GÖTEBORGS UNIVERSITET
HANDELSHÖGSKOLAN

BITCOIN OCH BORGENÄRERNA

En kryptovaluta i konflikt med konkursinstitutet?

Examensarbete Juristprogrammet 30 hp.
Höstterminen 2017
Juridiska Institutionen
Handelshögskolan vid Göteborgs universitet

Författare: Stina Karinsdotter
Handledare: Kristoffer Schollin

SAMMANFATTNING

2008 lanserades Bitcoin, den första blockkedjan. Tio år senare är Bitcoin hetare än någonsin och värdeökningskurvan har hösten 2017 varit brantare än för något annat egendomsslag i mannaminne.[1] Men det är inte bara den fluktuerande kursen som gör Bitcoin till en vilde.

Den drivande tanken bakom Bitcoin är att skapa en möjlighet för människor att på ett oberoende sätt utföra värdeöverföringar *peer-to-peer*, det vill säga utan inblandning av stater, banker och liknande institut som mellanhänder. Lösningen bygger på programmering och stark kryptografi. Det finns inget centrum eller styrande rättssubjekt bakom systemet.

Kryptografiska lösningar i Bitcoin medger också säker autentisering mot systemet utan krav på koppling till användarens verkliga identitet. Motiven bakom detta är ideologiska och syftar till att vår integritet ska vara lika enkel att skydda i den digitala miljön som i den fysiska. Varje transaktion du gör innehåller information om ditt livsmönster och därigenom om dig. Enligt de ideologiska strömningar som ligger bakom Bitcoin bör detta vara din privata information. Du själv ska ha kontrollen över vem som får ta del av den.

Ambitionen med detta arbete är att undersöka vad som händer när Bitcoin, ett decentraliserat system som motsätter sig all inblandning av utomstående parter och som därtill förespråkar rätten till anonymitet, möter konkursinstitutet som i allt väsentligt bygger på en motsatt logik och som därtill är beroende av åtkomst till såväl egendom som information om inblandade rättssubjekt för att fungera.

Genom en redogörelse av några av de mest centrala ideologiska hållpunkterna som legat bakom utvecklingen av blockkedjan och Bitcoin belyses *varför* systemet är utformat som det är. Genom en relativt djuplodande redogörelse för de tekniska aspekterna av Bitcoin förklaras *hur* systemet fungerar i praktiken. Därefter söker uppsatsen att utreda vad Bitcoins särart får för *konsekvenser*, dels generellt för den förmögenhetsrättsliga klassificeringen och därefter mer specifikt vid en hantering i konkurs.

Min tes är att ett *peer-to-peer*-nätverk bygger på en tvåpartslogik där tredjemansförhållanden inte beaktas. Bitcoin, vars intention varit att eliminera behovet av betrodda intermediärer vid värdeöverföringar, får som bieffekt att skyddet för tredje man undergrävs i obeståndssituationer.

[1] Morris, D. Z. (3 december 2017). *Here's What Bitcoin's Smartest Skeptics are Telling Investors*. Hämtat från fortune.com: http://fortune.com/2017/12/03/heres-what-bitcoins-smartest-skeptics-are-telling-investors/ den 11 december 2017.

INNEHÅLLSFÖRTECKNING

1 INTRESSET FÖR BITCOIN OCH HUR JAG GÅTT TILL VÄGA 5

1.1 BITCOIN OCH KONKURSINSTITUTET – EN PROBLEMATISK SYSTEMKROCK? 5
1.1.1 HUVUDSAKLIGT SYFTE 5
1.1.2 FÖRFATTARENS AMBITION OCH FÖRHOPPNINGAR I ÖVRIGT 6
1.2 METOD 7
1.2.1 OLIKA METOD FÖR OLIKA DELAR 7
1.3 ÄMNESMOTIVERING OCH AVGRÄNSNINGAR 9
1.3.1 FRÅN BLOCKKEDJA TILL BITCOIN 9
1.3.2 FRÅN JURIDIK I ALLMÄNHET TILL KONKURSINSTITUTET I SYNNERHET 10
1.4 ANVÄNDNING OCH ÖVERSÄTTNING AV SÄRSKILDA ORD OCH BEGREPP 12
1.5 EN ÖVERBLICK ÖVER DEN FORTSATTA DISPOSITIONEN 14

2 CYPHERPUNK OCH LIBERTARIANSKA IDEOLOGIER 16

2.1 DET KRYPTOGRAFISKA KRIGET FÖR INTEGRITETSSKYDDET 16
2.1.1 A CYPHERPUNK'S MANIFESTO 16
2.1.2 DIFFIES ASYMMETRISKA NYCKLAR – ETT KRYPTOGRAFISKT GENOMBROTT 18
2.1.3 PRETTY GOOD PRIVACY – FÖR ALLA 19
2.1.4 BITCOIN – NAKAMOTO LÖSER PROBLEMET MED DUBBELUTGIFTER 19
2.2 BITCOIN OCH LIBERTARIANISMEN 20
2.2.1 BITCOIN, LIBERTARIANISMEN OCH KONKURSINSTITUTET 22

3 BLOCKKEDJAN BITCOIN "FOR DUMMIES" (OCH DE FLESTA JURISTER) 24

3.1 FEM VIKTIGA GRUNDER FÖR ATT FÖRSTÅ BITCOIN 25
3.2 SKILLNADEN PÅ BLOCKKEDJA, PROTOKOLL, COINS OCH TOKENS 26
3.3 DE CENTRALA DELARNA I DEN TEKNISKA UPPBYGGNADEN 28
3.3.1 HUVUDBOKEN 28
3.3.2 TRANSAKTIONEN OCH AUTENTISERING GENOM DIGITALA SIGNATURER 28
3.3.3 HUR NODERNA HÅLLER ORDNING PÅ HUVUDBOKEN GENOM TRANSAKTIONSKEDJOR 30
3.3.4 VARFÖR DET KALLAS "BLOCKKEDJA" OCH VAD BLOCKEN FYLLER FÖR FUNKTION 31
3.4 ÖVRIGA TEKNISKA ASPEKTER SOM ÄR BRA ATT KÄNNA TILL 33
3.4.1 HUR MAN HÅLLER SINA BITCOINS SÄKRA OCH LITE OM OLIKA PLÅNBOKSTYPER 33
3.4.2 NÅGOT OM ANONYMITET 35
3.4.3 VAD HÄNDER OM DEN MÄNSKLIGA FAKTORN FELAR? 36
3.4.4 HUR SÄKRA ÄR NYCKLARNA? 36

4 BITCOIN SOM EKONOMISKT OCH FÖRMÖGENHETSRÄTTSLIGT FENOMEN 38

4.1 EGENDOM, OBJEKTSFIKTION OCH "ÄGANDERÄTT" 38
4.1.1 "ICKE-FYSISK" EGENDOM 39
4.2 VAD FÖR SORTS EGENDOM ÄR BITCOIN? 39
4.2.1 FINANSIELLT INSTRUMENT? 40
4.2.2 VALUTA, LEGALT BETALNINGSMEDEL ELLER BARA ETT BETALNINGSMEDEL? 41

4.2.3 FORDRAN ELLER FIATPENGAR – LÄMPLIGA LIKNELSER? 43
4.2.4 HANDELSVARA? 46
4.3 BETYDELSEN AV BRISTEN PÅ FYSISKA EGENSKAPER 47
4.3.1 RELEVANT BETALNINGSPARADIGM – EN RELEVANT FRÅGA? 47
4.3.2 KONTANTER, KONTOPENGAR, KRYPTOVALUTA 48
4.3.3 DIGITAL BESITTNING UTAN OBJEKTSFIKTION – EN MÖJLIGHET? 54

5 BITCOIN I KONKURS 57

5.1 INLEDNING 57
5.1.1 INGÅR BITCOIN I KONKURSBOET 57
5.2 BORGENÄRSSKYDD – GRÄNSDRAGNING FÖR PRIORITET 59
5.2.2 BORGENÄRSSKYDDSFALLEN 61
5.2.3 SEPARATIONSRÄTTSFALLEN 63
5.2.4 MÖJLIGHETER TILL PANTSÄTTNING AV BITCOIN 65
5.2.5 MÖJLIGHET TILL ESCROW-LIKNANDE ARRANGEMANG UTAN TREDJE PART 66
5.2.6 NÅGOT OM FÖRHÅLLANDET TILL FÖRETAGSHYPOTEKSUNDERLAGET 66
5.3 BORGENÄRERS SKYDD MOT GÄLDENÄRENS OBEHÖRIGA FÖRFOGANDEN 67
5.3.1 EN KONFLIKT MELLAN MOTSTÅENDE LOGIKER 67
5.3.2 SÄKERSTÄLLANDE AV EXEKUTIONSUNDERLAGET 68
5.3.3 BETYDELSEN AV ANONYMITET OCH BEVISSVÅRIGHETER 69
5.3.4 KONKURSFÖRVALTARENS ANSVAR OCH NÅGOT OM FÖRSÄKRING? 70

6 NÅGRA AVSLUTANDE REFLEKTIONER 72

KÄLLFÖRTECKNING 73

RÄTTSFALLSREGISTER 77

1 INTRESSET FÖR BITCOIN OCH HUR JAG GÅTT TILL VÄGA

1.1 Bitcoin och konkursinstitutet – en problematisk systemkrock?

1.1.1 Huvudsakligt syfte

Allt fler pratar om blockkedjor och många menar att de kommer att revolutionera hela finanssektorn och på sikt även leta sig in i en rad andra branscher. Det pratas om ett nytt paradigm, om ett nästa stort steg efter internet, om ett ”internet för värde”.[2]

I och med Bitcoins (och därmed även blockkedjans) lansering 2008, lanserades också en lösning på ett länge diskuterat problem inom kryptografikretsar,[3] nämligen hur ett system kan verifiera värdeöverföringar utan inblandning av betrodda intermediärer[4] och utan att detta medför risk för dubbelutgifter. Det verkligt revolutionerade med blockkedjan är just att det går att *överföra* digitala resurser i ett peer-to-peer nätverk. Med överföra avses här överföra på så vis att *avsändaren inte längre har åtkomst till resursen samtidigt som mottagaren ges exklusiv åtkomst*. Detta innebär en stor skillnad från när man i vardagligt tal använder överföra synonymt med att *skicka över en kopia,* vilket normalt är fallet då information överförs på internet. Det är denna skillnad som gör att blockkedjan anses kunna *överföra värde* och det är detta som gör att blockkedjan förutspås utgöra ett nytt paradigm i paritet med internet. I blockkedjans egen värld finns inga gränser för vad som går att göra i en blockkedja. Men vad händer när de tekniska konstruktionerna möter de juridiska?

Att se Bitcoin som en utveckling sprungen ur ren teknik-fetischism leder troligen till en underskattning av fenomenets potential och vilja att förändra spelplanen. Bakgrunden till utvecklingen är främst ideologisk med integritet som hjärtefråga och rötterna hårt förankrade i den libertarianska skolan.

---

[2] Se bl.a. Greenhalgh, H. (21 september 2016). *Blockchain, Asset managers quick to adopt blockchain*. Hämtat från Financial Times: https://www.ft.com/content/ee6d8454-7f27-11e6-bc52-0c7211ef3198 den 12 december 2017;
Marr, B. (21 september 2017). *14 Things Everyone Should Know About Blockchains*. Hämtat från Forbes: https://www.forbes.com/sites/bernardmarr/2017/09/21/14-things-everyone-should-know-about-blockchains/#4097154252a7 den 12 december 2017;
The Economist. (9 maj 2015). Blockchain, *The next big thing*. Hämtat från The Economist: https://www.economist.com/news/special-report/21650295-or-it-next-big-thing den 12 december 2017;
Yaw-Owusu, F. (1 november 2017). *Cryptocurrencies, Blockchain: Moving from the Internet of Information to the Internet of Value*. Hämtat från The Market Mogul: https://themarketmogul.com/blockchain-information-internet-value/ den 12 december 2017.

[3] Kryptografi är sätt att utforma kommunikation på ett sådant sätt att den inte går att avläsa eller avlyssna för obehöriga. Ett mycket enkelt exempel är rövarspråket, som är svårt att förstå för den som inte vet reglerna för hur ord förändras till rövarspråk. Det handlar alltså om att med hjälp av ett system av regler, en så kallad ”kryptografisk nyckel” översätta ett vanligt meddelande till krypto, en hemlig kod. Mottagaren behöver då både det hemliga meddelandet och nyckeln för att kunna översätta kryptot till vanliga ord.

[4] Betrodda intermediärer är min egen terminologi inspirerad av engelskas ”trusted third parties”, som frekvent används för att beskriva vad Bitcoin eliminerat, tillsammans med Lindskogs terminologi; betalning-eller mottagarintermediärer för de kontohållare som förmedlar en transaktion med kontopengar.

Den drivande tanken bakom Bitcoin är att skapa möjlighet för människor att på ett oberoende sätt utföra transaktioner *peer-to-peer*, det vill säga utan inblandning av stater, banker och liknande institut. Lösningen bygger på programmering och stark kryptografi. Det finns inget centrum eller styrande rättssubjekt bakom systemet. Kryptografiska lösningar medger också säker autentisering mot systemet utan krav på koppling till användarens verkliga identitet. Syftet är att vår integritet ska vara lika enkel att skydda i den digitala miljön som i den fysiska. Varje transaktion du gör innehåller information om ditt livsmönster och därigenom om dig. Enligt de ideologiska strömningar som ligger bakom Bitcoin bör detta vara din privata information. Du själv ska ha kontroll över vem som får tillgång till informationen.

Även om mycket har skrivits och skrivs om blockkedjor och kryptovalutor är det, trots otvivelaktig relevans, relativt lite av den text som produceras som ligger inom ramen för det juridiska fältet. Även de ideologiska aspekterna saknas i de flesta framställningar.

Syftet med detta arbete är att undersöka vad som händer när Bitcoin, ett decentraliserat system som motsätter sig all inblandning av utomstående parter och som därtill förespråkar rätten till anonymitet, möter konkursinstitutet som är beroende av åtkomst till såväl egendom som information om inblandade rättssubjekt för att fungera och som i allt väsentligt bygger på en motsatt logik med en central styrning från en utomstående.

Min tes är att ett *peer-to-peer*-nätverk bygger på en tvåpartslogik där tredjemansförhållanden inte beaktas. Bitcoin, vars intention varit att eliminera behovet av betrodda intermediärer vid transaktioner, får som bieffekt att skyddet för tredje man undergrävs i obeståndssituationer.

1.1.2 Författarens ambition och förhoppningar i övrigt

Utöver mitt huvudsakliga syfte, som beskrivits ovan, hoppas jag genom kapitel 2 kunna intressera läsaren för de ideologier och åsiktsströmningar som legat bakom utvecklingen av Bitcoin och blockkedjan. I mina egna efterforskningar har jag upplevt att den ideologiska bakgrunden hamnat just i bakgrunden och att förgrunden till stor del tagits över av teknikfetischism. Det tycker jag är synd. En bakgrundsförståelse gör det lättare att se vilka intressemotsättningar som kan uppstå och i övrigt sätta fenomenet i en större och behövlig kontext.

Jag vill också, genom kapitel 3, öka den tekniska förståelsen för blockkedjan i allmänhet och kryptovalutan Bitcoin i synnerhet. En viktig del av juristens roll är att hålla sig uppdaterad och allmänbildad. Författandet av detta arbete har erbjudit mig en möjlighet att sätta mig in i kryptovalutornas och blockkedjans något svårtillgängliga värld. Kapitlet är mitt försök att förmedla den förförståelse av tekniken som jag själv har behövt skaffat mig under arbetets gång. Kapitlet är tänkt som en kunskapsplattform som jag tror att läsaren behöver stå på för att fullt kunna tillgodogöra sig efterföljande kapitel. Jag hoppas att den kunskapsplattform jag sökt bygga även ska vara till nytta för en jurist som har anledning att snabbt sätta sig in i tekniken i andra syften än att tillgodogöra sig innehållet i detta arbete.

Slutligen hoppas jag att genom kapitel 4 kunna visa på vad som gör Bitcoin speciellt från ett förmögenhetsrättsligt perspektiv. Framförallt vill jag i denna del utmana juristens tendens att använda en egendoms fysiska eller icke-fysiska natur som utgångspunkt för klassificering och problemhantering. Jag kommer istället att föreslå ett, som jag ser det, mer pragmatiskt förhållningssätt som utgår ifrån de egenskaper hos egendom som i praktiken har den avgörande betydelsen för kontrollen över den.

1.2 Metod

1.2.1 Olika metod för olika delar

På ett mycket övergripande plan har detta arbete fyra huvudsakliga delar (kapitel 2, 3, 4 och 5), varav endast de två senare använder sig av ett juridiskt perspektiv i egentlig mening. Vad gäller blockkedjan och Bitcoin är mitt intryck att den mesta och bästa informationen finns fritt på internet. Det ligger i Bitcoins kultur och intresse att sprida information på det viset. Det är på nätet det går att hitta ett inifrånperspektiv. Den media som bevakar kryptovalutor tenderar också att i första hand vara nätbaserad.

1.2.1.1 Cypherpunk och ideologierna bakom Bitcoin

Den första delen är en ideologisk bakgrund. I denna del har jag inledningsvis sökt runt på internet för att försöka förstå om, och i så fall vilka, ideologier som legat bakom Bitcoin-fenomenet. Jag har här valt att utgå från Eric Hughes tongivande text *A Cypherpunk's Manifesto* för att försöka återge ett inifrånperspektiv där de ideologiska rötterna tydligt framgår. Jag har därefter byggt på framställningen och tar med läsaren genom historien med hjälp av ett axplock av tekniska framsteg och betydande frontfigurer. Kapitlet gör inte anspråk på att vara varken analytiskt eller vetenskapligt, utan ska ses som en kortare sammanfattning av beskrivande karaktär för att ge läsaren en inblick i den ideologiska bakgrunden.

1.2.1.2 Blockkedjeteknik och Bitcoin

För att själv förstå Bitcoin och blockkedjan har jag först och främst utgått ifrån Satoshi Nakamotos berömda white paper: *Bitcoin: A Peer-to-Peer Electronic Cash System.*[5] Dokumentet släpptes vid Bitcoins lansering 2008 och är en översiktlig genomgång av systemet författad av dess skapare.[6] För att bättre förstå de olika delarna samt fylla ut på områden som inte behandlas i Nakamotos white paper har jag läst mängder av teknikbloggar, forumtrådar, nyhetsartiklar m.m. Jag har också använt YouTube flitigt för att titta på föreläsningar och olika förklarande filmer från teknikvurmande YouTube-profiler. Eftersom programmering och kryptografi inte är områden jag själv behärskar eller har någon utbildning inom (och blockkedjan är en mycket avancerad lösning även för de som behärskar fältet) är det förstås svårt för mig att förhålla mig kritisk till mina källor. För att få en uppfattning av vilka källor som är tillförlitliga, har jag bekräftat att den information en viss källa ger stämmer överens

[5] Nakamoto, S. (31 oktober 2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Hämtat från bitcoin.org: https://bitcoin.org/bitcoin.pdf den 12 december 2017.
[6] Satoshi Nakamoto förmodas vara en pseudonym. Under årens lopp har det spekulerats i vem eller vilka som kan tänkas ligga bakom pseudonymen. Nakamotos verkliga identitet är än idag obekräftad.

med andra källor. När viss information återges från flera håll bedömer jag att det är större sannolikhet att informationen är tillförlitlig och stämmer. Jag har sedan med utgångspunkt i vissa källor som jag funnit särskilt användbara försökt att göra en sammanställning som jag tror ska vara begriplig för en utomstående som liksom jag inte har några förkunskaper.

1.2.1.3 Bitcoin som finansiellt fenomen

Inte heller de finansiella aspekterna ligger inom ett område jag behärskar. Till skillnad från kryptografins och programmeringens värld är de finansiella auktoriteterna, i form av framstående ekonomer och finansiella rådgivare och analytiker, mer allmänt kända. Det har därför varit lättare att här hitta källor som kan värderas såsom trovärdiga även om jag inte mer än lekmannamässigt kan bedöma rimligheten i olika synsätt.

1.2.1.4 Juridiska aspekter

Tonvikten i kapitel fyra och fem ligger på juridisk analys. Jag har i stora delar av mitt arbete tagit avstamp i Emil Elgebrants bok *Kryptovalutor*.[7] Boken, som gavs ut 2016, är mig veterligen det hittills enda, eller i vart fall mest omfattande, juridiska arbete som gjorts ur ett svenskt perspektiv på ämnet kryptovaluta. *Kryptovalutor* är i sin helhet runt hundra sidor och är långt ifrån uttömmande. Den inventerar olika områden där rättslig problematik kring kryptovaluta kan tänkas uppkomma i svensk rätt och skisserar olika argumentationslinjer utan att göra några djuplodande analyser. Även om jag många gånger känt att min egen uppfattning, eller i vart fall infallsvinkel, skiljer sig från Elgebrants, har boken varit oerhört värdefull för mig i mitt arbete. Dels för att kunna navigera mellan olika delar som kan vara värda att belysa, dels för att ha en ståndpunkt som jag kan förhålla mig till genom att hålla med eller problematisera.

