i samma skede tappat kontroll över det faktiskt inflytande på dess användning.

När det inte längre finns en central punkt för distribution, som en server eller dylikt, är det svårt att säga vem som har kontroll över dess befinnande. Av den anledningen välkomnas en sådan fråga för EU-domstolen att ta ställning i. I takt med att en publik blockkedja växer blir det dock svårare och svårare att försöka fastställa någon bestämmanderätt eller personuppgiftsansvarig i förhållande till grundarna eller utvecklarna. I ett tidigt skede eller i privata blockkedjor torde detta vara möjligt, men i förlängningen på publika blockkedjor är det inte utvecklarna som själva gör nya inlägg på blockkedjan. Den franska dataskyddsmyndigheten CNIL har i förhållande till utvecklare dock nämnt att de i vissa fall kan ses som personuppgiftsbiträden i de fall blockkedjan eller funktioner på blockkedjan som bl.a. smarta kontrakt utfärdas på uppdrag av en personuppgiftsansvarig.[95] Det handlar dock om enskilda ingripanden eller utfärdande av tjänster vari personuppgifter de facto behandlas av utvecklaren. En utvecklare av en publik blockkedja torde dock inte träffas av denna definition då utvecklaren inte i designen av blockkedjan själv utfärdar funktioner som smarta kontrakt på blockkedjan på någons begäran.

4.2.3 Blockutvinnarna

En aktör på blockkedjan som kan diskuteras är blockutvinnarna eller de s.k. *miners* vars uppgift är att komponera nästa block av transaktioner och genom detta säkra kedjan. Den behandling dessa företar är att komponera block av de väntande transaktionerna och sedan räkna ut dess hashsumma för att vid rätt försök få belöning i form av inflation.[96] Det som kan tala för att blockutvinnare kan gå fria från ansvar under GDPR är att de själva inte bestämmer varken innehåll, ändamål eller medel för behandlingen. En blockutvinnare får färdiga transaktioner eller information tilldelade som väntandes transaktioner. Den behandling som företas är emellertid endast att bunta ihop dessa och tillsammans med en slumpmässig faktor prova sig fram

[95] Se CNILs vägledning s. 3 f.
[96] Se avsnitt 2.5.

till dess att en hashsumma som accepteras av nätverket har lyckats genereras. Blockutvinnare introducerar således ingen egen information till blockkedjan och kan sammantaget inte i en publik blockkedja anses ha något personuppgiftsansvar.

Samtidigt kan det argumenteras för att det är just blockutvinnare som publicerar själva blockkedjan då det utan blockutvinnare inte blir några tillgängliga block att bygga kedjan på. En sådan slutsats kan dock enkelt avfärdas på dels ovan nämnda brist på bestämmanderätt samt att informationen redan publicerats till nätverket från noderna som väntande transaktioner. Den nu nådda slutsatsen att blockutvinnare inte bör anses som personuppgiftsansvarig delas även av den franska tillsynsmyndigheten i sitt yttrande.[97] Däremot nämns inte huruvida de skulle kunna vara att anses som personuppgiftsbiträde då de komponerar block på uppdrag av alla användare (då utvinnaren får en monetär vinning av det samtidigt som användaren får sin transaktion inlagd i nästa block). En sådan konstruktion med blockutvinnare som personuppgiftsbiträde kräver dock både avtal med den som är att anses som personuppgiftsansvarig vilket inte kan anses förekomma på publika blockkedjor. Det vore långsökt att genom konkludent handlande ingå ett sådant avtal med blockutvinnaren vid användandet av blockkedjeprogramvaran, särskilt som det med största sannolikhet skulle brista i de krav som GDPR ställer på ett sådant personuppgiftsbiträdesavtal i artikel 28.3.[98]

4.2.4 Noderna

Noder som agerar på användares uppdrag kan likställas det som nu sagts om blockutvinnare med det undantag att en nod inte ämnar komponera några nya block. Istället håller noder i nätverket ansvar för att själv inneha en uppdaterad version av den längsta kedjan och till nätverket annonsera nya väntande transaktioner som gjorts av dess användare. Sedan noder ofta körs av bl.a. handelsplattformar, tjänster för digitala plånböcker m.m. kan det finnas tusentals användare som kommunicerar till nätverket genom noden, likt hur en internetleverantör förmedlar dess användares trafik. Noder har således likt blockutvinnare inte själva något inflytande över vad för transaktionsinformation som användarna vill förmedla till nätverket. Inte heller har noden något inflytande över hur den information som finns i transaktionen behandlas utan endast att den förmedlas. Hur den väntande transaktionen förmedlas är redan bestämt av protokollet för att det tekniskt ska fungera. Nodernas ansvar som personuppgiftsansvarig torde därför kunna avskrivas på denna grund. Inte heller CNIL nämner något som skulle föranleda någon annan slutsats.

[97] Se CNILs vägledning s. 2.
[98] Se avsnitt 3.5.

Däremot kan tänkas att en nod står närmare till hands att definieras som personuppgiftsbiträde än blockutvinnare. Det grundas i att bl.a. handelsplattformar eller tjänster som åt sina användare kör en nod i många fall har användaravtal som behöver godkännas för att användare exempelvis ska kunna handla på plattformen. Det finns således ofta möjlighet för en närmare avtalad relation som kan tolkas som ett personuppgiftsbiträdesavtal mellan användarna och noderna än mellan användarna och blockutvinnarna. Här kan exempelvis tänkas att den som kör en nod genom avtal med sina användare kan fastställa inbördes ansvar för informationen som förmedlas till nätverket genom noden. Dock är det inte särskilt sannolikt då den som kör noden ofta är i en starkare ställning än användaren vilket blir motsägelsefullt om personuppgiftsbiträdet är den som skulle bestämma medel för behandlingen. En person eller företag som kör en nod för en blockkedja torde inte heller vilja ta på sig rollen som biträde då det medför risker om alternativet är att helt enkelt undgå ansvar. Resonemanget liknar det om internetleverantörer varvid en internetleverantör inte rimligen vill bära ett delansvar för vad köpare väljer att göra på internet om nu användaren skulle vara att anse som personuppgiftsansvarig och själv bestämma över ändamål och medel. Även fast möjligheten till att avtal sluts mellan noder och användare finns lämnas ingen vägledning av CNIL hur och om det i praktiken skulle fungera vilket kritiserats av debattörer inom området.[99] Noder får därför i det närmsta likt blockutvinnare inte utan svårighet kunna tillmätas någon ansvarsroll stipulerad i GDPR.

4.2.5 Användarna

Vad ovan sagts om noder gäller för de noder som förmedlar användares transaktioner till nätverket. En transaktionspart eller ”vanlig användare” kan emellertid själv köra en nod och på så vis kommunicera direkt med nätverket utan att behöva förlita sig på att en annan nod är online och förmedlar transaktionen korrekt till nätverket. Ser man därför till användarnas roll på publika blockkedjor är det användarna som väljer vem transaktionen ska göras med och vilket innehåll som ska finnas med i den transaktion som förmedlas till blockkedjans nätverk. Även om användarna inte själva är de som utvinner block vilket fäster transaktionsdata på kedjan är det användarna som gör transaktionsdata tillgänglig i form av väntande transaktioner. Införandet av personuppgifter till väntande transaktioner på nätverket får därför utgås ske

[99] Jfr bl.a. Cooper D., Nash, G. & Bertin S., *The CNIL Publishes Report On Blockchain and the GDPR*, Inside Privacy, “https://www.insideprivacy.com/financial-institutions/the-cnil-publishes-report-on-blockchain-and-the-gdpr/”, lydelse 2019-01-03 samt Dipshan, R., *France’s Regulatory Guidance on GDPR, Blockchain Leaves More Questions Than Answers*, Legaltech News, “https://www.law.com/legaltechnews/2018/10/05/frances-regulatory-guidance-on-gdpr-blockchain-leaves-more-questions-than-answers/?slreturn=20190003225633” , lydelse 2019-01-03.

från användarna. En blockutvinnare kan följaktligen inte modifiera vilken data som transaktionen innehåller.

Användarna är med denna bakgrund den aktör som har det största bestämmande inflytandet över ändamål och medel för personuppgiftsbehandlingen. Transaktionsskaparen bestämmer de facto vem den vill utföra en transaktion till, vilken data som transaktionen ska innehålla samt medlet, användandet av blockkedjan, för behandlingen. Det bestämmande inflytandet över ändamål och medel för behandlingen av de uppgifter som finns i varje transaktion får därför anse tillfalla användaren som skapar transaktionen. En sådan slutsats når även CNIL som menar på att användarna kan ses som personuppgiftsansvariga.[100] CNIL uttrycker sig dock enligt min mening något vagt i detta hänseende och lämnar, olyckligtvis, en del följdfrågor i förhållande till ansvar obesvarade. Medan CNIL pekar på att användare *kan* vara personuppgiftsansvariga specificerar de senare att användare *är* personuppgiftsansvariga under särskilda omständigheter. Dels kan det vara fråga om användaren är en fysisk person och att behandlingen görs i relation till en kommersiell aktivitet och dels om användaren är en juridisk person som registrerar personuppgifter på blockkedjan.[101] Resultatet blir motsatsvis att en fysisk person som utför en transaktion på blockkedjan i strikt privat intresse inte bör ses som personuppgiftsansvarig.