Elgebrants intresse för kryptovaluta tycks sammankopplat med hans tidigare arbeten kring utsläppsrätter och elcertifikat[8] som liksom kryptovaluta var nya företeelser när de kom. Personligen uppfattar jag detta som både en styrka och en svaghet. Å ena sidan kan författaren dra nytta av tidigare erfarenheter och hitta liknande argumentationsvägar, vilket är tacksamt när ett ämne är så nytt och outforskat. Samtidigt ser jag en risk i detta då det lätt leder till att man uppmärksammar likheter men blundar för väsentliga skillnader som hade kunnat påverka argumentationen i en annan och outforskad riktning.

Det ligger kanske närmast till hands att säga att jag använt mig av en rättsdogmatisk metod i de juridiska delarna. Begreppet ”rättsdogmatisk metod” är dock så brett att det egentligen säger mycket lite. Förvisso har jag använt mig av exempelvis lagtext, rättsfall och namnkunnig doktrin på området för att förstå och argumentera. Men rättsdogmatisk metod beskrivs vanligen som inriktad på att tolka och systematisera ”gällande rätt”. Kan man då tala om en rättsdogmatisk metod när analysen rör ett nytt fenomen där det ännu inte finns några tyngre rättskällor att helt luta sig mot?

[7] Elgebrant, E. (2016). Kryptovalutor, Särskild rättsverkan vid innehav av Bitcoins och andra liknande betalningsmedel.
[8] Här åsyftas främst Elgebrants avhandling Ägande och värde av utsläppsrätter och andra handelsobjekt från 2012.

Jag tillhör de som tycker att begreppet ”gällande rätt” skaver. Det får juridiken att förefalla mer statisk och svartvit än den i själva verket är. Men om man väljer att se på gällande rätt som de normer som kan väntas få genomslag om ett fall skulle prövas vid domstol, torde den rättsdogmatiska metoden vara den mest användbara för att göra en prognos av utfallet, även i de fall fenomenet är ungt och underlaget tunt.

När redan etablerade fenomen ska analyseras används rättsdogmatisk metod snarast för att utröna vad som brukat gälla, *de lege lata,* och prognosen bygger sedan på sådana efterforskningar. När ett nytt fenomen, såsom Bitcon, ska analyseras kommer metoden istället att användas för att mejsla fram nya argumentationslinjer, *de lege ferrenda*. I båda fallen handlar det dock om att upprätthålla vissa grundläggande värden. Kring etablerade fenomen finns i stor utsträckning ett samförstånd om vilka normer som ska tillämpas. Med nya fenomen måste ett sådant samförstånd skapas. Om rättsdogmatisk metod framgent ska kunna användas för att prognostisera hur rätten kommer att tillämpas måste samma metod omvänt användas för att skapa koherens kring vilka argumentationslinjer som, när problemen uppstår, bör tillämpas. En sådan koherens bygger i grunden på vissa centrala värden, en teoretisk systematik baserad på ändamålsenlighet och praktisk genomförbarhet.

I en strävan efter att hitta argumentationslinjer som motiveras av dessa värden och därmed har större möjlighet att skapa koherens kring valet av normer, har jag så att säga burit runt på den rättsdogmatiska verktygslådan genom mitt arbete. Jag har dock haft ett allt annat än strikt förhållningssätt. Jag har i mycket låtit min nyfikenhet och mitt intresse styra och jag har tillåtit mig själv att fritt reflektera över tänkbara problemsituationer. Jag har också, *de lege ferenda*, sökt konstruera en sakrättslig systematik kring Bitcoin, som delvis försöker att fungera tillsammans med den sakrättsliga idévärld som redan existerar, men i vissa delar även medvetet sökt bryta mot vissa vedertagna tankekonstruktioner för att undersöka om det går att skräddarsy nya, pragmatiska lösningar.

1.3 Ämnesmotivering och avgränsningar

1.3.1 Från blockkedja till Bitcoin

1.3.1.1 Blockkedjan

Blockkedjan innebär en mängd nya möjligheter och användningsområden med juridisk relevans. Blockkedjan kan användas för att förvara och överföra kryptovaluta, men den kan exempelvis också användas som en säker databas för att spåra en vara till dess ursprung, föra register över, eller på annat sätt hantera andra tillgångar än kryptovalutor.

Blockkedjans potential är något som bland annat Lantmäteriet för närvarande undersöker med avseende på det svenska fastighetsregistret och musiktjänsten Spotify har investerat i med förhoppning om en rättvisare, mer transparent och lönsam miljö för kreatörer och

rättighetshavare.[9] Ett annat område som det pratas mycket om är så kallade ”smarta kontrakt” som går att programmera och lägga ut som program på en blockkedja.

Att behandla alla de nya möjligheter och svårigheter som blockkedjan medför inom ramen för ett examensarbete är inte möjligt. Den här uppsatsen kommer därför att fokusera på kryptovalutor och då främst Bitcoin.

1.3.1.2 Kryptovaluta

Anledningen till att jag valt detta fokus är att kryptovalutor är det område som under uppsatsens tillblivelse är av störst praktisk betydelse. Det finns därför ett mer konkret underlag att studera i jämförelse med andra potentiella användningsområden för blockkedjeteknik. Jag tror också att det finns poänger med att ”börja från början” och utforska det första och mest utvecklade användningsområdet av blockkedjan. Alternativen hade tvingat mig att lägga på det ytterligare lager av teoretisering som hade blivit nödvändigt om jag valt att hantera de potentiella framtida användningsområdena. Förhoppningsvis kan juridiska insikter från en analys av det första användningsområdet, kryptovaluta, vara till nytta även för kommande användningsområden.

1.3.1.3 Bitcoin

Bitcoin är den första och i nuläget överlägset största kryptovalutan. Det känns därför naturligt att välja att avgränsa framställningen till just Bitcoin i de sammanhang det inte går att dra några generella slutsatser som har bäring för alla varianter av kryptovaluta. Den centrala gemensamma nämnaren är att kryptovalutorna bygger på samma databaskonstruktion, blockkedjan, som bland annat möjliggör värdeöverföring i ett digitalt, decentraliserat *peer-to-peer*-nätverk. Men blockkedjan kan, som nämnts ovan, också användas till andra saker än kryptovalutasystem och kryptovalutasystemen kan ha väsentliga skillnader sinsemellan. Vad databasen används till avgörs av det protokoll som anger reglerna för databasens användning och funktioner. Bitcoin är ett sådant protokoll och det använder blockkedjan till att skapa, lagra och överföra Bitcoin. Eftersom Bitcoin är den idag mest utbredda företeelsen tänker jag mig att den obeståndsrättsliga problematik som kan uppstå kring kryptovaluta i praktiken främst kommer att röra sig om Bitcoin-fallet.

1.3.2 Från juridik i allmänhet till konkursinstitutet i synnerhet

1.3.2.1 ”Objektet”

Sakrätten har alltid intresserat och fängslat mig. Ordet ”sak” tenderar att föra tankarna till fysiska ting. Atomer i en sådan formation som gör att de går att greppa och förflytta.

[9] Se bl.a. Lantmäteriet. (24 augusti 2016). Lantmäteriet. Hämtat från Lantmäteriet har tittat på blockkedjetekniken: https://www.lantmateriet.se/sv/Nyheter-pa-Lantmateriet/lantmateriet-har-tittat-pa-blockkedjetekniken/ den 4 december 2017 och
Wallenberg, B. (26 april 2017). Dagens Industri, Digital. Hämtat från Spotify köper blockkedjebolag: https://digital.di.se/artikel/spotify-koper-blockkedjebolag den 12 december 2017.

Exemplen i undervisningen tenderar att bestå av bilar, maskiner, spannmål och liknande välkända, konkreta och greppbara ting. På ytan skiljer sig Bitcoin väsentligt från de gängse skolboksexemplen. Det viktiga med sakrättens saker är emellertid inte att de bokstavligen går att ta på, utan deras materiella integritet. Med materiell integritet menar jag förmågan att ge innehavaren exklusiv och av omgivningen oberoende rådighet. Den materiella integriteten kommer i skolboksexemplen av sakernas fysiska egenskaper. Att fysisk form innebär en hög grad av materiell integritet innebär inte omvänt att materiell integritet kräver fysisk form. Som kommer att framgå nedan i avsnitt 4.3 är min uppfattning att Bitcoin har mycket hög materiell integritet. Till skillnad från skolboksexemplen beror den materiella integriteten inte på fysiska egenskaper utan på banbrytande programmering och kryptografiska lösningar. Att sätta Bitcoin i en sakrättslig kontext föreföll som ett bra sätt att visa på Bitcoins allt annat än iögonfallande särdrag.

1.3.2.2 Subjekten

Som nämnts ovan är Bitcoin är ett decentraliserat peer-to-peer nätverk där värdeöverföringar görs direkt mellan de inblandade subjekten utan förmedling av en betrodd intermediär såsom en bank. Dessutom möjliggörs och förespråkas en hög grad av anonymitet i systemet. Detta är avsiktligt menat att hindra utomstående från insyn och påverkan på systemet. Systemet är kort sagt utformat så att användarnas mellanhavanden ska kunna förbli deras ensak om de så önskar. Jag tyckte mig i detta se hur *peer-to-peer*-upplägget kunde utgöra en potentiell konfliktyta med rättsfiguren tredje man. Detta var något jag ville undersöka närmare.

1.3.2.3 Konkursinstitutet

Konkursinstitutet, med sin ingripande och centraliserade förvaltning samt behov av information om inblandade parters mellanhavanden kändes som den bjärta kontrast jag var ute efter. Dessutom är sakrätten ett mycket närvarande inslag i konkurssituationen, vilket skulle ge mig anledning att också lyfta frågan om materiell integritet. På det hela taget matchades mitt kunskapsintresse väl genom en avgränsning till konkurssituationen.

1.4 Användning och översättning av särskilda ord och begrepp

På grund av att arbetet innehåller dels terminologi från olika branschperspektiv, dels från både svenska och engelska har jag behövt göra en del val gällande vilken term som ska användas för en viss betydelse. I vissa fall har jag också funnit det lämpligt att konstruera nya termer, främst genom fria översättningar till svenska. Målsättningen har varit att göra texten lättläslig och begriplig, samtidigt som läsaren ska kunna känna igen sig och göra korrekta paralleller till andra källor på området. Nedan följer ett antal ord, begrepp och förkortningar som jag tror att läsaren har nytta av att få en närmare förklaring av.

Betrodd intermediär
Detta är min egen terminologiska konstruktion. Inspirerad av engelskans ”trusted third parties”, som frekvent används för att beskriva vad Bitcoin eliminerat, tillsammans med Lindskogs terminologi; betalning-/mottagarintermediärer för de kontohållare som förmedlar en transaktion med kontopengar. Termen används i detta arbete för att beskriva vad som saknas i Bitcoin-systemet vid en jämförelse med exempelvis banker, och betalningstjänster av olika slag.

Bitcoin(s) och Bitcoin-systemet
Med Bitcoin menar jag i regel själva valutan. Jag har vid behov använt pluralformen Bitcoins eftersom en engelsk pluraländelse kändes mer passande än en svensk. När jag åsyftar helheten, det vill säga protokollet, huvudboken, användarna, valutan osv. har jag använt termen Bitcoin-systemet.

Blockkedja
Blockkedjan är själva tekniken. Med blockkedja menas förenklat att så kallade *block* med information länkats kryptografiskt på ett sådant sätt att förändringar i ett tidigare block kommer att invalidera informationen i de senare. Själva grundidén bygger på att information länkas kronologiskt så att det inte ska gå att manipulera historiken.

BTC
Förkortningen för valutan Bitcoin. En Bitcoin skrivs som 1 BTC.

Coins
Coins kallas de enheter som inte representerar något annat värde än det värde enheten själv har på marknaden. En Bitcoin (BTC) är, som namnet antyder, ett exempel på en typ av coin eller mynt. Tanken med coins är att de ska gå att använda som pengar.

Cypherpunk(are)
Eftersom Cypherpunk-rörelsen är starkt kopplad till internet, vars ”modersmål” är engelska, har jag valt att inte översätta termen som på svenska närmast hade översatts till shiffer- eller krypto-punkare. Cypherpunk är en ordlek med det mer kända begreppet cyberpunk och cypher, d.v.s. chiffer eller krypto.

Dubbelutgifter
Egen översättning av engelskans *double spendings*. Dubbelutgifter är ett problem främst för digitala betalningsmedel. Problemet uppstår på grund av att digital information, till skillnad från kontanter, normalt sätt kan reproduceras relativt enkelt. Med digitala betalningsmedel finns därför vanligen en högre risk för att innehavaren gör en kopia av sina medel som överförs samtidigt som denne själv behåller originalet.

Escrow
Escrow är ett avtalsarrangemang där en tredje part förvaltar och disponerar över pengar på uppdrag av de primära avtalsparterna. Escrow-upplägg används bland annat när parter har avtalat om tilläggsköpeskilling. Tilläggsköpeskillingen hålls i sådant fall hos den tredje parten tills det att köparen bekräftar att säljaren uppfyllt de villkor som uppställts för att tilläggsköpeskillingen ska betalas ut.

Huvudbok
Med huvudbok menas i detta arbete engelskans Open-Ledger i blockkedjekontexten. Jag tycker att översättningen är mer belysande än den mer ordagranna översättningen ”öppen liggare”. Trots att jag valt att använda en svensk term för själva huvudboken kommer tekniken att kallas Open-Ledger-Technology (OLT) eftersom denna term konsekvent används i andra sammanhang för att beskriva tekniken som sådan.

Mining, Miners
Termen miners, eller grävare syftar till att skapa associationer till guldgrävare. *Miners* är särskilda noder som lånar ut datorkraft till att verifiera blocken genom proof-of-work (*mining*). För detta får de en belöning i form av nya Bitcoin som systemet självt genererar.

Proof-of-work
Proof-of-work är data som är *dyr och tidskrävande att producera* men *lätt för andra att verifiera.* När arbetet väl är utfört är det alltså lätt för alla noder i nätverket att verifiera blocket godkänts genom proof-of-work.

Protokoll
Ett protokoll kan förenklat sägas styra kommunikationen i nätverket. Det är ett kodat regelverk för hur deltagarna ska kommunicera med varandra för att få delta i nätverket. Bitcoin är ett protokoll.

Tokens
Tokens, till skillnad från coins, är enheter som representerar någonting utanför blockkedjan och har ett bredare användningsområde. Ett token kan exempelvis ha ett värde genom att utgöra en fordran på en underliggande tillgång som kan vara såväl fysisk som digital.

1.5 En överblick över den fortsatta dispositionen

Kapitel 1, som du troligen just läst, innehåller de klassiska delarna, syfte, metod, avgränsningar så att du som läsare ska kunna avgöra om du vill fortsätta från denna punkt.

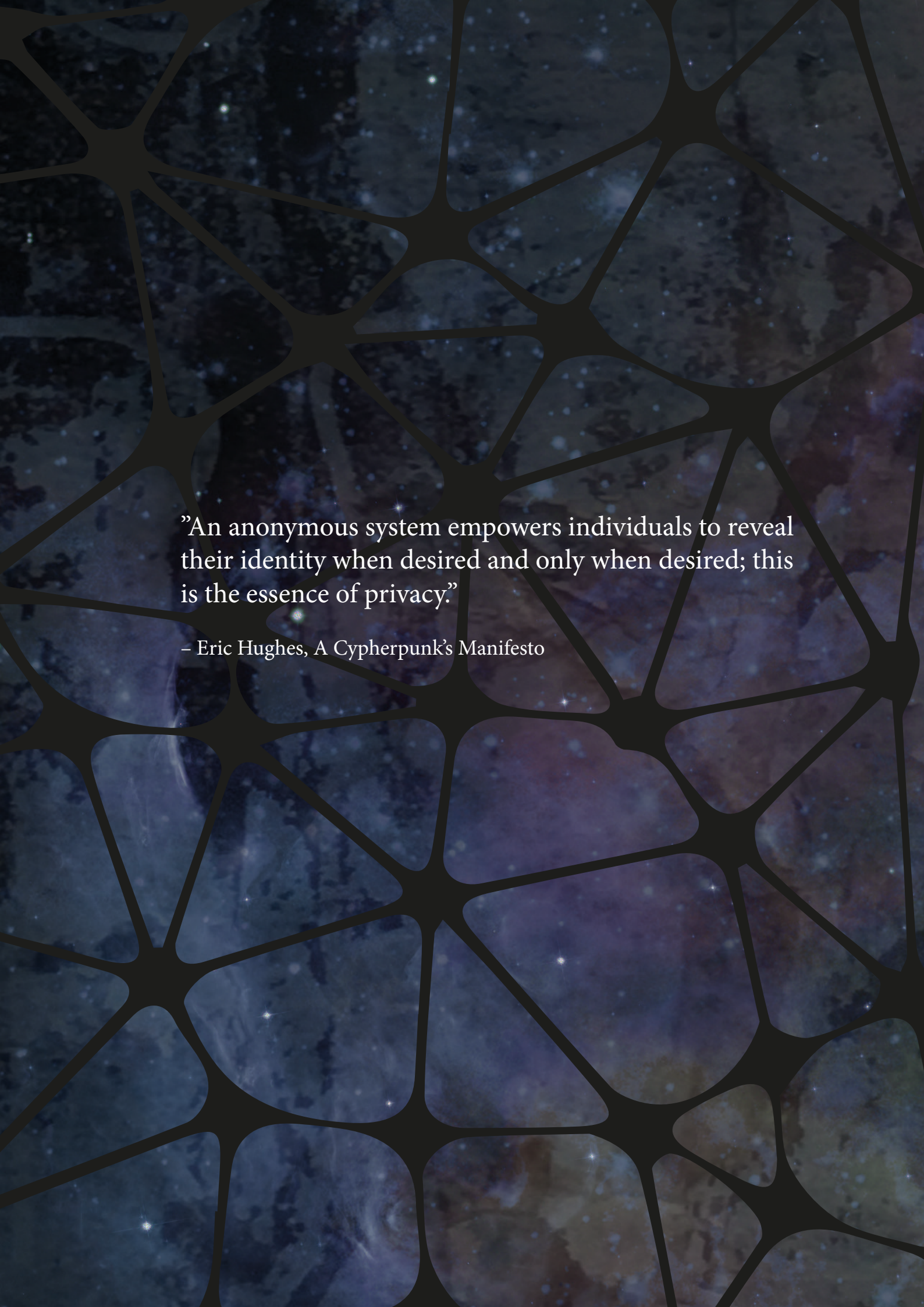
Kapitel 2 ger en ideologisk bakgrund till Bitcoins och blockkedjans framväxt för att ge dig som läsare en förståelse för den kulturella och politiska kontexten.

Kapitel 3 är mitt försök att ge dig en ”for dummies”-version av blockkedjans tekniska aspekter. Är du bekant med hur blockkedjor och kryptovalutor fungerar kan du hoppa över detta avsnitt.

Kapitel 4 diskuterar centrala förmögenhetsrättsliga aspekter av kryptovalutor som behöver utredas innan konkurssituationen kan analyseras. Här behandlas frågeställningar såsom: Vilken typ av egendom är kryptovaluta? Är kryptovaluta över huvud taget egendom? Är det valuta? Är det ett betalmedel? Vad är det annars? Hur skiljer sig Bitcoin-certifikat från Bitcoin ut ett förmögenhetsrättsligt perspektiv? Osv.

Kapitel 5 utforskar vad som händer i mötet mellan Bitcoin-systemet och konkursinstitutet när Bitcoin ingår i konkursboet. Först diskuteras borgenärsskyddet i dess klassiska betydelse, det vill säga konkursförvaltarens utgångspunkt för gränsdragning för prioritet mellan sakrätts- och fordringshavare. Därefter diskuteras Bitcoin konsekvenser för konkursinstitutet som sådant, främst hur egendomsslagets särart kan tänkas underminera konkursförvaltarens möjligheter att genomdriva ett effektivt konkursförfarande. I detta fall handlar det om ett övergripande skydd för det kollektiva borgenärsintresset som kursförvaltaren har att tillgodose.

Kapitel 6 bjuder på några avslutande reflektioner av övergripande karaktär.



”An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.”

– Eric Hughes, A Cypherpunk’s Manifesto

2 CYPHERPUNK OCH LIBERTARIANSKA IDEOLOGIER

För att förstå Bitcoin som fenomen behöver något sägas om dess bakgrund och de ideologier som präglat framväxten av kryptovaluta. Den ideologiska bakgrunden gör det också mer begripligt varför utvecklaren eller utvecklarna inte gör något som helst anspråk på den potentiellt revolutionerande tekniken och därtill har valt att förbli anonym(a).[10]

2.1 Det kryptografiska kriget för integritetsskyddet

Kryptovaluta var något som började diskuteras redan på 80-talet inom den så kallade cypherpunk-rörelsen. ”En cypherpunk är en aktivist som förespråkar en vidsträckt användning av stark kryptografi och andra integritetsförhöjande tekniker som en väg mot social och politisk förändring.”[11] Den sociala och politiska förändring som cypherpunkare eftersträvar handlar främst om att försvara och utöka rätten till privatliv i den digitala världen.

2.1.1 A Cypherpunk’s Manifesto[12]

En av rörelsens grundare, matematikern och programmeraren Eric Huges[13], skrev 1993 ett manifest som sammanfattar kärnan i cypherpunk-rörelsens ideologi. Manifestet är belysande för den som vill förstå de motsättningar som kan uppstå när nya kryptografiska lösningar sprungna ur cypherpunk-ideologin introduceras i samhället.

Inledningsvis vill Hughes betona skillnaden mellan privat och hemligt. Han menar att något privat är något som man inte vill att hela världen ska få reda på medan något hemligt är något man inte vill att någon ska få reda på. Privatliv, eller integritet, ska förstås som möjligheten att välja sin publik. Denna möjlighet är enligt Hughes helt nödvändig om vi vill ha ett öppet samhälle även i den elektroniska eran. Vem vågar yttra sig om alla alltid kan lyssna?

---

[10] Bitcoin och blockkedjans skapare går under pseudonymen Satoshi Nakamoto. Även om det förekommit många rykten och spekulationer kring Nakamotos verkliga identitet(er) (och några personer försökt att själva ta på sig äran) har inget hittills kunnat bevisas och den eller de som står bakom Satoshi Nakamoto har förblivit anonym(a).

[11] Wikipedia. (2 december 2017). *Cypherpunk*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Cypherpunk den 14 12 2017. Författarens egen översättning, originalspråk: ”A cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.”

[12] Huges, E. (9 mars 1993). *A Cypherpunk's Manifesto*. Hämtat från activism.net https://www.activism.net/cypherpunk/manifesto.html den 12 december 2017. Avsnitt 2.1.1. bygger på en fri översättning och återgivning av de delar ur manifestet som jag funnit särskilt relevanta för mitt arbete.

[13] Wikipedia. (23 oktober 2017). *Eric Hughes (cypherpunk)*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Eric_Hughes_(cypherpunk) den 15 december 2017.

Han poängterar vidare att syftet inte är att begränsa yttrandefriheten. Tvärt om menar Hughes att de nya, gränsöverskridande gruppsamtal och informationsutbyten som elektronisk kommunikation möjliggör, behöver ett effektivt sätt att skydda integriteten. I det digitala rummet blir kryptografi därför nödvändig om vi vill kunna styra vem som vet vad.

Rätten att vara och förbli anonym är central. Att man väljer att vara anonym behöver inte innebära att man egentligen har något att dölja. Som exempel tar Hughes situationen då någon köper en tidning och betalar med kontanter.[14] Det finns då ingen anledning för butiksbiträdet att be personen att identifiera sig. På internet röjs i regel motsvarande identitet på grund av de underliggande mekanismerna för själva transaktionen. Köparen kan inte välja om hen vill identifiera sig eftersom identifieringen blir en oundviklig del i att genomföra en transaktion. Den som vill hålla sina inköp privata utesluts från marknaden. Hughes menar därför att privatliv i ett öppet digitalt samhälle kräver *anonyma transaktionssystem*. Om utgångspunkten är anonymitet krävs också kryptografiska signaturer för att kunna identifiera sig som behörig utan att röja sin identitet.[15]

Enligt Hughes kan vi inte förvänta oss att staten, företag eller andra organisationer frivilligt kommer att respektera vår integritet eftersom det ligger i deras intresse att hålla sig informerade och prata om oss. Det blir därför upp till oss privatpersoner att försvara vår integritet om vi vill ha någon. Enligt manifestet är detta cypherpunkarens uppgift; att försvara vår rätt till privatliv genom kryptografi.

Utifrån sin ideologi skriver cypherpunkare kod och skapar olika sorters mjukvara. I ideologin ligger också att sådan kod ska vara öppen, globalt tillgänglig och gratis för andra att bygga vidare på. Det mycket omfattande arbete som lagts och läggs ner inom ramen för cypherpunk-rörelsen är alltså ideologiskt till stor del ideellt. Frågor som uppstår längs vägen besvaras genom att fråga sig vilken lösning som bäst främjar det ideologiska syftet.

Det finns också en rebellisk ton i manifestet. Hughes förkunnar att en cypherpunkare inte bryr sig om ifall vi inte vill acceptera rörelsens metoder eftersom mjukvara inte kan förstöras och ett tillräckligt utspritt system inte kan stängas ned. En cypherpunkare motsätter sig också reglering av användandet av kryptografi eftersom, menar Hughes, konsten att kryptera är fundamentalt privat till sin natur. Eftersom kryptering har möjligheten att undandra information från det allmänna skapar det också ett privat territorium dit lagens långa arm inte når. Det handlar alltså på det hela taget om politisk aktivism av den civil-libertarianska skolan. Själva aktivismen består i att ge allmänheten verktyg för att skydda sina civila rättigheter, främst rätten till privatliv, gentemot staten och andra organisationer men också gentemot andra individer. Verktygen bygger på användandet av kryptografi.

[14] Att Hughes valt att exemplifiera med just kontanter är knappast tillfällig. Likheter mellan Bitcoin och kontanter kommer jag att återkomma till nedan i avsnitt 4.3.
[15] Hur detta fungerar kommer jag att redogöra för i avsnitt 3.3.2.

2.1.2 Diffies asymmetriska nycklar – ett kryptografiskt genombrott

I artikeln ”Crypto Rebels”,[16] som publicerades strax innan Hughes manifest, tas motsättningen med staten upp ur ett ytterligare perspektiv. Cypherpunk-rörelsen ville slå hål på det monopol staten, i detta fall genom NASA, tidigare haft på kryptografiska verktyg.[17] Detta monopol skakades 1975 i grunden av en ung datorguru vid namn Whitfield Diffie.

Den traditionella metoden för att säkra information genom kryptering går ut på att kryptera själva meddelandet genom användandet av en kryptografisk nyckel.[18]. Mottagaren behöver då ha tillgång till nyckeln för att kunna omvandla meddelandet till dess ursprungliga och begripliga form. Problemet med metoden är att åstadkomma en säker förflyttning av själva nyckeln mellan avsändare och mottagare. Om nyckeln skickas via en osäker kanal finns risken att någon får tag på nyckeln och sedan använder den för att avkryptera all följande kommunikation mellan parterna. Detta problem brukade typiskt sett lösas genom att alla nycklar samlades på en ”säker plats” dit endast *betrodda administratörer* har åtkomst.

För Diffie var lösningens svaghet tydlig: Användarens integritet berodde på i vilken grad administratörerna var villiga att skydda den. Diffie ville istället använda sig av ett *decentraliserat system* där varje användare hade nyckeln till sin egen data. Frågan var hur detta skulle fungera.

I ett samarbete med Martin Hellman[19] och Ralph C. Merkle[20] hittade Diffie 1975 en lösning på problemet. Lösningen heter *publik-nyckel-kryptografi* och används inom blockkedjetekniken och Bitcoin.[21] Publik-nyckel-kryptografi går ut på att varje användare i systemet har två nycklar, en publik och en privat. Den *publika* kan visas utåt utan att riskera säkerheten medan den *privata* ska hållas endast av användaren själv. Nycklarna utgör ett asymmetriskt par som matematiskt sett fungerar så att ett meddelande som krypteras med den ena nyckeln kan avkrypteras med den andra. Avsändaren använder *mottagarens publika nyckel* för att kryptera innehållet och mottagaren använder *sin privata* nyckel för att avkryptera. Verktyget för att avkryptera, det vill säga den privata nyckeln, behöver aldrig överföras.[22]

---

[16] Levy, S. (1 februari 1993). *Crypto Rebels*. Hämtat från Wired: https://www.wired.com/1993/02/crypto-rebels/ den 28 oktober 2017.

[17] Innan cypherpunk-rörelsen var avancerad kryptografi inte tillgänglig utanför den statliga verksamheten eller i vart fall inte utom statens kontroll.

[18] I dess enklaste form kan en nyckel vara exempelvis att varje bokstav byts ut mot bokstaven efter i alfabetet.

[19] Martin Hellman är en amerikansk kryptolog, främst känd för sitt arbete med publik-nyckel-kryptografi I samarbete med Whitfield Diffie och Ralph Merkle.

[20] Ralph Merkle är en amerikansk datavetare som utöver att ha varit en av männen bakom publik-nyckel-kryptografi även är känd för sitt arbete med kryptografiska hash funktioner och kryonik.

[21] Författarens egen översättning av termen ”public key cryptography”. Jag kommer att återkomma till de tekniska finesserna med användandet av publik-nyckel-kryptografi i blockkedjan senare i avsnitt 3.3.2 och 3.4.1.

[22] Samma princip blir omvänt användbar för autentisering. Endast den person som har den privata nyckeln kan använda denna för att kryptera. Motparten kan använda personens publika nyckel för att läsa av informationen och kan då vara säker på att den skickats just av den avsändare som har den privata nyckeln. Meddelandet och den säkra signaturen blir på så vis det samma.

Genombrottet var monumentalt och till skillnad från många andra kryptografiska framsteg togs detta inte av någon stat utan av en enskild integritetsivrare. Lösningen banade väg för en ny rörelse inom kryptografikretsar.

2.1.3 Pretty Good Privacy – för alla

"Vad skulle hända om alla ansåg att laglydiga medborgare borde använda vykort för all sin post? Det skulle då verka misstänkt om någon modig själ försökte hävda sin integritet genom att använda ett kuvert."[23] Så skriver Zimmerman i sin text *Why I wrote PGP*. Som tur är, menar Zimmerman, lever vi inte i ett samhälle där myndigheter skulle anse att ett kuvert var så misstänkt att det kanske måste öppnas och undersökas. Anledningen är att användandet av kuvert är så allmänt utbrett.

På samma sätt menade man inom kryptografikretsar att kryptografi var något som alla borde använda för att se till att de som använder kryptografi inte framstår som misstänkta. Mjukvaran PGP (Pretty Good Privacy) lanserades 1991 och bygger på publik-nyckel kryptografi. Zimmerman valde att släppa mjukvaran fri i förhoppningen att den skulle hinna sprida sig tillräckligt för att överleva även om staten skulle komma att förbjuda gemene man från att använda kryptografi. Även om detta aldrig skedde blåste det rejält kring PGP när tekniken först lanserades. Öppen PGP, som bygger på Zimmermans ursprungliga mjukvara, är idag den mest använda krypteringsstandarden för e-post.[24] I texten *Why I wrote PGP* är den politiska tonen tydlig och Zimmerman vidhåller att ”integritet är lika amerikanskt som konstitutionen”.[25]

2.1.4 Bitcoin – Nakamoto löser problemet med dubbelutgifter

Nästa viktiga steg för cypherpunk-rörelsen var att garantera användares integritet, inte bara vid digital överföring av information, utan också vid digitala värdeöverföringar. Visionen om ett sådant anonymt betalningssystem återfinns redan i Eric Hughes manifest från 1993.[26] Först femton år senare, 31 oktober 2008, lanseras Bitcoin, den första blockkedjan.

På samma sätt som publik-nyckel-kryptografi var ämnat att eliminera behovet av *betrodda administratörer*, är Bitcoin utformat för att eliminera behovet av *betrodda intermediärer*. Anledningen till att tekniken som använts för säker *peer-to-peer*-överföring av information inte utan vidare löser motsvarande problem vid värdeöverföringar beror på dilemmat med *dubbelutgifter*.[27] Dubbelutgifter är ett problem främst för digitala betalningsmedel. Problemet uppstår på grund av att digital information, till skillnad från kontanter, normalt sätt kan reproduceras relativt enkelt. Med digitala betalningsmedel finns därför vanligen en högre risk

---

[23] Författarens egen översättning, originalspråk: “What if everyone believed that law-abiding citizens should use postcards for their mail? If some brave soul tried to assert his privacy by using an envelope for his mail, it would draw suspicion.” Källa: Zimmerman, P. (1 juni 1991). *Why I Wrote PGP*. Hämtat från philzimmermann.com: https://philzimmermann.com/EN/essays/index.html den 2 december 2017.

[24] OpenPGP. (u.d.). *OpenPGP, Email encryption. For all operating systems. Standing the test of time.* Hämtat från openpgp.org: https://www.openpgp.org/ den 27 november 2017.

[25] Författarens egen översättning., originalspråk: ”Privacy is as apple-pie as the Constitution”

[26] Se ovan under avsnitt 2.1.1.

[27] Författarens egen översättning av det engelska begreppet *double spending*.

för att A gör en kopia av sina digitala *tokens*[28] för att skicka till B (exempelvis en säljare eller en annan part) samtidigt som A själv behåller originalet. En av uppgifterna för betrodda intermediärer, såsom banker, är att se till att sådana dubbelutgifter inte förekommer.[29]

Bitcoin är Nakamotos förslag på hur problemet med dubbelutgifter kan lösas i ett *peer-to-peer*-nätverk. Bitcoin lanserades tillsammans med Satoshi Nakamotos[30] berömda white paper *Bitcoin: A Peer-to-Peer Electronic cash system*.[31] Nakamoto beskriver själv sin lösning som en renodlad *peer-to-peer*-version av elektroniska kontanter som möjliggör direktbetalningar över nätet utan inblandning av finansiella institut (betrodda intermediärer).[32] I Bitcoin verifieras transaktioner på ett säkert sätt som förhindrar dubbelutgifter utan att någon betrodd intermediär behövs för att göra kontrollen. Hur detta går till återkommer jag till i avsnitt 3.3. Jag kommer senare i avsnitt 4.3 argumentera för varför detta, bland andra egenskaper, ger Bitcoin en mycket hög materiell integritet, trots att Bitcoin saknar fysisk form.

2.2 Bitcoin och libertarianismen

Ideologiskt sett har Bitcoin och cypherpunk-rörelsen sina rötter i och en stark koppling till libertarianismen.[33] Som jag ser det har Bitcoin, genom sin struktur, lyckats omsätta många av libertarianismens ideal i praktiken.

Libertarianismen utgår ifrån *individen* och dess rätt- och skyldigheter. Individer har rätt till säkerhet vad gäller deras liv, frihet och egendom. Denna rätt anses inte komma från staten eller samhället utan är en del av människans natur. Individen är autonom, hen gör sina val och är ansvarig därefter.[34] I Bitcoin-systemet har varje användare full kontroll över sina egna tillgångar. Individens omedelbara kontroll i kombination med möjligheterna till anonymitet medger stor handlingsfrihet. Var och en är fri att sköta sina affärer efter eget gottfinnande. Staten, privata företag eller andra organisationer har svårt att övervaka användarnas mellanhavanden eller rent praktiskt lägga sig i. En effekt av att individen har full kontroll är att det egna ansvaret ökar. Exempelvis har den enskilda individen bara sig själv att skylla

---

[28] Översatt betyder token ungefär polett. Jag har ändå valt att behålla det engelska uttrycket. En närmare redogörelse för innebörden ges i avsnitt 3.2.

[29] Investopedia. (u.d.). *Double-Spending*. Hämtat från Investopedia: https://www.investopedia.com/terms/d/doublespending.asp den 16 december 2017.

[30] Se not 10 ovan.

[31] Nakamoto, S. (31 oktober 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Hämtat från bitcoin.org: https://bitcoin.org/bitcoin.pdf den 12 december 2017.

[32] Ibid s 1.

[33] Se bl.a. Redman, J. (16 januari 2017). *Do Satoshi's Libertarian Statements from the Past Matter Anymore?* Hämtat från bitcoin.com: https://news.bitcoin.com/satoshis-libertarian-statements-past-matter-anymore/ den 12 december 2017;
Libertarian Party. (u.d.). *Bitcoin*. Hämtat från Libertarian Party: https://www.lp.org/donate/bitcoin/ den 17 december 2017;
Trustnodes. (21 september 2017). *Bitcoin Millionaires Announce Plans to Form a Libertarian Country*. Hämtat från trustnodes.com: http://www.trustnodes.com/2017/09/21/bitcoin-millionaires-announce-plans-form-libertarian-country den 12 december 2017.

[34] Boaz, D. (1 januari 1999). *Key Concepts of Libertarianism*. Hämtat från Cato Institute: https://www.cato.org/publications/commentary/key-concepts-libertarianism den 16 december 2017.

om någon transaktion går till fel mottagare. Förvisso kan individen ha rättsordningens stöd för ett anspråk, men att i praktiken göra något åt saken kan bli besvärligt. Detta beror dels på möjligheterna till anonymitet, dels för att det inte finns någon betrodd intermediär att ta hjälp av. Systemet självt bygger minst sagt på frihet under ansvar.

Libertarianismen tror på en spontan ordning, det vill säga att den bästa ordningen är den som uppstår naturligt i ett samhälle. Civilsamhället är ett exempel på en sådan ordning. De enskilda relationerna inom civilsamhället har syften, medan civilsamhället, i avsaknad av att utgöra ett eget subjekt, inte har någon egen agenda. Lagar får aldrig vara maktfullkomliga utan ska alltid skydda individens möjlighet att söka lyckan på sitt eget sätt och inte vara utformade på ett sätt som tjänar något visst övergripande mål eller syfte.[35] Bitcoin-systemet bygger på en ordning som liknar exemplet med det civila samhället. Användarna har sina individuella syften, medan blockkedjan mycket förenklat är en historik över individernas mellanhavanden. Bitcoin-protokollet i sig har ingen agenda (utöver den som framförs här, nämligen att möjliggöra transaktioner inom ett system som saknar egen agenda).

En viktig grundsyn är att alla ska vara fria att söka förverkliga sina egna livsmål i sådan utsträckning att det inte inkräktar på någon annan individs rätt att göra det samma. En regering kan fylla ett syfte genom att skydda dessa rättigheter. Men libertarianismen förhåller sig alltid skeptisk till centraliserad maktutövning.[36] Bitcoins decentraliserade *peer-to-peer*-struktur svarar väl mot libertarianismens syn på lika möjligheter. Strukturen omöjliggör också, i sann libertariansk anda, all form av centraliserad maktutövning.

Libertarianer tror på en fri marknad. Rätten till egendom inbegriper möjligheten att utbyta egendomen baserat på ömsesidig partsvilja. Libertarianer tror att människorna blir både friare och mer framgångsrika om den politiska makten har ett så litet inflytande på ekonomin som möjligt. Det finns en tro på en naturlig intresseharmoni mellan fredliga, produktiva individer i ett rättvist samhälle. Det är när den politiska makten kommer in och vill premiera vissa grupper eller beteenden som individer tvingas gruppera sig i konflikt med andra grupper.[37] Genom att Bitcoin inte har något bakomliggande rättssubjekt ges den politiska makten ingen möjlighet att utöva påtryckningar mot systemet självt. Olika rättsordningar kan förstås försöka reglera användningen av Bitcoin, men sådan reglering kan endast försöka påverka fysiska och juridiska personer att använda Bitcoin på det sätt eller i den utsträckning som den egna rättsordningen medger. Att Bitcoin inte är ett juridiskt subjekt utgör dock ett betydande skydd mot politiskt inflytande.