Givet att GDPR i artikel 2.2.c skulle vara begränsat avseende det materiella tillämpningsområdet till att inte omfatta sådana privata transaktioner på blockkedjan är frågan vem som då är att se som personuppgiftsansvarig. Sedan en privat transaktion de facto innehåller eller kan innehålla personuppgifter är det inte tillfredsställande att låta en sådan behandling undvika exempelvis rätten till radering. Visserligen nämns i skälen till GDPR att rätten till skydd av personuppgifter inte är en absolut rättighet utan måste vägas mot andra grundläggande rättigheter så som yttrandefrihet och informationsfrihet i enlighet med en proportionalitetsprincip.[102] Det är således fullt rimligt att intresset för de kommersiellt betingade aktiviteterna inte alltid väger lika tungt som de personliga. Utfallet för behandlingen på blockkedjor blir dock något snedvriden när behandlingen sker på samma sätt, i samma system och i samma kontext för såväl privata transaktioner som kommersiella. Även om de flesta medlemsländer har straffrättsliga bestämmelser som behandlar medvetet spridande av kränkande uppgifter är det inom ramen för GDPR inte klart hur ansvarsfrågan för användare bör tolkas.

[100] Se CNILs vägledning s. 1.
[101] Ibid.
[102] Se skäl (4) GDPR.

Utgår vi att CNILs vägledning är att betrakta gällande rätt och att endast transaktioner av kommersiellt betingade användare omfattas av GDPR ska en sådan användare också svara för att radera uppgifterna på begäran enligt artikel 17 i GDPR. CNIL framhäver i sin vägledning att en sådan radering är praktiskt omöjlig för sådan distribuerad databasstruktur som blockkedjor använder sig av. CNIL rekommenderar följaktligen, något naivt, att personuppgiftsansvariga inte bör införa personuppgifter i klartext på blockkedjan utan istället använda sig av kryptografiska scheman för att omvandla personuppgifterna. Vid en senare begäran menar CNIL att den personuppgiftsansvariga då kan radera schemat som använts vid krypteringen vilket föranleder att hashsumman lagrad på blockkedjan inte längre kan betraktas som personuppgifter.[103] Den rekommendationen åsyftar i princip en sorts dataskydd som standard, vilket för oss tillbaks till resonemanget om att blockkedjan funktionellt begränsas.[104] Om en sådan funktionell begränsning endast bör träffa kommersiella användare riskerar skyddet för personuppgifter i GDPR bli ihåligt.

Vad den praktiska innebörden blir med anledning av vägledningen från CNIL är därför svårt att bilda sig en klar uppfattning om. Användare, särskilt kommersiella, torde dock på grund av dess inflytande bestämmande över ändamål och medel i enlighet med CNILs vägledning riskera stå närmst till hand att betraktas som personuppgiftsansvariga. Någon ytterligare faktisk innebörd om vad det innebär i dagsläget kan dock inte med säkerhet sägas då möjligheten att följa de krav GDPR ställer upp på bl.a. radering ter sig omöjlig.

[103] Se CNILs vägledning s. 8 f.
[104] Se avsnitt 4.1.2.

5. Avslutande kommentarer

Som ofta med snabbutvecklande teknologi kommer lagstiftning ofta vara släpande. Rubriken till denna uppsats ställer frågan om blockkedjeteknologin är förenlig med GDPR. I många hänseenden, framförallt i avtalsreglerade blockkedjor, är teknologin i sig definitivt möjlig att efterleva kraven i GDPR. För publika blockkedjor utan sådan reglering riskerar dock svaret att bli nekandes.

Med anledning av blockkedjans väsentliga skillnad i databasstruktur riskerar som i uppsatsen nu klargjort publika blockkedjor att stå i direkt strid med bl.a. bestämmelsen om rätten till radering. Inte heller finns en tillräckligt tillfredsställande vägledning eller praxis på hur ansvarsfrågan praktiskt bör tacklas trots att Bitcoins blockkedja nu varit aktiv i över ett decennium. Vidare nådde Artikel 29-arbetsgruppens redan i sitt yttrande år 2010, i vilken den identifierade frågan om personuppgiftsansvar i komplexa miljöer, slutsatsen att det inte fanns någon anledning att ifrågasätta att begreppen personuppgiftsansvarig och personuppgiftsbiträde skulle vara fortsatt tillämpbara.[105] Huruvida en sådan anledning nu blivit aktuell kan diskuteras. Säkerligen är detta inte endast en fråga som GDPR inrymmer utan måste ses ur ett större perspektiv som inkluderar bl.a. straffrättsliga överväganden och anonymitet som en faktor vid betänkande om praktiska lösningar på området.

Frågan om det går att effektivt passa in blockkedjor i detta regelverk retroaktivt eller om synsättet på databasstrukturen för behandlingar var föråldrad redan vid implementeringen av GDPR har varit föremål för diskussion den senaste tiden.[106] Många synes landa likt Kaufmann i slutsatsen att fastställandet av personuppgiftsansvarig i publika blockkedjor är mycket svårt i decentraliserade system.[107] Inte endast är det en fråga om hur GDPR skulle kunna tillämpas på området utan även om rimligheten och ändamålsenligheten i tillämpningen blir tillfredsställande. Medan det är förståeligt att CNIL inte vill vara för långtgående i sin rapport utan att begränsa den till GDPR är de nu identifierade spörsmålen något som måste adresseras i helhet av lagstiftaren. Huruvida lagstiftaren väljer att betrakta privat betingade transaktioner på blockkedjor som en uppgift för GDPR att omfatta eller lämna till straffrättsliga bestämmelser återstår att se.

[105] Artikel 29-arbetsgruppen, *Yttrande 1/2010*, s. 33.
[106] Se bl.a. Kaufmann s. 124 och s.126 f. samt McLean, S. & Padova, Y., *French Data Authority Issues Guidance on the Interplay between the GDPR and Blockchain Technology*, Baker McKenzie, "https://www.bakermckenzie.com/en/insight/publications/2018/10/french-data-protection-authority-issues-guidance", lydelse 2019-01-05.
[107] Kaufmann. s. 127.

6. Källförteckning

Offentligt tryck

Statens offentliga utredningar

SOU 2008:3, Skyddet för den personliga integriteten, Bedömningar och förslag.

SOU 2016:7, Integritet och straffskydd.

Propositioner

Prop. 2017/18:105, Ny dataskyddslag.

Departementsserien

Ds. 1998:14.

Europarättsligt material

EU-domstolens rättspraxis

C-70/10 Scarlet Extended SA. v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

C-582/14 Breyer v. Bundesrepublik Deutschland.

Yttranden

Artikel 29-arbetsgruppen för skydd av personuppgifter, *Yttrande 1/2010 om begreppen registeransvarig och registerförare*.

Artikel 29-arbetsgruppen för skydd av personuppgifter, *Yttrande 5/2012 om datormoln (cloud computing)*.

Artikel 29-arbetsgruppen för skydd av personuppgifter, *Yttrande 05/2014 om avidentifieringsmetoder*.

Utländskt material

Frankrike

Commission Nationale Informatique & Libertés (CNIL), *Blockchain and the GDPR: Solution for a responsible use of the blockchain in the context of personal data*, "https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf", lydelse 2019-01-02.

Rättsfall

HFD 2012 ref. 21.

Förvaltningsrätten i Stockholm, 2013-10-14, mål nr 9987-12.

Beslut

Datainspektionens beslut 2010-07-02, dnr 686-10.

Datainspektionens beslut 2015-06-22, dnr 2729-2014.

Litteratur

Drescher, Daniel, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, Berkeley CA, 2017.

Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, Studentlitteratur, Lund, 2013.

Sjöberg Magnusson, Cecilia (red.), *Rättsinformatik – juridiken I det digitala informations-samhället*, 2u, Studentlitteratur, Lund, 2016.

Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen: en kommentar*, 4 u., Norstedts Juridik, 2011.

Svensk Juristtidning

Jareborg, Nils, *Rättsdogmatik som vetenskap*, SvJT 2004.

Olsen, Lena, *Rättsvetenskapliga perspektiv*, SvJT 2004.

Tidsskrift for Rettsvitenskap

Sandgren, Claes, *Är rättsdogmatiken dogmatisk?*, TfR 2005.

Internetkällor

Med specificerad författare

Berentsen, Aleksander & Schär, Fabian, *A Short Introduction to the World of Cryptocurrencies*, "files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf", lydelse 2018-10-12.

Cooper Dan, Nash, Gemma & Bertin Sophie, *The CNIL Publishes Report On Blockchain and the GDPR*, Inside Privacy, "https://www.insideprivacy.com/financial-institutions/the-cnil-publishes-report-on-blockchain-and-the-gdpr/", lydelse 2019-01-03.