---

[35] Boaz, D. (1 januari 1999). *Key Concepts of Libertarianism*. Hämtat från Cato Institute: https://www.cato.org/publications/commentary/key-concepts-libertarianism den 16 december 2017. Texten kommer ursprungligen från första kapitlet i författarens bok *Libertarianism: A Primer (*New York: The Free Press, 1998)

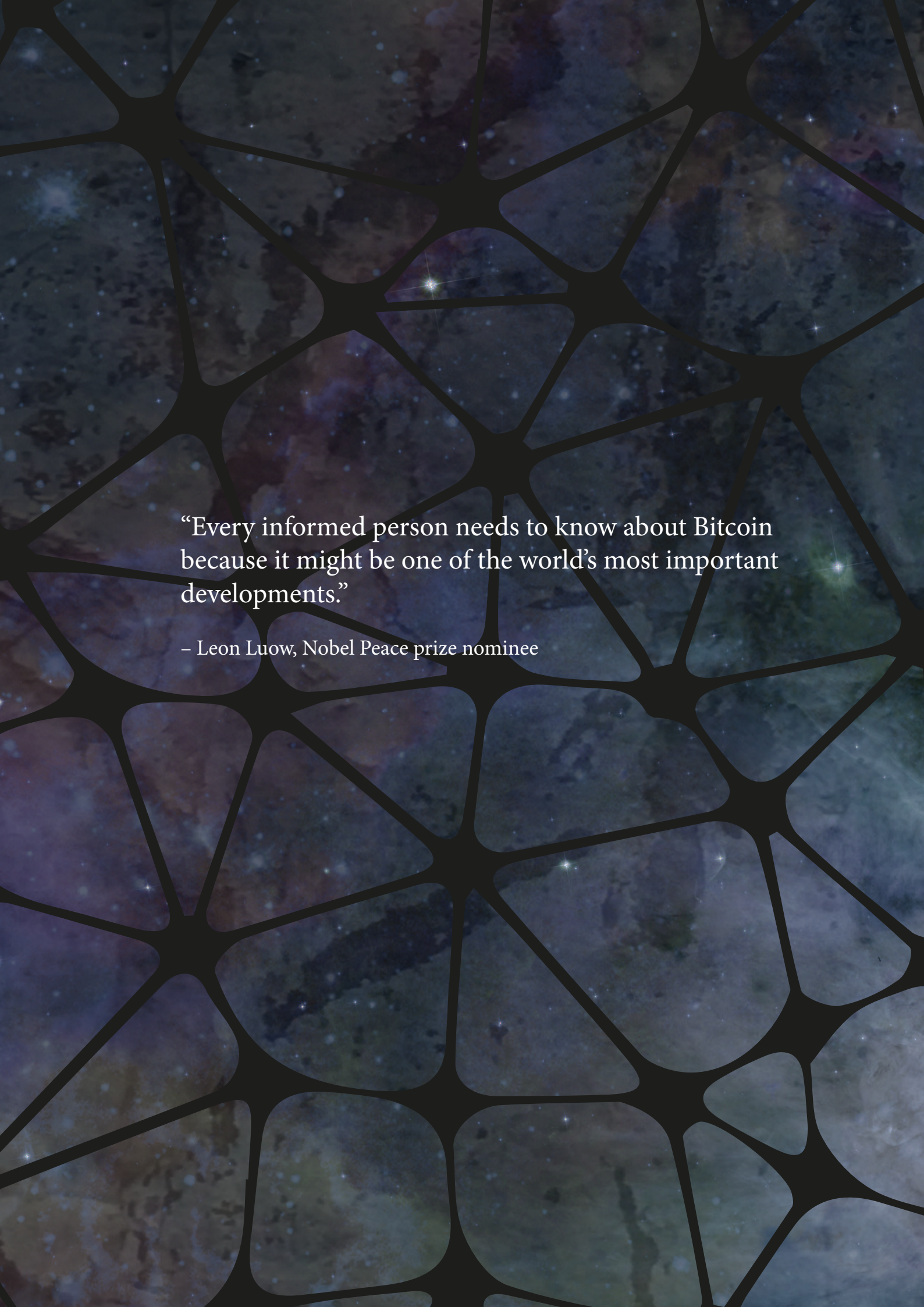
[36] Ibid.

[37] Ibid.

2.2.1 Bitcoin, libertarianismen och konkursinstitutet

Sammanfattningsvis kan sägas att såväl libertarianismen som Bitcoin utgår ifrån en autonom individ vars rättigheter och frihet ovillkorligt ska respekteras. Det är också individen som förväntas ta eget ansvar för sitt handlande. Både Libertarianismen och Bitcoin motsätter sig central maktutövning och ser politiskt inflytande på ekonomin som något negativt, eftersom idealet är en spontan ordning.

Som jag ser det är konkursinstitutet på sätt och vis en ideologiskt utmanande företeelse för libertarianer. Å ena sidan handlar insolvensrätten just om att se till att en individs rätt inte otillbörligt inkräktar på någon annans, vilket risken är stor för när tillgångarna inte längre räcker för att tillfredsställa alla de inblandade parternas intressen. Å andra sidan är tillvägagångssättet baserat på central, statlig maktutövning och ordningen allt annat än spontan.



"Every informed person needs to know about Bitcoin because it might be one of the world's most important developments."

– Leon Luow, Nobel Peace prize nominee

3 BLOCKKEDJAN BITCOIN "FOR DUMMIES" (OCH DE FLESTA JURISTER)

Det här avsnittet är en genomgång av blockkedjor som riktar sig till en läsare som inte är insatt i tekniken sedan tidigare. Det är en sammanfattning av blockkedjans huvuddrag följt av en relativt ingående teknisk beskrivning. Syftet är att ge läsaren den förkunskap som behövs för att själv kunna reflektera över juridiska aspekter av blockkedjan och Bitcoin. Kapitlet är också tänkt att skapa en kunskapsplattform som är behövlig för att fullt ut kunna tillgodogöra sig efterföljande kapitel.

Att jag valt att gå relativt djupt i de tekniska beskrivningarna, trots att detta är ett juridiskt examensarbete, beror på att jag själv tycker att det är svårt att känna sig bekväm med att tänka kring och använda begrepp utan att fullt ut förstå dem. Kryptovalutor är än så länge ett oreglerat område i Sverige, vilket medför att en juridisk analys kommer att innehålla försök till lämpliga analogier för att hitta såväl frågeställningar som lösningar. Att spekulera i hur något lämpligen bör hanteras utan att full ut förstå vad det är kan knappast skapa klarhet.

En annan sak är att det kan vara juridiskt helt irrelevant hur något rent tekniskt fungerar. Exempelvis kan vi tolka vissa regler för utformning av webbplatser utan att veta särskilt mycket om vad internet är på ett tekniskt plan. Min personliga upplevelse är dock att man bör skaffa sig en god kunskap om ett område för att alls kunna ta ställning till vilken fakta som kan ha juridisk relevans och vilken som kan läggas åt sidan i den juridiska analysen.

Som jag tidigare nämnt i mitt metodavsnitt bygger denna sammanfattning på att jag själv läst, hört och tittat på en mängd tekniska beskrivningar av varierande kvalitet. Detta har jag gjort för att själv skapa mig en förståelse och utifrån den kunna göra en sammanfattning som är både tekniskt korrekt samtidigt som informationen är sållad, prioriterad och strukturerad på ett sätt som jag funnit lämpligt i detta sammanhang. Jag kommer därför inte att göra några källhänvisningar till varje faktum som läggs fram eftersom i princip all fakta tenderar att återkomma i samtliga källor jag använt mig av.[38]

[38] Som jag nämnt i avsnitt 1.2.1.2 bygger min tekniska förståelse av Bitcoin snarare på att jag tagit till mig samma information från en mängd olika håll för att kunna göra kunskapen till min egen och därigenom sammanställa den på det sätt jag själv finner mest lämpligt. I mängden av källor jag använt mig av vill jag dock särskilt framhålla följande, då dessa varit särskilt centrala för min förståelse: Webbplatsen Bitcoin Wiki (som drivs av Bitcoin-anhängare på liknande sätt som Wikipedia); Youtube-kanalerna CuriousInventor och Ivan on Tech samt Satoshi Nakamotos berömda White Paper *Bitcoin: A Peer-to-Peer Electronic Cash System.*

3.1 Fem viktiga grunder för att förstå Bitcoin

3.1.1.1 Det går inte att ta på

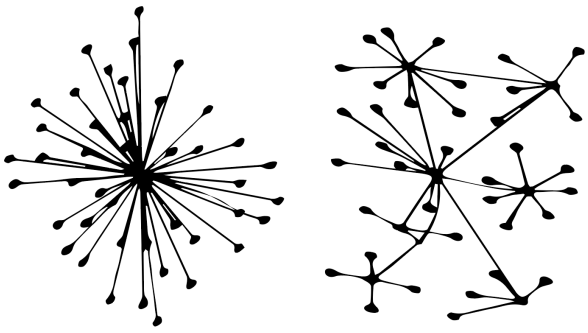
Bitcoin är digitalt, det vill säga en icke-fysisk valuta[39] som skapas, förvaras och överförs helt digitalt. Bitcoin skapas av ett protokoll som strikt följer en algoritm och körs över en stor mängd datorer som fungerar som noder i Bitcoin-nätverket. Det finns inte heller någon underliggande fysisk tillgång, såsom guld, som backar upp Bitcoin och säkrar dess värde.

3.1.1.2 Det finns ingen topp

Bitcoin har ingen suverän auktoritet. Inte ens skaparen eller skaparna[40] gör något anspråk på att äga eller styra Bitcoin. Ingen individ, organisation eller statsmakt har någon kontroll över Bitcoin. Bitcoin är också gränslös såtillvida att transaktioner kan göras helt oberoende av geografiska aspekter så länge det finns internetuppkoppling. I den mån Bitcoin krockar med regler inom en viss jurisdiktion är detta något som Bitcoin-systemet självt är helt okänsligt för. Det är alltså upp till lagstiftaren och rättstillämparna att hantera Bitcoin utifrån Bitcoins egna premisser. Bitcoin går inte att förhandla med eller förändra genom reglering. Det som kan regleras är lagligheten i att använda Bitcoin på olika sätt, men regleringen kan bara träffa användarna eftersom Bitcoin inte är eller har något ansvarigt rättssubjekt utan är en databas som styrs autonomt av sitt protokoll.

3.1.1.3 Det finns ingen mitt

Bitcoin är helt decentraliserat. Det finns ingen central utgivare av Bitcoin. Nya Bitcoins uppkommer genom så kallad ”mining”.[41] Det finns heller ingen annan central knutpunkt eller central kontroll. Datorer som ingår i Bitcoin-nätverket utgör så kallade noder. Dessa noder är varandras likar *(peers)* i ett så kallat *peer-to-peer*-nätverk och har alltså inte någon hierarki sinsemellan.

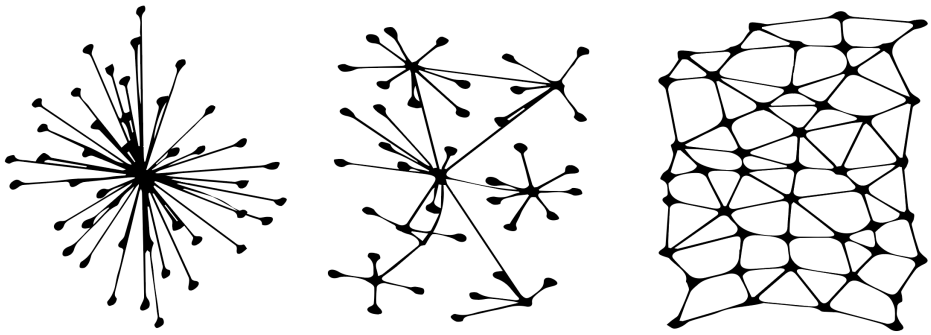


Centraliserat *Decentraliserat*

[39] Bitcoin utgör inte en valuta i egentlig mening. Jag återkommer till detta i avsnitt 4.2 Vad jag menar med ”icke-fysisk” förklaras närmare i avsnitt 4.1.1.1.
[40] Som än idag lyckats förbli anonym(a) och går under pseudonymen Satoshi Nakamoto.
[41] Något om mining finns att läsa i avsnitt 3.3.4.3.

3.1.1.4 Alla vet allt och ingen vet något.

Bitcoin är distribuerat med så kallad *Open Ledger Technology* (OLT) vilket gör att alla noder i nätverket hela tiden hålls uppdaterade med all information. Ett enbart decentraliserat system kan ha innebörden att alla vet något men ingen vet allt. I ett fullt ut *decentraliserat och distribuerat* system *vet alla allt*. Detta är också en av de stora styrkorna. Ett decentraliserat och distribuerat system som bygger på OLT är extremt motståndskraftigt mot attacker och försök till manipulation av data. Systemet verifierar hela tiden sin data genom att jämföra och synkronisera kopiorna som finns i full version hos varje nod. Om data skiljer sig hos en nod kommer systemet att tvinga noden att rätta in sig i ledet. En attack i syfte att manipulera data behöver därför rikta sig mot en majoritet av noderna i nätverket samtidigt. Att lyckas med en sådan attack är i stort sett praktiskt omöjligt, vilket gör säkerheten i systemet svårslagbar.



Centraliserat *Decentraliserat* *Distribuerat*

3.1.1.5 Det behövs ingen tillit (?)

Bitcoin-protokollet är uppbyggt av en mängd matematiska och kryptografiska finesser som kan autentisera användare och kontrollera täckningen för varje transaktion för att på olika sätt förhindra bedrägerier. Användandet av betrodda intermediärer såsom banker utgår från ett behov av partstillit i transaktionen. Bitcoin-systemet är istället programmerat så att partstillit inte behövs eftersom utrymmet för bedrägligt beteende inom systemet eliminerats. Att säga att ingen tillit behövs är dock missvisande. Parterna måste, om de ska kunna lita på varandra, ha tillit till systemet. *Parts-tilliten* kan sägas ha ersatts av *system-tillit*.

3.2 Skillnaden på blockkedja, protokoll, coins och tokens[42]

Blockkedjan är själva tekniken. De allra flesta kryptovalutor, med Bitcoin som främsta exempel, bygger på blockkedjeteknik. Med blockkedja menas förenklat att så kallade *block*

[42] Informationen baserar sig främst på en video publicerad av Youtube-kontot Ivan on Tech. Ivan on Tech. (22 september 2017). *Difference between COIN, TOKEN and PROTOCOL - Programmer explains*. Hämtat från YouTube: https://www.youtube.com/watch?v=pcilyT3fh-0 den 30 januari 2018.

med information länkats kryptografiskt på ett sådant sätt att förändringar i ett tidigare block kommer att invalidera informationen i de senare. Själva grundidén bygger på att information länkas kronologiskt så att det inte ska gå att manipulera historiken. Med blockkedjans grundidé som fundament går tekniken att vidareutveckla genom att addera olika *protokoll*.

Ett protokoll kan förenklat sägas styra kommunikationen i nätverket. Det är ett kodat regelverk för hur deltagarna ska kommunicera med varandra för att få delta i nätverket. Bitcoin är *ett* protokoll. Andra exempel på kryptovalutaprotokoll som bygger på blockkedjeteknik är Etherium, Ripple, Litecoin m.fl. Egenskaper såsom Bitcoins lösning för att motverka dubbelutgifter ligger i *protokollets* utformning. Protokollet är alltså ett ytterligare lager ovanpå blockkedjan som styr användning av och egenskaper hos just den blockkedjan.[43] I huvudsak går Bitcoin-protokollet ut på att distribuera blockkedjan till hela nätverket så att konsensus avseende transaktionshistoriken hela tiden föreligger.

Coins och *tokens* kan förstås som konceptuella enheter i blockkedjan. 1 Bitcoin (BTC) är en sådan enhet i blockkedjan Bitcoin. Digitala coins eller tokens är inget som kan förvaras på en hårddisk eller liknande. Att inneha dessa enheter är i själva verket att inneha en *nyckel* som ger möjlighet att gå in och logga transaktioner på blockkedjan som innebär att ens enheter omdisponeras till andra adresser med egna unika nycklar. Enheterna kan sägas vara en specifik mängd digitala resurser som användaren kontrollerar på sådant sätt att denne kan överlåta kontrollen till någon annan.

Coins kallas de enheter som inte representerar något annat värde än det värde enheten själv har på marknaden. En Bitcoin (BTC) är, som namnet antyder, ett exempel på en typ av coin eller mynt. Tanken med coins är att de ska gå att använda som pengar.

Förenklat är *Tokens*, till skillnad från coins, enheter som representerar någonting utanför blockkedjan och har ett bredare användningsområde. Ett token kan exempelvis ha ett värde genom att utgöra en fordran på en underliggande tillgång som kan vara såväl fysisk som digital. Blockkedjor kan på så vis användas för att skapa säkra överlåtelsekedjor för löpande skuldebrev avseende en skuld på vad som helst.

Ett token kan också användas för att skapa transparens i en distributionskedja. Kontrollen över ett token som representerar en viss vara förflyttas i blockkedjan genom att varje aktör som handhar varan använder sin digitala signatur för att digitalt överföra aktuellt token i samband med att en fysisk överlämning sker genom de vanliga distributionskanalerna. På så vis kan slutkonsumenten förvissa sig om att varan fysiskt har gått den väg som blockkedjan anger och har det ursprung som återförsäljaren hävdar. Det går också att låta ett token representera en röst i ett val. Det är framförallt tokens som koncept som gör att blockkedjan kan få så många olika användningsområden.

[43] Protokoll är ett mer allmänt begrepp som används även utanför blockkedjan i andra system som behöver just regler för kommunikation i ett nätverk.

3.3 De centrala delarna i den tekniska uppbyggnaden

I detta avsnitt beskriver jag vad det innebär att inneha, överföra och ”gräva” Bitcoins ur ett rent tekniskt perspektiv. Som jag nämnt ovan är min uppfattning att en relativt djupgående teknisk förståelse kan vara nödvändig för att kunna tillgodogöra sig den följande analysen.

3.3.1 Huvudboken

I grund och botten är blockkedjan i Bitcoin en digital fil eller databas som håller reda på konton och saldon, härefter kallad *huvudboken.*[44] Huvudboken är distribuerad genom att kopior av huvudboken hela tiden finns, underhålls och uppdateras på samtliga datorer i nätverket. Jag kommer hädanefter att använda begreppet *noder* för de datorer som ingår i nätverket.

Genom att noderna gemensamt och genom konsensus för huvudboken ser till att uppdateringar hela tiden distribueras till hela nätverket, skyddas huvudboken på ett effektivt sätt mot attacker som syftar till att förändra huvudbokens innehåll. För att ändra innehållet i huvudboken räcker det inte att hacka en nod i nätverket eftersom detta medför att det inte längre råder konsensus mellan noderna kring huvudbokens korrekta innehåll. Nätverket kommer i ett sådant läge att se till att den avvikande huvudbokskopian uppdateras så att den stämmer överens med nätverkets gemensamma uppfattning om det korrekta innehållet. Det är därför extremt svårt att lyckas manipulera innehållet i huvudboken.

Bitcoin är på det hela taget väldigt säkert till följd av den starka kryptografi som används. Även om det hypotetiskt sett finns en möjlighet att Bitcoin skulle råka ut för en större attack i framtiden är teknik- och kryptografiexperter eniga om att en sådan attack är mycket osannolik i närtid.[45]

3.3.2 Transaktionen och autentisering genom digitala signaturer

För en vanlig Bitcoin-användare skiljer sig inte transaktionsupplevelsen nämnvärt från hur det går till vid en vanlig kontoöverföring på bank. Användaren anger att hen vill sända x mängd Bitcoin till en viss adress och får efter ett antal minuter bekräftat att så har skett. I Bitcoin-systemet finns inte banken, vilket medför att händelseförloppet mellan det att användaren ”beställer” en överföring och att överföringen fullbordas ser annorlunda ut.

Det som händer är att användaren sänder ut en signal till nätverket som föreslår att ”saldot” på dennes konto ska gå ner och ”saldot” på mottagarkontot ska gå upp. [46] Noderna i

---

[44] På engelska används ordet ”ledger” för filen och begreppet ”Open Ledger Technology” (OLT) för den teknik som används för att distribution. Jag kommer hädanefter att använda mig av översättningen ”huvudbok” för filen och OLT när jag syftar på tekniken för att distribuera en sådan huvudbok i ett nätverk.
[45] Reiff, N. (12 december 2017). *Can Bitcoin Be Hacked?* Hämtat från Investopedia: https://www.investopedia.com/articles/investing/032615/can-bitcoin-be-hacked.asp den 26 december 2017.
[46] Att kalla det för ”konto” och ”saldo” är något missvisande, vilket kommer att framgå senare i detta kapitel. Av pedagogiska skäl har jag dock valt att använda dess begrepp för att bättre kunna förklara vissa företeelser för någon som är främmande för tekniken.

nätverket lägger till transaktionen till sina huvudböcker och för vidare informationen till andra noder. (Jag återkommer strax till hur detta går till i detalj.) Till skillnad från bankfallet känner användaren inte bara till sin egen transaktion. Alla i nätverket hålls uppdaterade på alla transaktioner som görs.[47]

De flestas upplevelse av vanliga banktransaktioner är att de kan lita på att banken ser till att alla transaktioner går rätt till (eller att de i vart fall kommer att ha rättsordningens stöd om något går fel). I Bitcoin-systemet har användaren istället att göra med en stor mängd anonyma främlingar som hen egentligen inte har någon anledning att lita på och ofta inte har någon reell möjlighet att ställa till svars i en domstol. Bitcoin är uppbyggt så att tilliten du normalt känner till banken eller någon annan betrodd intermediär istället ersätts av matematiska funktioner som skyddar varje del av nätverkets interaktioner och omöjliggör avvikelser från protokollet.

3.3.2.1 Publik-nyckel-kryptografi och digitala signaturer

Som nämnts ovan använder sig Bitcoin bland annat av publik-nyckel-kryptografi. Bitcoins motsvarighet till att vara kontohavare innebär i praktiken att man har åtkomst till ett nyckelpar bestående av en *privat nyckel* med en tillhörande *publik nyckel*.[48] Den *publika nyckeln*, som ser ut som ett långt komplicerat lösenord, är öppen för systemet och fungerar som mottagaradress, alltså den adress en användare ger till andra som ska skicka Bitcoin till användaren. Den *privata nyckeln* är användarens ”egentliga” lösenord och ska hållas just privat. Den som har den privata nyckeln kallas fortsättningsvis av pedagogiska skäl för *kontohavaren*.

Exempel:
Ahmed vill skicka 1 BTC till Betty. Ett meddelande går ut till nätverket som föreslår att saldot på det konto Ahmed förfogar över ska gå ner och att saldot på ett konto Betty förfogar över ska gå upp, härefter kallat *transaktionsmeddelande*.