Dipshan, Rhys, *France's Regulatory Guidance on GDPR, Blockchain Leaves More Questions Than Answers*, Legaltech News, "https://www.law.com/legaltechnews/2018/10/05/frances-regulatory-guidance-on-gdpr-blockchain-leaves-more-questions-than-answers/?slreturn=20190003225633" , lydelse 2019-01-03.

Felten, Ed, *Does Hashing Make Data "Anonymous"?*, Federal Trade Commission, 2012, "www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous", lydelse 2018-12-05.

Garrod, Lucy, *Who is the Data Controller and Processor on your blockchain*, "hackernoon.com/who-is-the-data-controller-and-processor-on-your-blockchain-79dbe6b107d8", lydelse 2018-11-23.

Kaufmann, Jörg, *Blockchain meets Data Privacy – Blockchain and the Data Controller*, Legal Revolutionary, 120, "legal-revolution.com/images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf", lydelse 2018-12-06.

LeMahieu, Colin, *Nano: A Feeless Distributed Cryptocurrency Network*, "nano.org/en/whitepaper", lydelse 2018-10-09.

Lundqvist, Daniel, Gustafsson, Fredrik, Tomas da Costa, Emily, Bogsjö Österberg, Hanna, Jarkell, Emma & Sahibli, Tahmina, *GDPR – några tillämpningsfrågor*, Kahn Pedersen, "kahnpedersen.se/wp-content/uploads/2017/10/KahnPedersen_GDPR_web.pdf", lydelse 2018-12-06.

Lyons, Tom, *Blockchain Innovation Europe*, The European Union Blockchain Observatory and Forum, www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf", lydelse 2019-01-02.

Matzutt, Roman, Hiller, Jens, Henze Martin, Ziegeldorf Jan Henrik, Müllman, Dirk, Hohlfeld, Oliver & Wehrle, Klaus, *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin*, International Financial Cryptography Association, "https://fc18.ifca.ai/preproceedings/6.pdf", lydelse 2019-01-04.

McLean, Sue & Padova, Yann, *French Data Authority Issues Guidance on the Interplay between the GDPR and Blockchain Technology*, Baker McKenzie, "https://www.bakermckenzie.com/en/insight/publications/2018/10/french-data-protection-authority-issues-guidance", lydelse 2019-01-05.

Merkle, Ralph Charles, *Secrecy, Authentication, and Public Key Systems*, Technical Report No. 1979-1, "www.merkle.com/papers/Thesis1979.pdf", lydelse 2018-10-14.

Nakamoto, Satoshi, *Bitocin: A Peer-to-Peer Electronic Cash System*, "https://bitcoin.org/bitcoin.pdf", lydelse 2018-10-05.

Okupski, Krzysztof, *Bitcoin Developer Reference: Working Paper*, 2016, "https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf ", lydelse 2018-10-05.

Perez, Beatrice, Musolesi, Mirco & Stringhini, Gianluca, *You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information*, "www.ucl.ac.uk/~ucfamus/papers/icwsm18.pdf", lydelse 2018-12-10.

Schär, Fabian, *Certificates based on Blockchain Technology*, "cif.unibas.ch/fileadmin/user_upload/cif/press_release_EN.pdf", lydelse 2018-10-10.

Wang, Di, *Secure Implementation of ECDSA Signatures in Bitcoin*, "http://www.nicolascourtois.com/bitcoin/thesis_Di_Wang.pdf", lydelse 2018-10-14.

Utan specificerad författare

Bitcoin.org, *Block Size Limit, "*https://bitcoin.org/en/glossary/block-size-limit", lydelse 2018-10-14.

Blockchain.com, *Block #545180*, "www.blockchain.com/btc/block/00000000000000000001084d6d26cd688036887daaa505afbf83ad677c9b67fc6", lydelse 2018-10-09.

CoinMarketCap, *All Cryptocurrencies | CoinMarketCap | Cryptocurrencies by market capitalization*, "www.coinmarketcap.com/historical/20180909/" , lydelse 2018-09-09.

Federal Information Processing Standards Publication, *Secure Hash Standard (SHS)*, "nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf", lydelse 2018-10-14.

Lantmäteriet, *Framtidens husköp i blockkedjan*, "www.lantmateriet.se/contentassets/ee30ed78dcdb4dd698cf454001369cf8/blockkedjan-framtidens-huskop.pdf", lydelse 2018-10-11.

Stockholmsuniversitet
Juridiskainstitutionen
SE-106 91 Stockholm
Telefon/Phone: 08 – 16 20 00
www.su.se