Frågan blir då hur nätverket kan veta att det är Ahmed som skickar ut transaktionsmeddelandet. Att det är just Ahmed får nätverket inte veta, men det behöver verifieras att det är *kontohavaren* som skickar ut transaktionsmeddelandet, det vill säga att Ahmed har den privata nyckeln. Eftersom den privata nyckeln av säkerhetsskäl aldrig ska avslöjas för systemet kan Ahmed inte använda nyckeln som sådan för att bevisa sin behörighet.

Bitcoin kräver istället att Ahmed använder en *digital signatur*.[49] Signaturen konstrueras kryptografiskt genom att använda den *privata nyckeln* och *transaktionsmeddelandet* som

[47] Möjligheten till anonymitet medför dock att transaktionerna sällan kan kopplas till de fysiska eller juridiska personer som agerar avsändare och mottagare. Jag återkommer till anonymiteten nedan i avsnitt 3.4.2.
[48] Detta har omnämnts ovan som publik-nyckel-kryptografi i avsnitt 2.1.2.
[49] Liksom en vanlig handskriven signatur används den digitala signaturen för att autentisera. Skillnaden är att den digitala signaturen som används i Bitcoin istället är en matematisk algoritm som utesluter möjligheten till kopior och förfalskningar av signaturen i den digitala sfären.

komponenter. Genom avancerad kryptografi kan noderna i nätverket, med hjälp av Ahmeds *publika nyckel*, kontrollera att den tillhörande privata nyckeln ingått som komponent i skapandet av den aktuella signaturen. Signaturen *bevisar* på så vis att Ahmed *har den privata nyckeln utan att avslöja den för systemet.*[50] Eftersom även transaktionsmeddelandet alltid ingår som en komponent för att skapa en giltig signatur kommer signaturerna automatiskt att bli unika för varje transaktion. Detta garanterar att signaturen inte kan återanvändas för att göra ytterligare transaktioner från kontot eftersom en använd signatur därigenom är förbrukad.[51]

3.3.3 Hur noderna håller ordning på huvudboken genom transaktionskedjor

Till skillnad från vad man lätt kanske föreställer sig innehåller huvudboken inte någon lista över konton med ett saldo bredvid som berättar hur mycket Bitcoin som för tillfället finns på varje konto. Frågan blir då hur systemet kan kontrollera att en kontohavare har täckning på sitt konto för att skicka den summa som hen angett i sitt transaktionsmeddelande.

3.3.3.1 Inputs

Istället för ett saldo redovisas tillgodohavanden genom referering till länkar till tidigare transaktioner som kontot varit inblandat i. För att kunna skicka 1 BTC måste det gå att referera länkar till transaktioner som tillsammans fört över minst 1 BTC med kontots publika nyckel som mottagaradress, så kallade *inputs*. De noder som ska kontrollera täckningen för den transaktion som kontohavaren föreslår kommer att kontrollera länkningarna och se så att kontohavaren verkligen var mottagare och att summan totalt uppgår till minst 1 BTC.

Genom länkarna till dessa refererade inputs överförs kontrollen över en Bitcoin i en slags kedja där giltigheten av varje transaktion är beroende av giltigheten i varje tidigare transaktion. När man installerar en plånboksfil [52] för Bitcoin på sin dator är det första steget att programvaran importerar alla tidigare transaktioner och kontrollerar deras giltighet på samma sätt hela vägen tillbaka till den första transaktionen.[53] Varje transaktion kan bara användas som input en enda gång, därefter är den förbrukad.[54]

Sammanfattningsvis kontrolleras tre saker av noderna då ett transaktionsmeddelande skickas ut i nätverket, nämligen:

1. att inputs är gjorda till det den publika nyckel som kontohavaren vill skicka pengar ifrån;

---

[50] Det går också att skapa andra villkor såsom att flera givna signaturer krävs för att exempelvis möjliggöra en escrow-liknande transaktion.

[51] Signaturens beroende av transaktionsmeddelandet medför också att ingen kan göra förändringar i transaktionsmeddelandet eftersom en förändring i meddelandet hade medfört att signaturen inte längre är giltig och utan en giltig signatur kommer inte transaktionen att genomföras, det vill säga föras in i den gemensamma huvudboken.

[52] Vad en plånboksfil är kommer jag återkomma till i avsnitt 3.4.1.

[53] I Bitcoin lär denna ha gjorts av Satoshi Nakamoto i samband med lanseringen.

[54] En förenklingsregel gör att en användare helt måste spendera en input som hen använder i en transaktion. Om transaktionsbeloppet understiger den input hen använder kommer en överföring av det överskjutande beloppet göras tillbaka till kontohavaren och utgöra en ny oförbrukad input.

2. att de inputs som refereras till är tillräckliga för att täcka den överföring kontohavaren föreslår och
3. att de inputs som refereras till inte redan är förbrukade.

Ett vanligt kontosaldo fås som bekant genom att alla inkomster till kontot adderas och alla utgifter subtraheras oberoende av varifrån inkomsterna kommer. Saldot är helt enkelt summan och vilka transaktioner det rör sig om är ointressant. Bitcoin-systemets sätt att hålla ordning på kontons betalningsförmåga kan tyckas onödigt komplext, men detta utgör en del i den konstruktion som gör att man kan vara säker på att samma medel inte spenderas flera gånger trots att man är i en digital miljö och trots att inga betrodda intermediärer kontrollerar transaktionerna.

Huvudboken är alltså en enorm lista över alla transaktioner som någonsin gjorts. Att ”äga” Bitcoins innebär att transaktioner i huvudbokens lista pekar mot en publik nyckeln som ”ägaren” kontrollerar genom tillgång till en privat nyckel och att transaktionerna som pekar mot den publika nyckeln ännu inte använts som inputs i en ny transaktion.

3.3.3.2 Outputs

En output är det samma som en input, men sett från avsändarens perspektiv. Att göra en output är inte så enkelt som att skicka något till ett annat konto. Det kan snarare liknas vid att deponera medel på ett offentligt konto och lägga till ett matematiskt problem som måste lösas för att mottagaren ska komma åt det deponerade. I regel är det matematiska problemet sådant att en viss publik nyckel (mottagarens) behövs för att lösa det.[55] Upplägget garanterar att endast den avsedda mottagaren får en input. Mjukvara som vanligen används vid Bitcoin-transaktioner döljer de här avancerade matematiska konstruktionerna från användaren. Upplevelsen är istället att en kontohavare skickar Bitcoin till ett annat konto och att mottagaren en stund senare ser dem på sitt konto.

3.3.4 Varför det kallas ”blockkedja” och vad blocken fyller för funktion

Hittills har jag gått igenom två viktiga delar av Bitcoin-systemets säkerhetslösning för transaktioner. För det första hur autentiseringen genom signaturer säkerställer att transaktionsmeddelandet kommer från den person som enligt Bitcoin-protokollet är behörig att förfoga över det aktuella kontot. För det andra hur nätverket kontrollerar att medlen som ska skickas inte redan är spenderade genom att kontrollera referenser till tidigare transaktioner. Men det är fortfarande ett stort problem som kvarstår och det hör ihop med den decentraliserade strukturen.

[55] Ett undantag av rent kuriosa-värde är den första transaktionen någonsin som skickades från grundaren Satoshi Nakamoto 2009 där det matematiska problemet var konstruerat så att vem som helst kunde lösa det och bli 50 BTC rikare.

3.3.4.1 Ordningens betydelse för att upprätthålla ordningen

Eftersom det rör sig om en decentraliserad struktur utgår inte transaktionsmeddelandet från ett centrum utan passerar nod för nod genom nätverket. Det finns därför ingen garanti att en viss nod får meddelandena i den ordning det skickades ut. Låt säga att två transaktionsmeddelanden skickas och att dessa anger samma referenser till inputs. Den första transaktionen ska då genomföras och den andra stoppas eftersom de inputs som refererats till redan har förbrukats. Frågan blir då hur nätverket avgör vilken transaktion som ska gå igenom. Vi kan se det som en teknisk variant av ”äldst rätt vinner” [56] där nätverket måste kunna utpeka vem som ska anses ha äldst rätt vid ett försök till dubbelutgift.

Förvisso är alla transaktioner tidsstämplade men tidsstämplar går inte att lita på helt eftersom det är relativt lätt att manipulera sådana. En nod kan därför inte med säkerhet veta vilken av två transaktionsmeddelanden som skickades först. Detta skulle kunna öppna upp för bedrägerier där någon försöker spendera samma medel två gånger och där vissa noder anser att transaktion x kom först medan andra anser att y var före. Det behövs därför ett sätt att säkerställa att konsensus kring transaktionsordningen uppnås. Det är här *blocken* och *blockkedjan* kommer in.

3.3.4.2 Blocken och kedjan

Bitcoin avgör transaktioners ordning genom att gruppera transaktioner i så kallade block och sedan sammanlänka blocken i en så kallad blockkedja.[57] Varje block har en referens till det föregående blocket och det är dessa referenser som visar i vilken ordning blocken lagts till. Blockkedjan kan spåras ända tillbaka till det första blocket av transaktioner.

Transaktioner som ingår i samma block anses ha hänt samtidigt. Transaktioner som ännu inte ingår i ett block anses som ännu inte godkända. Vilken nod som helst kan gruppera ett antal inkomna transaktionsmeddelanden och sända ut blocket till nätverket som ett förslag på hur nästa block ska se ut. Detta medför att flera noder kan skapa block samtidigt och med olika innehåll. Frågan uppstår därför hur nätverket ska avgöra vilket block det accepterar. Liksom med transaktionsmeddelandena kan vi inte förlita oss på i vilken ordning blocken når nätverket eftersom informationen skickas runt nod för nod och därför kan inkomma i olika ordning till olika noder.

3.3.4.3 Proof-of-work

Lösningen är att varje godkänt block måste innehålla det rätta svaret på ett specifikt matematiskt problem[58] som genereras av systemet självt. Lösningen går inte att komma fram

---

[56] Med detta juridiska uttryck menas att den som har ett äldre anspråk till något prioriteras framför den som har ett yngre anspråk.

[57] Blockkedjan ska inte förväxlas med den tidigare nämnda transaktionskedjan. Transaktionskedjan bygger på referenser och fungerar som en ägandehistorik. Blockkedjans funktion är att fastslå transaktionsordningen. Om blockkedjan placerar en transaktion till kontohavaren A före andra försök att spendera samma inputs kommer transaktionen att gå igenom och ingå i ägandehistoriken eller transaktionskedjan som en input som pekar mot A:s adress.

[58] Den som vill veta mer kan söka på ”Cryptographic hash functions”.

till på annat sätt än att gissa på slumpvisa kombinationer och det krävs oerhört många gissningsförsök. Det korrekta svaret utgör *proof-of-work*. Proof-of-work är data som är *dyr och tidskrävande att producera* men *lätt för andra att verifiera.* När arbetet väl är utfört är det alltså lätt för alla noder i nätverket att verifiera att blocket godkänts genom proof-of-work. För en normal dator skulle det ta flera år att hitta rätt svar. I Bitcoin är det *miners*[59] som använder sin datorkraft för att gissa och därigenom försöka uppnå proof-of-work. Den miner som först gissar rätt sänder ut sitt senaste förslag på nytt block och får det tillagt i blockkedjan.[60]

Det matematiska problemets slumpartade natur sprider ut sannolikheten för när någon gissar rätt på ett sådant sätt att det är osannolikt att två eller fler lyckas gissa rätt samtidigt. Ibland händer dock just detta och vi hamnar åter i problemet hur systemet ska avgöra vad som kommer först. Det som initialt händer är att blockkedjan förgrenar sig med de block som samtidigt accepterats genom att varje nod bygger vidare på det block som når noden först. Detta kan som sagt variera eftersom all ny information skickas runt mellan noderna i den decentraliserade strukturen. Problemet upphör normalt sett så snart nästa block är löst eftersom en regel i protokollet anger att alla noder ska byta till den längsta kedjan om det finns mer än en gren att välja på. Det kan förstås hända att det återigen är så att fler än en nod gissat rätt samtidigt även om det är ovanligt att det händer flera gånger i rad. Principen att bygga vidare på den längsta kedjan gör att systemet snabbt stabiliserar sig och uppnår konsensus kring blocken i blockkedjan.[61]

3.4 Övriga tekniska aspekter som är bra att känna till

3.4.1 Hur man håller sina Bitcoins säkra och lite om olika plånbokstyper

Bitcoin-plånböcker lagrar inte Bitcoins i sig utan de privata nycklarna som användaren behöver för att få åtkomst att disponera sina Bitcoins. Det finns fyra huvudsakliga typer av plånböcker: Mjukvaruplånböcker, online-plånböcker, hårdvaruplånböcker och pappersplånböcker. Om du hört talas om att någon blivit hackad och bestulen på sina Bitcoins så är detta något som sker på plånboksnivån när plånboken är uppkopplad.

---

[59] Termen miners, eller grävare, syftar till att skapa associationer till guldgrävare. *Miners* är särskilda noder som lånar ut datorkraft till att verifiera blocken genom proof-of-work. För detta får miners en belöning i form av nya Bitcoin som systemet självt genererar. Genom att svårigheten på problemen som ska lösas justeras så att ett nytt block genereras var tionde minut, kontrolleras också den mängd Bitcoin som tillförs till systemet genom miner-belöningar. Antalet Bitcoin som genereras per block minskar geometriskt, med en minskning med 50% varje 210 000 block d.v.s. ungefär vart fjärde år. Resultatet är att antalet Bitcoin som existerar inte förväntas överstiga 21 miljoner. Algoritmen som styr den minskade ökningen av Bitcoin har konstruerats för att efterlikna hastigheten för guldutvinning, därav termen *miners*.

[60] Förenklat kan sägas att den *hash* i varje block som utgör proof-of-work bildar en länk till föregående block och att dessa kedjor av block tillsammans innehåller en mycket stor mängd proof-of-work. Det går inte att manipulera *ett* block eftersom länkningen inte längre skulle stämma och blocket då underkännas av nätverket. För att byta ut ett block måste proof-of-work förändras i *hela kedjan*, vilket är enormt resurskrävande. Detta skyddar blockkedjan från manipulering.

[61] Transaktioner som fanns i det avklippta blocket och inte ingår i ett block i den längre grenen återgår till poolen av obekräftade transaktioner.

Mjukvaruplånböcker är datorprogram eller mobilapplikationer som kopplar upp mot Bitcoin-nätverket och tillåter användaren att disponera sina Bitcoins i nätverket. När en plånbok är uppkopplad kallas det ofta för en *hot wallet*. En sådan plånbok är mindre säker eftersom en uppkopplat plånbok kan hackas.

Onlineplånböcker fungerar på liknande sätt som mjukvaruplånböcker. Den stora skillnaden är att plånboken tillhandahålls som en tjänst, en så kallad *Software as a Service*. Detta gör att tanken med att undvika användandet av en betrodd intermediär går förlorad. Det är främst online-plånböcker som varit utsatta för omfattande säkerhetsskandaler. Många av de som tillhandahåller dessa tjänster väljer dock att förvara merparten av kundernas Bitcoins ”kallt” det vill säga *off-line* och har dessutom tecknat olika försäkringar för att täcka riskerna.

Hårdvaruplånböcker är ett säkrare alternativ och utgörs av hårdvara, oftast någon form av USB-minne. Denna typ av plånbok är en så kallad *cold wallet* och är fredad från hackers genom att själva hårdvaran genererar privata nycklar utan uppkoppling mot internet. De flesta hårdvaruplånböcker erbjuder backuplösningar och möjlighet att ställa in lösenord för åtkomst till själva plånboken.

Pappersplånböcker är alla typer av fysiska ting som håller privata nycklar.[62] Det är exempelvis enkelt att via webbtjänster generera nya nycklar och skriva ut dessa på vanlig skrivare.[63]
Det är alltid säkrast att generera nya nycklar på en enhet som inte är ansluten till internet för att garantera att ingen kan ha tjuvkikat då du genererade nycklarna.[64]

Till kategorin pappersplånböcker hör också varianter av förproducerade ”mynt” och ”sedlar”. För att dessa ska fungera tillfredställande måste mottagaren vara säker på att överlåtaren inte sett den privata nyckeln. Samtidigt måste den innehålla just en privat nyckel. Detta kan exempelvis lösas genom att den privata nyckeln är inbäddad under ett hologram som inte går att få bort utan att göra sådan åverkan att det tydligt syns. Mottagaren kan alltså vara säker på att överlåtaren inte har sett den privata nyckeln så länge hologrammet är intakt. Det enda som syns på utsidan är den publika nyckeln, som gör det möjligt för mottagaren att kontrollera i blockkedjan att det finns Bitcoin kopplat till nyckeln.[65]

Privata nycklar till större mängder Bitcoins bör aldrig förvaras online. För att genomföra transaktioner måste man förstås vara uppkopplad, men stora mängder Bitcoins bör av säkerhetsskäl förvaras ”kallt” i en hårdvaruplånbok eller pappersplånbok.

---

[62]Om du sett bilder på något som kan beskrivas som fysiska Bitcoin-mynt är detta en form av pappersplånbok.
[63] Vid tillverkning av en pappersplånbok är det olämpligt att använda en nät-skrivare av samma skäl som det är olämpligt att vara online när nya nycklar genereras – det finns risk att bli hackad. Utskrift bör istället ske genom kabel-anslutning.
[64] Det finns webbsidor som genererar nycklar och som går att spara ner lokalt så att de sedan kan användas när datorn inte längre är uppkopplad mot ett nätverk.
[65] bitcoin.se. (4 augusti 2012). *Bitcoin som sedlar eller mynt*. Hämtat från bitcoin.se: https://www.bitcoin.se/2012/08/04/bitcoin-som-sedlar-eller-mynt/ den 10 februari 2018.

3.4.2 Något om anonymitet

Bitcoin-systemet beskrivs ofta som *anonymt* eftersom det är möjligt att skicka och ta emot Bitcoins utan att utge någon personligt identifierande information. Att uppnå en någorlunda god anonymitet med Bitcoin kan dock vara tämligen komplicerat och full anonymitet kanske helt omöjlig. Mer riktigt är att kalla Bitcoin för ett *pseudo-anonymt* system. Det användare avslöjar när de skickar och tar emot Bitcoins är jämförbart med att gå under en *pseudonym*. I Bitcoin-systemet är din pseudonym den adress till vilken du får Bitcoin, det vill säga din publika nyckel. Om en pseudonym kopplas till en användares verkliga identitet, kommer alla transaktioner gjorda till den nyckeln att kunna kopplas till personen eftersom alla transaktioner finns lagrade i huvudboken.

Ett sätt att öka anonymiteten är att använda nya nycklar för varje transaktion.[66] Det finns ingen gräns för hur många publika nycklar du kan ha. Sett till den här aspekten blir det något missvisande att likna nyckelparet med ett bankkonto eftersom konton normalt sett inte skapas för engångsbruk och absolut inte i den utsträckning och med den enkelhet som förekommer inom Bitcoin-systemet. En närmare jämförelse är i så fall kontantkort till mobiltelefoner som inte är kopplade till en person utan endast till ett nummer. Vill man inte att någon ska kunna lägga samman ett mönster av vilka samtal man ringt kan man välja att använda nya kontantkort för varje samtal.

Något som ändå riskerar att röja användarens identitet är om flera adresser ingår i samma plånbok. Om användarens identitet är kopplad till någon av dessa adresser, kommer ingen av adresserna att behålla sin anonymitet. Ett sätt för användaren att öka sin anonymitet är därför att även använda flera plånböcker. Det finns smidiga program som låter användare ha flera plånböcker på ett sätt som ändå är lätthanterligt.

Ytterligare en möjlighet är så kallade *mixing services* som erbjuder att ersätta en användares Bitcoins med Bitcoins med en annan historik. Det är alltså en form av pengatvätt. Metoden är riskfylld eftersom den kräver att användaren överför Bitcoin till en tredje part som tar emot Bitcoin från olika håll i syfte att sammanblanda dem. Användaren måste alltså lita på att den tredje parten kommer att betala tillbaka det inbetalade beloppet. En del online-plånböcker kan också bidra till ökad anonymitet genom liknande sammanblandningar.

Ett ytterligare sätt att öka anonymiteten är att använda en TOR-webbläsare för att ansluta till Bitcoin-nätverket.[67] En teknikkunnig användare har alltså många möjligheter att vara anonym, eller rättare sagt förbli pseudonym.

---

[66] Detta är något Satoshi Nakamoto förespråkar i sitt White Paper. Se Nakamoto, S. (31 oktober 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System,* s 6. Hämtat från bitcoin.org: https://bitcoin.org/bitcoin.pdf den 12 december 2017.

[67] TOR står för *The Onion Router* och är ett frivilligt initiativ som tror på anonymitet och övervakningsfri internetanvändning. TOR skickar slumpmässigt runt en användarens signaler mellan noderna (användarna) i TOR-nätverket innan den når sin slutliga destination. Det blir därför extremt svårt att identifiera IP-adressen eller systemet från vilket meddelandet eller transaktionen sändes. Det var ett kombinationsupplägg av TOR och Bitcoin som möjliggjorde den uppmärksammade och illegala marknadsplatsen *Silkroad.*

3.4.3 Vad händer om den mänskliga faktorn felar?

En viktig aspekt att ha i åtanke när man har att göra med Bitcoin-systemet är att avsaknaden av betrodda intermediärer medför att det inte finns någonstans att vända sig om man exempelvis gör en överföring till fel adress eller tappar bort sin privata nyckel. Ett slarvfel kan leda till oerhörda värdeförluster och det finns ofta inget praktiskt sätt att återfå sina Bitcoins även om man juridiskt sett skulle ha rätt till exempelvis en återbetalning från den mottagare som felaktigt fått en input.

En förlorad privat nyckel innebär att de Bitcoins som hörde till den publika nyckeln i nyckelparet är förlorade. Utan tillgång till en privat nyckel som kan generera en godkänd signatur finns inget sätt att disponera medlen vilket skapar en permanent låsning. Medlen är förlorade såväl ur användarens förmögenhet som ur hela Bitcoin-ekonomin.

3.4.4 Hur säkra är nycklarna?

Det finns olika tjänster som kan generera nya nycklar. Vanligt är att använda en tjänst som är inbyggd i en så kallad mjukvaruplånbok[68] där du enkelt trycker på en knapp i applikationen för att slumpa fram ett nytt nyckelpar. Det finns också webbsidor med samma funktion. När nya nycklar slumpas fram görs ingen kontroll för att säkerställa att nycklarna inte redan finns ute och används. Om du skulle slumpa fram samma nycklar som någon annan redan använder skulle du också få tillgång att spendera alla deras Bitcoins. Sannolikheten att detta skulle ske är dock i stort sett obefintlig.[69] Däremot är det extremt viktigt att hålla sin privata nyckel just privat och i säkert förvar.

[68] För beskrivning av mjukvaruplånbok, se avsnitt 3.4.1.

[69] En jämförelse som gjorts för att förstå proportionerna är att antalet möjliga nyckeladresser vida överstiger vad som uppskattningsvis är det totala antalet sandkorn i världen. Antalet möjliga adresser är så stort att den matematiska sannolikheten av att två likadana nycklar slumpas fram är teoretisk möjlig men i princip praktiskt obefintlig.

”[…] a good investment vehicle if you have an appetite for risk. But it won’t be a currency until volatility slows down.”

- David Marcus, CEO of Paypal

4 BITCOIN SOM EKONOMISKT OCH FÖRMÖGENHETSRÄTTSLIGT FENOMEN

4.1 Egendom, objektsfiktion och ”äganderätt”

Förmögenhet består av egendom. Egendom delas upp i olika underkategorier och dessa underkategorier är ofta av betydelse för hur rättigheterna till egendomen regleras i olika situationer. Det är därför av intresse att inledningsvis försöka placera in kryptovaluta i egendomsstrukturen för att sedan kunna diskutera de juridiska konsekvenser och komplikationer som kan uppstå i specifika situationer.

En första fråga som kan behöva besvaras är om kryptovaluta alls är att räkna som egendom. Elgebrants slutsats är att ”Även utan särskild lagstiftning eller andra auktoritativa åtgärder torde kryptovalutor utgöra egendom i svensk rätt”.[70] Som en förutsättning för detta tycks Elgebrant lägga objektsfiktionen, vilken enligt honom kan anses uppkomma sedvanerättsligt genom att parterna accepterar kryptovaluta som om det vore egendom. Egendom beskrivs enligt Elgebrant med flera som ”äganderättens objekt”. Om en företeelse inte är ett objekt kan det alltså inte utgöra egendom och då inte vara föremål för äganderätten. Detta leder i min mening in i ett cirkelresonemang vars logik baseras helt på fiktion. Äganderätt kan bara anses finnas om vi *låtsas* att det finns ett objekt och vi *låtsas* att det finns ett objekt för att detta ska gå att äga.

Äganderätten är, som jag ser det, ett tankemässigt stödhjul som enligt många har pedagogiska poänger. Sådana stödhjul kan på samma sätt som för den som lär sig cykla inge en känsla av stabilitet och kontroll. I själva verket löper användaren av stödhjul större risk att vingla till och ramla om personen tvingas använda en riktig cykel. Objektsfiktionen tycks mig som ännu ett stödhjul som fungerar i par med äganderätten. Eftersom det inte går bra att bara ha ett stödhjul på ena sidan (äganderätten) måste det till ett stödhjul även på andra (objektsfiktionen). ”Icke-fysiska” fenomen görs till egendom genom objektsfiktion så att äganderätten får något att fästa vid.

Vidare skriver Elgebrant att det diskuterats i den rättsvetenskapliga debatten huruvida det är nödvändigt att tala om objekt när det är fråga om ”icke-fysisk” egendom som egentligen bara kan beskrivas utifrån de rättigheter och skyldigheter som innehavaren får genom innehavet. Han landar därefter ändå i att objektsfiktionen skulle vara nödvändig.

[70] Elgebrant, E. s 31.

Min inställning är att alla relationer till egendom bäst beskrivs genom just de rättigheter och skyldigheter som uppstår mellan de subjekt som står i relation till egendomen. De problem som uppstår i ett samhälle och som juridiken är ämnad att lösa är alltid relationella och jag tror därför att de bästa och mest pragmatiska lösningarna måste utgå ifrån de inblandade subjekten snarare än från objektet ifråga. Om detta synsätt oftare anammas avseende ”icke-fysisk” egendom ser jag det som en styrka i de resonemangen snarare än en brist som behöver läkas genom objektsfiktion.

4.1.1 ”Icke-fysisk” egendom

Att tala om ”icke-fysisk” egendom innebär att man klumpar ihop en lång rad och på många sätt väsensskilda egendomsslag enbart på grund av den gemensamma avsaknaden av fysiskt greppbar form. Som jag kommer att återkomma till nedan i avsnitt 4.3 bör man, som jag se det, ta fasta på olika egendomsslags gemensamma kvalitéer utifrån ett funktionellt perspektiv, snarare än att fästa juridisk vikt vid huruvida egendom utgörs av greppbara atomer. Jag kommer att i avsnitt 4.3 också visa att Bitcoin, från ett sådant funktionellt perspektiv, snarast har liknande kvaliteter som fysiska ting och i praktiken inte har särskilt mycket gemensamt med annan ”icke-fysisk” egendom såsom kontopengar eller olika rättigheter. Att jag ändå väljer att tala i termer av ”fysisk” och ”icke-fysisk” egendom beror alltså inte på att jag förespråkar en sådan uppdelning. Tvärtom har det sin grund i att jag motsätter mig den. För att kunna göra dessa poänger har jag dock valt att prata om Bitcoin som just ”icke-fysisk” på grund av att det inte rör sig om greppbara atomer. Detta för att kunna förklara hur bristen på fysisk form inte innebär brist på fysiska egenskaper eller *materiell integritet*. Det är, i min mening, dessa egenskaper som bör tillmätas relevans. I förlängningen ser jag det som önskvärt att hitta nya begrepp för att juridiskt kunna prata mer nyanserat om olika slag av ”icke-fysisk” egendom. Ett relevant begrepp som jag ser fördel i att använda är *besittningsbar*, vilket jag vill hävda inte behöver begränsas till greppbara atomer utan snarast bör tolkas ur ett funktionellt perspektiv. Mer om detta i avsnitt 4.3.3.

4.2 Vad för sorts egendom är Bitcoin?

Den mest grundläggande uppdelningen i olika egendomsslag är den mellan det som genom jordabalkens definitioner anses som fast egendom[71] och all annan egendom som definieras negativt gentemot fast egendom och därmed utgör lös egendom. Bitcoin är alltså lös egendom på den grund att den inte kan vara fast egendom.

Lös egendom för ofta tankarna till lösöre, det vill säga lösa saker eller fysiska ting. Lös egendom är dock ett vidare begrepp som innefattar såväl andra sorters rättigheter än det som brukar kallas ”äganderätt” exempelvis andelsrätter och nyttjanderätter. Lös egendom omfattar också ”icke-fysisk” egendom såsom immaterialrätter, finansiella instrument och överhypotek.

[71] 1 kap. 1 § Jordabalk (1970:994)

Som jag tidigare nämnt är klassificeringen av egendom ofta av betydelse för hur egendomen regleras i olika sammanhang. Eftersom kryptovaluta ännu inte är ett reglerat område ligger det nära till hands att metodiskt använda sig av analogier för att på så vis klassa kryptovaluta tillsammans med det eller de fenomen som systematiskt bär störst likhet. I följande avsnitt kommer olika kategoriseringar att diskuteras i förhållande till Bitcoin.

4.2.1 Finansiellt instrument?

Elgebrant inventerar i sin framställning ett antal möjligheter till analogier. Han anser att det är mindre troligt att kryptovaluta kan klassas som finansiella instrument, i vart fall så länge kryptovaluta förblir oreglerat. Även om kryptovaluta kan anses vara en form av värdepapper i vid mening menar Elgebrant att det är osannolikt att det rättsligt skulle definieras som sådant. Han drar här paralleller till de turer som hittills funnits kring utsläppsrätter, elcertifikat och andra kyotoenheter. Eftersom särreglering av dessa, enligt Elgebrant närliggande fenomen, varit en förutsättning för att de ska kunna bedömas som finansiella instrument är hans bedömning att även kryptovalutor kommer att behöva regleras särskilt innan de kan omfattas av definitionen i MiFID II, bilaga 1, avsnitt C. [72] [73]

Vad gäller möjligheten att klassa kryptovaluta som ett finansiellt instrument ser jag ett än större problem än det Elgebrant betonar. Finansiella instrument delas in i två klasser. Den ena klassen är den där instrumentet ger eller kan komma att ge aktieinflytande. Detta är med avseende på Bitcoin uteslutet. Som tidigare diskuterats är Bitcoin inte i sig något företag eller annan form av organisation och det är inte heller sammankopplat till något företag på ett sådant sätt att Bitcoin-innehav kan innebära ett aktieinflytande.

Den andra klassen utgörs av instrument som baserar sig på obligationsrättsliga avtal mellan två eller flera parter. För att Bitcoin ska kunna räknas hit krävs att Bitcoin, som är ett dataprotokoll utan koppling till något styrande rättssubjekt, erkänns som en juridisk person med rättskapacitet.

Att erkänna Bitcoins rättskapacitet skulle innebära att en databas med ett styrande protokoll kunde ha rättigheter och skyldigheter, egendom och skulder. Även om detta eventuellt skulle gå att konstruera hypoteser kring menar jag att det stannar just vid hypoteser. Mitt personliga synsätt faller tillbaka på Hohfelds rättighetsbegrepp som innebär att en verklig rättighet kräver en korrelerande skyldighet hos en motpart och en möjlighet att utöva påtryckning på motparten att uppfylla skyldigheten.[74] Ett dataprotokoll kommer bara att fullgöra de skyldigheter som det ursprungligen är programmerat att utföra. Det finns med andra ord inget sätt att ställa protokollet till svars genom påtryckningar utifrån. Omvänt är det svårt att se hur Bitcoin, om protokollet skulle anses ha rättigheter, skulle kunna utkräva dessa gentemot de motparter som i så fall skulle ha skyldigheter gentemot protokollet.

---

[72] Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (MiFID II).

[73] Elgebrant, E. s 36 ff.

[74] Se Hohfeld, W. N. (1913). Some Fundamental Legal Conceptions as Applied in Judicial Reasoning. *The Yale Law Journal*, s 16-59.

Som jag ser det skulle det krävas en vidgning av begreppet finansiella instrument som går långt utöver att införa en ny punkt där kryptovalutor läggs till på det sätt som gjordes med utsläppsrätter. Att låta kryptovalutor ingå i begreppet finansiella instrument innebär, som jag ser det, införandet av en ny klass bland de finansiella instrumenten.

Den väsentliga skillnaden mellan utsläppsrätter och kryptovaluta är inte det faktum att den ena är reglerad och den andra inte. Utsläppsrätter har gått att reglera så som ett finansiellt instrument på grund av att det i likhet med andra finansiella instrument bygger på en obligationsrättslig grund. Utan att erkänna dataprotokoll som ett rättsligt subjekt går det, som jag ser det, inte att tala om något obligationsrättsligt förhållande och därmed inte heller något finansiellt instrument.[75] Att jämföra Bitcoins med exempelvis utsläppsrätter framstår för mig som ett resultat av den förvirring som tycks uppstå då något av värde saknar fysisk form. Att de båda egendomsslagen saknar fysisk form är en likhet, men inte nödvändigtvis en likhet att fästa betydande vikt vid.[76]

4.2.2 Valuta, legalt betalningsmedel eller bara ett betalningsmedel?

4.2.2.1 Valuta?

För den som själv har Bitcoin känns det kanske inte så märkligt att det ofta kallas för valuta.[77] Det går att via olika tjänster köpa Bitcoin för svenska kronor och sedan att använda sina Bitcoins för att köpa tillbaka svenska kronor eller någon annan önskad valuta. Priset kommuniceras så som växelkurser i allmänhet kommuniceras. Bitcoin och många andra kryptovalutor har dessutom ett valutatecken som ytterligare förstärker bilden av att det skulle handla om just valuta.

Men att använda begreppen *kryptovaluta* eller *virtuell valuta* är möjligen missvisande ur ett juridiskt perspektiv. Enligt Elgebrant krävs, utöver att ett betalningsmedel är allmänt accepterat, även att lagstiftaren specifikt har angett att det är en valuta.[78] Jag har inte hittat stöd för att lagstiftning skulle vara ett rekvisit i bedömningen av huruvida något utgör valuta. Begreppet valuta är dock ofta starkt förknippat med pengar som utgör legalt betalningsmedel i ett eller flera länder. Att svenska sedlar och mynt är legala betalningsmedel inom riket är lagstadgat.[79] Deras lagstadgade status som legala betalningsmedel i landet Sverige bör enligt alla definitioner av valuta medföra att den svenska kronan tveklöst hör hit. Jag låter det dock vara osagt om ribban generellt ligger så pass högt för att något ska anses utgöra valuta.

---

[75] Bitcoin-certifikat är däremot att betrakta som finansiella instrument. Ett certifikat är ett skuldebrev mot en emittent. Det finns alltså en motpart och ett obligationsrättsligt förhållande. Bitcoin är i detta fall den underliggande tillgången som påverkar certifikatens värde.
[76] Betydelsen av fysisk form kommer att utvecklas nedan i avsnitt 4.3.
[77] Exempelvis genom de frekvent förekommande termerna *kryptovaluta* eller *virtuell valuta*.
[78] Elgebrant, E. s 40. Han grundar dock detta påstående på att det skulle vara ”gängse uppfattning”.
[79] Se 5 kap. 1 § Lagen (1988:1385) om Sveriges riksbank.

Bitcoin inte är bunden till någon nation utan gäller över hela världen. I några fall av nyhetsrapportering har Bitcoin angetts ha fått status som *legal tender* det vill säga *legalt betalningsmedel.* [80] Detta torde dock främst röra sig om begreppsförvirring.[81] Om världen är Bitcoins geografiska område kan i vart fall konstateras att Bitcoin inte är ett legalt betalningsmedel inom detta område eftersom det endast i ett fåtal fall (om några) har ansetts utgöra legalt betalningsmedel. Jag ser det därför som osannolikt att Bitcoin skulle rymmas inom det traditionella valuta-begreppet. En annan sak är att kryptovaluta har hanterats *som om det vore* valuta även i rättsliga sammanhang. Vad ordet valuta egentligen står för tycks variera. EU-domstolen valde att uttrycka sig i följande ordalag när de hanterade Bitcoin:

”Transaktioner rörande icke-traditionella valutor, det vill säga andra valutor än valutor som är lagligt betalningsmedel i ett eller flera länder, utgör dock finansiella transaktioner i den mån parterna i transaktionen accepterat dessa valutor som alternativa betalningsmedel till de lagliga betalningsmedlen och de inte har något annat syfte än att utgöra betalningsmedel.” [82]

Domen rörde skatterättsliga frågor och domstolen valde att låta Bitcoin inbegripas i valuta-begreppet och därigenom omfattas av undantaget i artikel 135. (e) i mervärdesskattedirektivet.[83]

4.2.2.2 Legalt Betalningsmedel

Att Bitcoin och andra kryptovalutor i de flesta länder klassas som lagligt ska inte förväxlas med att det handlar om legala betalningsmedel.[84] Viktigt i detta sammanhang är just att skilja på *betalningsmedel som är lagliga* i brist på förbjudande lagstiftning (lovliga betalningsmedel) och *legala eller lagliga betalningsmedel.* Med *legala betalningsmedel* menas ett betalmedel som erkänns av rättssystemet som giltiga för att betala en skuld med befriande verkan *(*tvungna betalningsmedel).[85] Det är alltså betalmedel med en särskild rättslig status som är tänkt att skapa trygghet för innehavaren. Kontanter utgivna av Sveriges Riksbank är exempel på legala betalningsmedel.[86] Med att Bitcoin är lagligt i Sverige menas egentligen bara att det inte är olagligt, det vill säga att företeelsen inte har förbjudits genom någon lagstiftning. Bitcoin utgör alltså ett *lovligt betalningsmedel.* Detsamma gäller de flesta andra länder. De som uttryckligen förbjudit Bitcoin är i dagsläget Bolivia, Ecuador, Kirgizistan, Bangladesh, och

---

[80] Sådan nyhetsrapportering finns bland annat angående Tyskland och Japan. Beroende på hur termen legalt betalningsmedel ska tolkas är det dock oklart om termen *legal tender* använts korrekt.

[81] Birch, D. (4 april 2017). *Legal, tender and legal tender.* Hämtat från Consult Hyperion: http://www.chyp.com/legal-tender-and-legal-tender/ den 19 december 2017.

[82] Mål C-264/14.

[83] Rådets direktiv 2006/112/EG av den 28 november 2006 om ett gemensamt system för mervärdesskatt.

[84] Uttrycket ”lagliga betalningsmedel” används synonymt med ”legala betalningsmedel”. Jag har dock valt att använda begreppet ”legala betalningsmedel” för att inte skapa ytterligare förvirring och språkförbistring i min jämförelse.

[85] Se bl.a. Lindskog, S. (2014). Betalning, Om kongruent infriande av penningskulder och andra betalningsrättsliga frågor. Stockholm: Norstedts Juridik, s. 73 f.

[86] Se 5 kap. 1 § Lagen (1988:1385) om Sveriges riksbank. Det har dock visat sig vara något som i de flesta fall går att avtala bort genom att på förhand upplysa presumtiva kunder om att kontanter inte tas emot. Som det ser ut är samhällstjänster såsom sjukvård de enda som egentligen är skyldiga att i alla lägen ta emot kontanter. Detta eftersom motparten inte alltid har något annat alternativ, vilket inte är fallet med exempelvis en restaurang eller klädbutik.

Nepal.[87] I de länder där Bitcoin klassas som lagligt kan dock inställningen till och hanteringen av Bitcoin variera kraftigt.

Bitcoin är som framgår inte något legalt betalningsmedel i Sverige.[88] Bitcoin fungerar alltså bara som betalningsmedel hos de aktörer som valt att acceptera Bitcoin. Motparten behöver inte på förhand informera om att Bitcoin och andra kryptovalutor inte accepteras eftersom det inte anses som en befogad förväntan att tro att det ska gå att betala med Bitcoins. En skuld kan alltså anses kvarstå även om gäldenären försökt betala genom att exempelvis överlämna ett fysiskt token eller en pappersplånbok som med det aktuella Bitcoin-priset täcker skuldbeloppet.

4.2.2.3 Betalningsmedel

Att Bitcoin varken utgör något traditionell valuta eller legalt betalningsmedel innebär inte att det inte är att anse som ett betalningsmedel i vidare mening. Ett betalningsmedel kan egentligen utgöras av vad som helst som går och får överlåtas och som parterna sinsemellan godtar som betalningsmedel i det enskilda fallet.[89] Detta innebär att Bitcoin är ett fullgott betalnings- eller bytesmedel så länge som mottagaren accepterar det som ett sådant. En domstol kan därför mycket väl utdöma att ett visst belopp ska anses betalt i Bitcoin med befriande verkan eller att en skuld ska betalas i Bitcoin om det är vad parterna avtalat. Detta bygger på avtalsfrihet och inte på att Bitcoin skulle utgöra något legalt betalningsmedel.

4.2.3 Fordran eller Fiatpengar – lämpliga liknelser?

4.2.3.1 Fordran

Elgebrant diskuterar också möjligheten till fordringsanalogi med hjälp av skuldebrevslagen.[90] [91] För att ett fordringsförhållande ska uppstå måste det dock finnas ett förhållande mellan gäldenär och borgenär. Att en fordring kan utgöra betalningsmedel är inte svårt att förstå. Värdet är en kombination av fordringens storlek och den risk som mottagaren tar beroende på vem som är gäldenär.

Vad som kanske inte känns lika självklart är att det mest centrala betalningsmedlet, pengar, länge var just en fordran i juridisk mening. Historiskt sett har valutor som backats upp mot en naturtillgång (vanligen guld) setts som en fordran mot staten. Riksbanken har då intagit gäldenärsposition. Riksbanken har behövt hålla sig med en guldreserv som garanterar innehavarna av valutan (borgenärerna) att deras fordran motsvarar en viss mängd guld som

[87] Wikipedia. (u.d.). *Legality of bitcoin by country or territory*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory den 1 december 2017.

[88] Se 5 kap. 1 § lagen (1988:1385) om Sveriges riksbank. Huruvida Bitcoin har sådan status i något annat land har diskuterats ovan.

[89] Elgebrant, E. s 40 med hänvisning till Lindskog, S. s 70.

[90] Elgebrant, E. s 41 ff.

[91] Lag (1936:81) om skuldebrev.

därigenom garanterar värdet.[92] Trots att de flesta valutor idag inte backas upp av någon naturtillgång dröjer sig förklaringsmodellen kvar.[93] [94]

4.2.3.2 Fiatpengar

Idag utgörs de flesta valutor, inklusive den svenska kronan, av så kallade *fiatpengar*. Ordet *fiat* är latin och betyder ungefär ”låt det bli gjort”. Fiatpengar är inte uppbackade av någon naturtillgång och har inte något inneboende värde i sitt material så som exempelvis mynt gjorda av ädelmetaller har. Värdet på fiatpengar beror istället på tillgång och efterfrågan. Tillgången går att kontrollera politiskt genom den utgivande centralbanken och genom reglering av kreditväsendet som genom sin kreditgivning hela tiden ökar tillgången. Efterfrågan beror främst på hur användbar valutan är på en marknad. Att valutan är användbar beror till stor del på att den institution som ger ut pengarna säger att de har ett värde. Det handlar i praktiken om att en stat genom sin riksbank ger ut pengar och förklarar dessa utgöra legala betalningsmedel inom jurisdiktionen, vilket garanterar valutans användbarhet inom riket.

Fiatpengar anses därigenom vara en *värdebärare* snarare än att utgöra en fordran mot staten. Detta medför dock inte den säkerhet som exempelvis ett mynt av ädelmetall innebär på grund av att myntet har ett *inneboende värde* som till stor del grundas på en begränsad tillgång av ädelmetallen. Eftersom fiatpengars värde är kopplat till den underliggande marknaden där valutan används kommer en ökad tillgång att leda till ett minskat reellt värde per enhet. Detsamma gäller om tilltron och därmed efterfrågan minskar. Eftersom valutan inte backas upp av någon egentligt användbar tillgång bygger värdet helt på den gemensamma upplevelsen av dess värde på marknaden. Generellt sätt kan sägas att valutor som svarar mot en guldreserv är stabilare och att risken för ekonomiska bubblor är större med en fiatvaluta.[95]

Att fiatpengar inte är en begränsad tillgång kan också ses som en fördel. Staten har större kontroll över tillgången och därigenom större möjlighet att kontrollera räntor, likviditet, kredittillgång och omsättningshastighet. Detta är dock inte någon fördel i en libertarians ögon, eftersom de förespråkar en spontan ekonomisk ordning utom statens kontroll. Bitcoin, som bygger på libertarianska värderingar har sökt undvika möjligheter till statlig inblandning.

4.2.3.3 Hur bör vi se på Bitcoin?

I avsnittet ovan är slutsatsen att Bitcoin inte utgör valuta eller legalt betalningsmedel i Sverige. Det kan däremot sägas utgöra ett betalningsmedel som är lagligt och som har sådana likheter med valuta att en likabehandling kan vara befogad. Diskussionen kring fiatvalutor jämfört

---

[92] Elgebrant, E. s 41.

[93] Ibid.

[94] Att förklaringsmodellen likväl dröjer sig kvar är i min mening mycket märkligt. För att det ska vara meningsfullt att använda fordran som förklaringsmodell måste fordran rimligen vara på något annat än det som analogivis utgör själva skuldebrevet. Om Riksbanken inte håller sig med något som har ett inneboende värde såsom guld, vad är det då vi skulle kunna fordra genom att överlämna våra kontanter?

[95] Investopedia. (u.d.). *Investopedia*. Hämtat från Fiat Money: https://www.investopedia.com/terms/f/fiatmoney.asp den 25 november 2017.

med valutor som backas av en underliggande naturtillgång handlar om olika former av nationell valuta som utgör legala betalningsmedel inom det aktuella landets jurisdiktion. Trots att Bitcoin inte har en sådan juridisk status kan det ändå vara intressant att fundera över om Bitcoin bär karaktärsdragen av den ena eller andra sortens valuta, främst för att bättre förstå Bitcoins karaktär.

Det i dag vanligaste betalningsmedlet, kontopengar, handlar enligt Lindskog ”inte om något annat än *fordringsförhållanden*”.[96] Det faktum att Bitcoin inte ägs av något företag eller organisation eller på annat sätt har en officiell utgivare, gör fordringsanalogin svårframkomlig. Det saknas helt enkelt en gäldenär som Bitcoin-innehavare kan rikta sitt anspråk mot. Bitcoin backas inte heller upp mot någon naturtillgång utan är helt beroende av marknadens uppfattning om dess värde.

Att det skulle röra sig om regelrätta fiatpengar är enligt ovan uteslutet eftersom Bitcoin inte är ett legalt betalningsmedel. Bitcoin bär den likheten med fiatpengar att dess värde inte backas upp av någon naturtillgång men till skillnad från fiatpengar är tillgången på Bitcoin begränsad eftersom ett tak för en maximal mängd Bitcoin är satt redan från början.[97] Algoritmen som styr tillgången på Bitcoin har konstruerats för att efterlikna hastigheten för guldutvinning. En annan viktig skillnad är att Bitcoin försöker hindra statlig kontroll, medan fiatvalutor vanligen underlättar densamma.

Huruvida Bitcoin bär mest likheter med fiatpengar eller guld är omdiskuterat.[98] Likheten är då med handelsvaran guld, inte med valutor som genom en fordran mot staten backas upp av en guldreserv. På senare år kan guld-kvaliteterna sägas ha ökat. Människor investerar i Bitcoin för att flytta över värde från fiatvalutor som tappat i trovärdighet. Bitcoin kan enligt vissa ses som ett sätt att analysera trovärdigheten hos andra valutor. Förra året var fiat-flykten störst från Kina och Venezuela.[99] Vad gäller Kina har detta att göra med att det är svårt att få ut sina pengar ut landet, vilket Bitcoin är en smidig och anonym lösning på.[100]

4.2.3.4 Pengar som pengar?

Ett ofta citerat rim på ekonomiska utbildningar är det om pengars funktion: "Money is a matter of functions four, a medium, a measure, a standard, a store." Den första funktionen är att pengar är ett *medium* för utbyte det vill säga att det går att byta pengar mot något annat. Detta kriterium uppfyller Bitcoin utan problem. Med *måttenhet* menas att det är möjligt att mäta värde i det, exempelvis att något är värt ett visst antal Bitcoin. Med standard menas en

---

96 Lindskog, S. S 66.

97 Antalet Bitcoin som tillkommer minskar geometriskt med 50% ungefär vart fjärde år. Resultatet är att antalet Bitcoin som kan existera får ett tak på 21 miljoner BTC.

98 Se bl.a. O'Connor, N. (25 november 2017). *Is bitcoin a fiat currency?* Hämtat från Capital & Conflict: https://www.capitalandconflict.com/investing-in-bitcoin/bitcoin-fiat-currency/ den 30 november 2017.

99 På sajten fiatleak.com går det att följa den så kallade fiat-flykten från världens olika ekonomier i realtid. fieatleak.com. (u.d.). *Watch the world's currencies flow to bitcoin in realtime.* Hämtat från fiatleak.com: http://fiatleak.com/den 19 december 2017.

100 O'Connor, N. (25 november 2017). *Is bitcoin a fiat currency?* Hämtat från Capital & Conflict: https://www.capitalandconflict.com/investing-in-bitcoin/bitcoin-fiat-currency/ den 30 november 2017.

standard för betalning vilket framgår av att det går att mäta en Bitcoin mot en amerikansk dollar eller Euro. Med *store* menas att det är möjligt att *lagra* värde, vilket är möjligt att göra även med Bitcoin. Kanske är det i många lägen mer givande att sätta Bitcoin som betalningsmedel som ett i mängden av andra typer av ”pengar” istället för att söka efter något existerande slag som kryptovalutor bör jämställas med.

4.2.4 Handelsvara?

I bland annat USA klassas Bitcoin sedan 2015 som en handelsvara av Commodity Futures Trading Commission (CFTC).[101] Det samma säger nu också Sydkoreas Centralbankschef och ledningen för Bank of Mexico.[102] Det har också förekommit mycket diskussion kring Bitcoins klassificering på senare tid.[103]

En av de mest inflytelserika ekonomiska kommentatorerna, Mohamed El Erian, hävdar att Bitcoin snarare bör räknas om en handelsvara än en valuta i vart fall till dess att värdet blivit betydligt stabilare.[104] Svenska Anders Elgemyr, Vd för Jarl Securities som sysslar med finansiell rådgivning och aktieanalys ser också Bitcoin snarare som en handelsvara än en valuta. Anledningen är att Bitcoin främst blivit ett instrument för spekulation. Utan en stark koppling till en underliggande ekonomi som sätter ett värde på valutan menar Elgemyr, kan priset, som i Bitcoin-fallet, komma att fluktuera kraftigt. På så vis fungerar Bitcoin snarare som en handelsvara än en vanlig valuta som genom sin koppling till den underliggande ekonomin stabiliseras.[105]

Min personliga uppfattning är att argumentationen som talar för att i dagsläget resonera kring Bitcoin som en handelsvara är mest övertygande. Om Bitcoin börjar att användas i långt större utsträckning som betalningsmedel snarare än investering kan det bli mer motiverat att se det främst som ett betalningsmedel. En handelsvara kan förstås alltid användas som

---

[101] Clinch, M. (18 september 2015). *Bitcoin now classed as a commodity in the US*. Hämtat från CNBC: https://www.cnbc.com/2015/09/18/bitcoin-now-classed-as-a-commodity-in-the-us.html den 03 december 2017.

[102] De, N. (3 november 2017). *Finance Bigwig Mohamed El-Erian Says Bitcoin Is a Commodity* . Hämtat från Coindesk: https://www.coindesk.com/allianz-chief-economic-advisor-says-bitcoin-is-a-commodity/ den 12 november 2017;
Zhao, W. (25 oktober 2017). *Bitcoin Is a Commodity Not a Currency, Says South Korean Central Bank Chief*. Hämtat från Coindesk: https://www.coindesk.com/bitcoin-commodity-not-currency-says-south-korean-central-bank-chief/ den 12 november 2017.

[103] Se bl.a. Bloomberg. (29 november 2017). *Goldman's Jeff Currie Says Bitcoin Is a Commodity*. Hämtat från Bloomberg: https://www.bloomberg.com/news/videos/2017-11-29/goldman-s-jeff-currie-says-bitcoin-is-a-commodity-video den 30 november 2017;
Forbes. (u.d.). *Forbes*. Hämtat från Think of bitcoin as a commodity, not a currency: https://www.forbes.com/pictures/efei45mhdf/think-of-bitcoin-as-a-commodity-not-a-currency/#4d3802ca1664 den 1 december 2017;
Hecht, A. (11 december 2017). *Basic Facts You Should Know About Bitcoin*. Hämtat från The balance: https://www.thebalance.com/is-bitcoin-a-commodity-4126544 den 14 december 2017.

[104] Lee, Y. N. (2 november 2017). Bitcoin is a commodity, not a currency, Allianz's Mohamed El-Erian says. Hämtat från CNBC: https://www.cnbc.com/2017/11/02/allianz-chief-economic-advisor-mohamed-el-erian-on-bitcoin-at-barclays-asia-forum.html den 3 december 2017.

[105] Törnwall, M. (13 november 2017). *Digitalt inbördeskrig sänker bitcoin: ”Valutan kommer dö*”.Hämtat från SvD Näringsliv: https://www.svd.se/digitalt-inbordeskrig-sanker-bitcoin-valutan-kommer-do den 4 december 2017.

betalningsmedel i vid mening. Att se Bitcoin som en handelsvara handlar inte om att utesluta att det är ett betalningsmedel utan om att tydliggöra att det i dagsläget inte är ett optimalt betalningsmedel och att det därför snarare används som en handelsvara.

4.3 Betydelsen av bristen på fysiska egenskaper

Även om det kan finnas fog för att betrakta Bitcoin som en vara snarare än pengar är det ändå ofrånkomligt att Bitcoin kommer att sättas i relation till just andra typer av pengar. Nedan kommer jag att diskutera de egenskaper som enligt mig är av betydelse för en juridisk förståelse av Bitcoins karaktär, framförallt utifrån ett sakrättsligt perspektiv. Jag har begränsat denna analys till att jämföra Bitcoin med de två mest vardaglig exemplen på pengar nämligen *kontanter* och *kontopengar*.

4.3.1 Relevant betalningsparadigm – en relevant fråga?

Lindskog har diskuterat skillnaderna mellan å ena sidan kontanter, det vill säga fysiska sedlar och mynt och å andra sidan kontopengar som Lindskog benämner såsom *imaginära*. Betalning är ett tillhandahållande av pengar – fysiska eller ej. Lindskog menar att man med detta synsätt kan se det så att betalningar, oavsett pengarnas form, i stora delar är att jämställa med omsättning av lösa saker även om pengar inte räknas som lösöre.[106]

Emot ett synsätt där såväl kontanter som kontopengar hanteras såsom lösa saker står det att kontopengar rent rättssystematiskt snarare utgör en fordran mot den aktuella banken eller liknande betrodda intermediär. Överföring av kontopengar utgör i så fall en fordringsöverlåtelse. En lösning vore att anse att betalning som rättslig företeelse bör följa en egen systematik oberoende av betalningssättet.[107] [108]

Lindskog hävdar vidare att han inte har hittat belägg för att behandla kontantbetalningar annorlunda än kongruenta infrianden av en generiskt bestämd varuskuld, även om pengar inte rättssystematiskt utgör lösöre. Kontanter som används för betalning ska därmed som utgångspunkt styras av samma rättsliga principer som gäller vid leverans av vara.[109]

Jag kommer nedan att argumentera för att Bitcoin, om något, snarare ska jämställas med kontanter än med kontopengar. Detta skulle i sin tur, genom en dubbelanalogi, medföra att det finns anledning att hantera Bitcoin som en vara även när det används just som betalningsmedel.

Vad gäller kontobetalning handlar det, som nämnts, rent rättssystematiskt om fordringsförhållanden. Lindskog menar emellertid att denna förklaringsmodell eller betalningsparadigm leder till långsökta konstruktioner av komplicerad art. Han menar att

---

[106] Lindskog, S. s 393 f.
[107] Ibid.
[108] Denna väg har bland annat utforskats av Ingrid Arnesdotter, Moderna Betalningsmetoder. [109] Lindskog, S. s 395.

man därför antingen bör tillämpa samma paradigm som för kontantbetalningar alternativt konstruera ett nytt och särskilt paradigm för kontobetalningar. Enligt Lindskog är det föregående att föredra, framförallt av pedagogiska skäl.[110] Lindskogs slutsats blir därmed att *"kontobetalningar ska bedömas efter samma rättsliga paradigm som kontantbetalningar"*.[111] Synsättet har även stöd i praxis.[112]

För gemene man var säkerligen den största omställningen vid övergången till kontopengar bristen på *fysisk form*. Istället för något konkret att förvara i plånboken hade pengar blivit något abstrakt, nytt och bokstavligen svårgripbart. Lindskogs resonemang bygger på de rättssystematiska frågor som uppstod när kontopengar, som nytt fenomen, kom in i bilden. Fokus läggs inledningsvis på pengars egenskaper som antingen *fysiska* eller *imaginära*. Som framhålls är dock det främsta argumentet mot en likabehandling av kontopengar och kontanter, inte det faktum att kontopengar saknar fysisk form, utan att kontopengar utgör *fordringsförhållanden*.

Att i rättsligt hänseende jämställa kontopengar med kontanter behöver, som jag ser det, inte innebära att man låtsas att kontopengar är något fysiskt. Det handlar snarare att för enkelhetens skull blunda för det faktum att kontopengar utgör ett fordringsförhållande, eftersom detta i praktiken är av liten betydelse för de inblandade parterna vid en betalning. Även om detta är ett hållbart argument fordras att inget annat talar emot ett sådant medvetet förbiseende. Det kan i det sammanhanget vara av intresse att fundera på om det är av betydelse att den ena varianten av pengar är fysisk och den andra inte. Som jag ser det behöver då bara konstateras att det *inte är av betydelse*. Att låtsas att icke-fysiska företeelser som kontopengar är fysiska och enligt Lindskogs modell tänka på kontomedel som *påsar med pengar* är inte nödvändigt. Om den fysiska formen är utan betydelse, varför behöver kontopengar i så fall göras fysiska med hjälp av objektsfiktion?

Mot detta kan ställas att Lindskogs kanske främsta argument för att likna kontopengar vid påsar med pengar på banken är att han upplever det som pedagogiskt mest välfungerande. Min uppfattning är att vi lever i en värld som blir allt mer digital. Även om tröskeln är svår att ta sig över tror jag mer på att hitta nya sätt att beskriva icke-fysiska fenomen, snarare än att ständigt använda mer eller mindre forcerade analogier. I detta finns självfallet inget rätt eller fel. Det handlar bara om olika sätt att hantera ordets makt över tanken.

4.3.2 Kontanter, kontopengar, kryptovaluta

Nedan kommer jag att behandla de egenskaper som jag ser särskild anledning att diskutera vad gäller kontanter, kontopengar och kryptovalutan Bitcoin. Mina slutsatser kommer att illusteraras genom en matris som gradvis byggs på. Slutsatserna bildar gemensamt en förklaringsmodell som är tänkt att visa dels på Bitcoins likheter med kontanter, dels hur brist fysiska egenskaper inte oreflekterat bör ges juridisk relevans.

---

110 Lindskog, S. s 96 f.
111 Lindskog, S. s 399.
112 Se bl.a. NJA 2009 s 182 och NJA 2009 s 500.

4.3.2.1 Fysik

Om fokus, i min mening felaktigt, läggs vid betalningsmedlens fysiska respektive icke-fysiska karaktär kan utvecklingen framstå som linjär i en riktning där betalningsmedlen blir allt svårare att greppa. Vi har med detta narrativ övergått från fysiska kontanter till fiktiva kontopengar för att nu gå in i en ytterligare nivå av abstraktion där fiktiva pengar, istället för att förvaltas av en bank, på något obegripligt sätt befinner sig ute i etern.

	Kontanter	Kontomedel	Kryptovalutan Bitcoin
Fysik:	Fysiskt betalningsmedel	Icke-fysiskt betalningsmedel	Ny variant av icke-fysiskt betalningsmedel

Jag vill istället beskriva utvecklingen så att den gått mot allt mer avancerade digitala lösningar och miljöer. Samtidigt ser jag Bitcoin snarare som en återgång till kontantsystemet än som en ytterligare abstraktion av kontopengar. Innan kontopengarna var pengarna bokstavligt talat i händerna på innehavaren, i plånbokens sedelklämma och börsens myntfack. Det som jag ser som den största skillnaden mellan kontanter och kontopengar är inte kontopengarnas brist på *fysik form*, utan införandet av en *betrodd intermediär*.

4.3.2.2 Åtkomst

Kontanter ger en direkt åtkomst genom att innehavaren själv, helt oberoende av andra parter, har både rätt och möjlighet att disponera sina kontanter. Kontomedel upplevs ofta på samma sätt men här har kontohavaren istället en rätt att kräva att den betrodda intermediären (typiskt sett en bank) disponerar kontohavarens pengar enligt dennes instruktioner. Även om det sällan händer, *kan* den betrodda intermediären neka kontohavaren åtkomst. Om detta skulle visa sig ogrundat har kontohavaren förvisso rättsordningens stöd för att kräva in sin fordran, men den direkta åtkomsten är ändå förlorad.

Ibland anses en betrodd intermediär ha fog för att neka kontoinnehavaren åtkoms. Exempelvis kan en betrodd intermediär, efter att ha blivit underrättad om en konkurs, neka gäldenären åtkomst till sina konton till förmån för konkursförvaltaren. Ett annat exempel är att vanliga bankkonton alltid är kopplade till en fysisk eller juridisk person. För att få intermediären att disponera innestående medel enligt viss instruktion behöver den som ger instruktionen med rimlig säkerhet kunna visa att hen är just den fysiska person som kontot är knutet till alternativt att hen har rätt att företräda motsvarande juridiska person.

Exempel:
Tänk dig in i en situation där du går in och köper en glass med kontanter, men att det framme vid kassan visar sig att du inte kan öppna din plånbok om du inte först hör av dig till ett privat företag och berättar vem du är och vad du tänkt handla.

Även om processen är så pass automatiserad och smidig att vi knappt märker av den, är detta ändå det som krävs för att kunna betala med kontopengar. Bitcoin är inte en vidareutveckling av kontopengar, *det är en motreaktion.*

Som jag ser det finns det visst fog för att göra skillnad på kontanter och kontopengar. Inte främst för att kontomedel kan ses som en fordran gentemot den betrodda intermediären, utan för att den betrodda intermediären genom sin de facto kontroll över medlen kan uppställa krav som kontohavaren måste uppfylla för att intermediären ska följa kontohavarens instruktioner, exempelvis att avslöja sin verkliga identitet.

Även Bitcoin uppställer krav för åtkomst. Den som vill instruera systemet att disponera vissa medel måste använda dithörande privata nyckel för att generera en av systemet godtagbar signatur. Min uppfattning är ändå att Bitcoin i allt väsentligt uppför sig som kontanter. Satoshi Nakamoto har uttryckt att Bitcoin är just ett ”peer-to-peer electronic *cash* system”.[113]

Skillnaden i förhållande till kontomedel är den att Bitcoin inte kan neka någon åtkomst i det enskilda fallet eftersom det inte finns någon betrodd intermediär med övergripande administratörsåtkomst som kan styra vilka transaktioner som släpps igenom och inte. Bitcoin är programmerat så att ovillkorlig åtkomst alltid ges till den som genererar en signatur med den relevanta privata nyckeln.

	Kontanter	Kontomedel	Kryptovalutan Bitcoin
Fysik:	Fysiskt betalningsmedel	Icke-fysiskt betalningsmedel	Ny variant av icke-fysiskt betalningsmed
Åtkomst:	Direkt fysisk åtkomst	Efter godkännande av betrodd intermediär	Direkt digital åtkomst

4.3.2.3 Rivalitet

Alexander Warnolf argumenterar i sin examensuppsats för en minskad fokusering på fysiska egenskaper och exemplifierar genom att hantera virtuella föremål.[114] Min uppfattning är att Bitcoin, på grund av sin kombination av att vara virtuellt och samtidigt ha en mycket hög materiell integritet,[115] har stora likheter med virtuella föremål. I sitt slutord skriver Warnolf: ”Som denna uppsats visat existerar föremål med verkligt värde, vilka trots en avsaknad av fysisk form, uppvisar samma egenskaper som lösa saker som en följd av hur de är utformade.

[113] Nakamoto, S. (31 oktober 2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Hämtat från bitcoin.org: https://bitcoin.org/bitcoin.pdf den 12 december 2017.
[114] Warnolf, A. (2007). *Egendomlig egendom - Argument för en minskad fokusering på fysiska egenskaper.* (Examensuppsats). Lund: Juridiska fakulteten vid Lunds universitet.
[115] Med *materiell integritet* hos Bitcoin avses egenskaper som, i likhet med egenskaper hos materiella ting, svårligen kan påverkas.

[…] Den viktiga vattendelaren utgörs av ett föremåls rivaliserande natur – inte huruvida det går att ta på eller ej."[116] Med rivaliserande natur menar Warnolf möjligheten att exkludera andra från att använda resursen. Han motsätter sig därmed att virtuella föremål analogivis klumpas ihop med immateriella tillgångar på grund av det faktum att båda kategorierna saknar fysisk manifestation av betydelse för värdet. Han menar att fokus istället ska läggas på föremåls rivaliserande natur. Med ett sådant synsätt påminner virtuella föremål främst om fysisk egendom "[…]traditionell egendoms rivaliserande karaktär kommer av dess fysiska manifestation medan virtuella föremål är rivaliserande som ett resultat av hur den programkod som de är uppbyggda av har konstruerats."[117]

De paralleller Elgebrant vill göra med utsläppsrätter och elcertifikat ligger närmre till hands än den jämförelse med immaterialrätter som Warnolf kritiserar. Elcertifikat och utsläppsrätter, till skillnad från immaterialrätter, är som tankekonstruktion rivaliserande. Rivaliteten hos dessa typer av icke-fysisk egendom är dock beroende av avtal och registerregler för att upprätthållas. Rivaliteten är därmed en *juridisk tankekonstruktion* och inte, som med fysiska föremål, ett *faktiskt förhållande*.

Bitcoin däremot är *rivaliserande till sin natur* enbart som ett resultat av källkodens uppbyggnad. Detta innebär, liksom hos fysiska föremål, en de facto-rivalitet. Det var just rivaliteten som fram till Bitcoins lansering hade varit den svåra nöten att knäcka och som i kryptografikretsar var det verkligt stora med innovationen.[118]

	Kontanter	Kontomedel	Kryptovalutan Bitcoin
Fysik:	Fysiskt betalningsmedel	Icke-fysiskt Betalningsmedel	Ny variant av icke-fysiskt betalningsmedel
Åtkomst:	Direkt fysisk åtkomst	Indirekt, efter godkännande av betrodd intermediär	Direkt digital åtkomst
Rivalitet:	Ja, fysisk	Indirekt, genom korrekt kontoföring hos intermediärer	Ja, genom källkodens uppbyggnad

4.3.2.4 Besittning och rådighet

Elgebrant tycks i sin framställning helt avfärda möjligheten att Bitcoin skulle kunna besittas. Han skriver exempelvis "För att presumtionsregeln i 4 kap. 18 § UB ska kunna tillämpas

[116] Warnolf, A. (2007). *Egendomlig egendom - Argument för en minskad fokusering på fysiska egenskaper.* (Examensuppsats). Lund: Juridiska fakulteten vid Lunds universitet, s 37.
[117] Ibid, s 19.
[118] Se avsnitt 2.1.4 om problemet med dubbelutgifter.

måste egendomen kunna besittas vilket omöjliggör en tillämning på kryptovaluta."[119] Den bakomliggande anledningen, förmodar jag, är avsaknaden av fysisk form.[120]

Eftersom bedömningen om huruvida något går att besitta får juridiska konsekvenser innebär en eventuell avgränsning av besittningsbegreppet till fysiska föremål att fysiska och icke-fysiska föremål kommer att behandlas olika. Frågan måste då ställas vad som motiverar att behandla fysisk och icke-fysisk egendom på olika sätt.

"[…] När en rättsregel knyter an till ett faktiskt förhållande såsom rättsfaktum har det en anledning. […] Om en rättsregel låter en faktisk närhet till en lös sak (dvs. besittningen av saken) såsom rättsfaktum leda till en viss rättsföljd, och skälet till det gör sig gällande också beträffande ett visst rättsligt förhållande med avseende på en icke-fysisk tillgång, då är det ett argument för att det rättsliga förhållandet vid tillämpning av regeln ska likställas med ett sådant faktiskt förhållande som konstituerar besittning […]. Den icke-fysiska tillgången skulle alltså, om inte motargument föranleder till annat, likställas med en lös sak och därmed anses besutten."[121]

Så skrev Lindskog i en utveckling av sin mening i rättsfallet NJA 2011 s 524. Resonemanget handlar om rådighet som är att jämställa med fysisk besittning till följd av ett *rättsligt förhållande*. I den punkt som föregår resonemanget konstaterar Lindskog att:

"I fråga om en icke-fysisk tillgång kan man nu inte tala om en fysisk närhet mellan denna och något subjekt. Det handlar helt enkelt inte om ett sådant faktiskt förhållande, som typiskt sett kännetecknar besittningssituationen […]. Om en icke-fysisk tillgång ska anses kunna besittas måste man i stället utgå från ett rättsligt förhållande. […]"[122]

Jag vill här ifrågasätta om ett *rättsligt förhållande* alltid är nödvändigt för att en icke-fysisk tillgång ska kunna anses besutten.[123] Jag vill hävda att den direkta åtkomst och rivalitet som erbjuds av Bitcoin-systemet är just sådana *faktiska förhållanden* som typiskt sätt kännetecknar besittningssituationen. Att dessa faktiska förhållanden inte kommer av fysiska egenskaper utan beror på källkodens uppbyggnad är som jag ser det utan betydelse.

"Den normativa bedömningen om det i fråga om en lös sak föreligger tillräcklig närhet till saken för att besittningsrekvisitet ska anses vara uppfyllt får med det synsättet en motsvarighet beträffande det ifrågavarande rättsliga förhållandet rörande den icke-fysiska tillgången."[124]

---

[119] Elgebrant, E. s 88.

[120] Möjligen stödjer sig Elgebrant på NJA 1984 s 656 där banktillgodohavande på motbokskonto har ansetts inte kunna vara föremål för besittning i den mening som avses i 4 kap 18 och 19 §§ utsökningsbalken. Argumentationen i rättsfallet är dock beroende av det fordringsförhållande som banktillgodohavanden inbegriper. Jag anser det därför inte tillämpligt på kryptovaluta.

[121] NJA 2011 s 524, Lindskogs utveckling av sin mening, p. 18.

[122] Ibid, p. 17.

[123] Jag menar inte att Lindskog resonerat felaktigt, men att uttalandet är mycket kategoriskt och att egendomsslag som Bitcoin sannolikt inte beaktats vid uttalandet.

[124] NJA 2011 s 524, Lindskogs utveckling av sin mening, p. 18.

På liknande vis menar jag att man i Bitcoin-fallet bör titta på den fysiska besittningens digitala motsvarighet, snarare än att uppställa ett krav på rättsligt förhållande. Att jag anser denna väg som framkomlig beror just på de särskilda egenskaper hos Bitcoin som enligt mig medför andra möjligheter än vad som typiskt sett finns för digitala resurser. Det jag här syftar på är främst de skillnader jag redan pekat ut, nämligen att såväl åtkomst som rivalitet uppstår på ett direkt sätt genom faktiska förhållanden som skapas av källkodens uppbyggnad.[125] Detta är inte något som Lindskog varken motsätter sig eller har missat. De citerade uttalandena handlar helt enkelt om mer traditionell icke-fysisk egendom som inte kan sägas ha sådana särskilda egenskaper som skulle motivera en likställning med besittning även utan ett rättsligt förhållande.

Om vi väljer att blunda för Bitcoins särart och tankemässigt gruppera Bitcoin med tidigare icke-fysiska tillgångar skulle detta, i enlighet med Lindskogs resonemang, innebära att rådighet genom ett rättsligt förhållande måste till för att läka bristen på fysisk närhet. Som jag redogjort för ovan medför Bitcoin-systemets karaktär *digitala faktiska förhållanden* som fyller samma funktioner som de fysiska förhållandena gör vid en typisk besittning, nämligen direkt åtkomst och möjlighet för besittaren av att exkludera andra genom egendomens rivaliserande natur. Det bör i min mening därför inte krävas något ytterligare för att uppnå en rådighet att jämställa med besittning. Om det på grund av Bitcoins icke-fysiska natur skulle fordras ett rättsligt förhållande utöver de faktiska förhållanden som källkoden medför så innebär detta, som jag ser det, ett högre krav för besittning av Bitcoin. Detta jämfört både med fysisk och andra typer av icke-fysisk egendom eftersom både faktiska och rättsliga förhållanden i så fall krävs.

	Kontanter	Kontomedel	Kryptovalutan Bitcoin
Fysik	Fysiskt betalningsmedel	Icke-fysiskt betalningsmedel	Ny variant av icke-fysiskt betalningsmedel
Åtkomst	Direkt fysisk åtkomst	Indirekt, efter godkännande av betrodd intermediär	Direkt digital åtkomst
Rivalitet	Ja, fysisk	Indirekt, genom korrekt kontoföring hos intermediärer	Ja, genom källkodens uppbyggnad

[125] Ett annat faktiskt förhållande som ytterligare kan anses bidra till Bitcoins materiella integritet är den begränsade tillgången. Bitcoin-värdet, liksom exempelvis värdet på guld, kan inte påverkas direkt av någon part på det sätt exempelvis den svenska kronan kan få ett förändrat värde på grund av riksbankens styrande beslut, eller bankernas kreditgivning.

Fortsättning	*Kontanter*	*Kontomedel*	*Kryptovalutan Bitcoin*
Besittning	Ja, fysisk	Ja, sådan rådighet som är att jämställa med besittning.[126]	Ja, digital

4.3.3 Digital besittning utan objektsfiktion – en möjlighet?

Av ovanstående modell framgår att åtkomst, rivalitet och besittning tycks följa en gemensam logik medan den fysiska formen följer en annan. En fråga som uppstår är om åtkomst och rivalitet bara är andra ord för besittning. Min uppfattning är att åtkomst och rivalitet är två sidor av samma mynt, nämligen besittning.

Terminologiskt vill jag kalla detta för *digital besittning* snarare än att använda mig av rådighetsbegreppet. Exakt hur besittning och rådighet bör definieras är inte någon självklarhet och begreppen används ibland synonymt.[127] Besittning är av betydelse i flera rättsliga sammanhang. Exempelvis ger besittning rättsligt skydd mot att någon egenmäktigt försöker störa besittningen. En besittare har i många fall också en bättre rätt och är av betydelse vid godtrosförvärv och tvesala. Vem som har något i sin besittning är också en viktig fråga vid konkurs för att avgöra prioritet mellan olika borgenärer.

Att tala om *digital besittning* kan säkert uppfattas som provocerande och felaktigt eftersom besittning traditionellt använts för att beskriva just förhållanden av direkt fysisk närhet. Det mest relevanta som den fysiska närheten medför är dock den *omedelbara kontroll* som *direkt åtkomst* och *de facto rivalitet* ger besittaren. Om en sådan *omedelbar kontroll* kan uppnås även för icke-fysisk egendom ser jag besittning som ett lämpligare begrepp än rådighet.

Utan att göra något anspråk på att kunna peka ut gränsen mellan vad som begreppsmässigt utgör rådighet och vad som utgör besittning, är min upplevelse att rådighet i regel används för att beskriva situationer som har en *brist i den omedelbara kontrollen*, men där bristen är sådan att den anses läkt av någon annan omständighet. I Lindskogs resonemang ovan handlar det om möjligheten att ersätta de facto-förhållanden med rättsliga förhållanden i fråga om icke-fysisk egendom. En annan variant är att överlåtaren *de facto* kan disponera ett fysiskt föremål, men är straffrättsligt förbjuden att göra det.[128] Rivaliteten är då inte någon faktisk omständighet utan är baserad på en rättslig konstruktion. Rådighet har också använts för att beskriva fall av medelbar besittning, där åtkomsten alltså är indirekt.[129]

---

126 Se bl.a. NJA 1994 s 480 och NJA 2011 s 524 (se särskilt Lindskogs utveckling av sin mening).

127 Se bl.a. Göranson, U. (2011). *Besittning och rådighet – är det samma sak?* i Lambertz, Lindskog, Möller *Festskrift till Torgny Håstad* (ss 209-224). Uppsala: Iustus.

128 Se NJA 2007 s 413.

129 Se bl.a. NJA 1984 s 456.

Ett tänkbart motargument mot en digital besittning i Bitcoin-fallet är att det är den privata nyckeln och inte de faktiska Bitcoin-enheterna som i så fall besitts och att åtkomsten därför skulle vara att anse som indirekt. Som jag ser det är detta irrelevant eftersom den privata nyckeln ger innehavaren de yttersta möjligheter som en fysisk besittning av de faktiska enheterna hade gett om en sådan varit möjlig, nämligen att överlåta och förstöra enheterna.[130] Det finns heller ingen betrodd intermediär bakom systemet som kan påverka detta direkta åtkomstförhållande.

Ett annat möjligt motargument är att ett subjekts fysiska närhet till ett objekt är iakttagbart med sinnena. Den digitala besittning jag föreslår är teoretiskt sett inte det.[131] En relevant aspekt som fysisk besittning medför är att besittarens rådighet har en yttre manifestation genom föremålets fysiska närhet till besittaren. Bristen på sådan yttre manifestation kan försvåra möjligheterna att uppskatta någons tillgångar. Vad gäller Bitcoin kan sägas att det är enkelt för besittaren att bevisa sin besittning genom att göra en överföring i blockkedjan till en annan nyckel under besittarens kontroll. Vad som däremot kan leda till problem är fall då en utomstående vill påvisa besittning, exempelvis vid en utmätning. Som jag ser det bör man inte lägga för stor vikt vid att det fysiska skulle vara iakttagbart med sinnena. Även om detta är teoretiskt korrekt finns det mycket som kan besittas fysiskt utan att detta manifesteras på ett sådant sätt som är tydligt och lätt att påvisa för en utomstående, exempelvis för att det är undangömt.

Som jag diskuterat ovan i avsnitt 4.1 ser jag, i motsats till bland andra Elgebrant, inte objektsfiktion som en nödvändighet för förståelsen av ett fenomen såsom Bitcoin. Om besittning, som föreslås i matrisen ovan, är baserad på direkt åtkomst och de facto rivalitet är objektet som sådant inte centralt för definitionen. Det handlar då inte längre om ett objekt i rummet utan om subjektets relation till en viss resurs. Om relationen medger direkt åtkomst och de facto rivalitet handlar det, som jag ser det, om besittning. En digital besittning kräver därför ingen objektsfiktion.

[130] Med förstöra menar jag här att permanent utsläcka möjligheten till åtkomst för sig själv och andra. Detta blir effekten om en säkert förvarad privat nyckel förstörs.
[131] Även om det i praktiken är högst sannolikt att den privata nyckeln inte enbart förvaras i besittarens minne utan manifesteras på något fysiskt iakttagbart sätt.


”Bitcoin is cash with wings”
- Charlie Shrem, Bitcoin Foundation

5 BITCOIN I KONKURS

5.1 Inledning

I en framställning som gör anspråk på att behandla borgenärers ställning måste självklart något sägas om borgenärsskyddet. Med borgenärsskyddet menar jag här det sakrättsliga förhållande som ger en borgenär bättre rätt till egendom än konkursboet och därmed prioritet framför övriga borgenärer. För den frågan är det bland annat centralt att utreda vad, om något, som bör utgöra sakrättsligt moment och om Bitcoin kan ha sådan särskiljningsförmåga att medlen blir föremål för separationsrätt.

Frågor som uppstår kring gränsdragningen för prioritet mellan olika borgenärer är självklart relevanta att ställa. Bitcoin är ett nytt och säreget egendomsslag och det är långt ifrån självklart hur en sakrättslig hantering bör gå till. Det är både teoretiskt utmanande och intressant att utreda gränsdragningen borgenärer emellan. Problematiken behandlas nedan i avsnitt 5.2.

De största svårigheterna som jag tror kan möta en konkursförvaltare är dock av mer praktisk natur. Som jag ser det uppstår en friktion mellan Bitcoin-protokollet och konkursinstitutets väsensskilda logiker. Friktionen undergräver konkursförvaltares möjligheter att förmå gäldenären att de facto respektera den gräns som sätts för prioritet mellan borgenärer och utöver det även de regler som skyddar borgenärskollektivet i sin helhet. Problematiken som jag ser uppstår i denna friktion behandlas nedan under avsnitt 5.3.

5.1.1 Ingår Bitcoin i konkursboet

Begreppet konkursbo används i två bemärkelser, dels för det särskilda rättssubjektet, dels för den förmögenhetsmassa som ska användas för att betala borgenärernas fordringar.[132] Här använder jag konkursbo i den senare betydelsen. Enligt 3 kap. 3 § konkurslagen[133] räknas till ett konkursbo (med vissa tillägg och undantag)" […] *all egendom* som tillhörde gäldenären när konkursbeslutet meddelades eller tillfaller honom under konkursen och som är sådan att den kan utmätas".[134]

Av lagkommentaren framgår att det med *egendom* avses tillgångar av alla slag.[135] Även om Bitcoin inte prövats med avseende på paragrafen torde det inte råda något tvivel om att Bitcoin ryms under lagrummets egendomsbegrepp.

---

[132] Karnov, lagkommentar till 1 kap. 1 § KonkL av Mikael Mellqvist.
[133] Konkurslag (1987:672).
[134] Författarens kursivering.
[135] Karnov, lagkommentar till 3 kap. 3 § KonkL av Gertrud Lennander.

En fråga som uppstår är i vilka fall Bitcoin kan anses *tillhöra gäldenären*. I inledningsfasen av en konkurs upprättar konkursförvaltaren en konkursbouppteckning där konkursboets tillgångar och skulder framgår. Konkursbouppteckningen grundas främst på en inventering av de faktiska förhållandena. Bokföring är inte alltid i god ordning eller uppdaterad men kan utgöra en utgångspunkt för vad för tillgångar och skulder som bör gå att få fram.[136] Enligt 4 kap. 18 § utsökningsbalken ska ”Gäldenären anses vara ägare till lös egendom som han har i sin besittning, om det ej framgår att egendomen tillhör annan.” Besittning utgör alltså presumtion för att lös egendom ska ingå i konkursboet.[137] Som förespråkats ovan ska innehav av en privat nyckel tolkas så att innehavaren besitter de Bitcoins som nyckeln ger åtkomst till. Denna syn leder till att en gäldenärs innehav av en sådan privat nyckel medför en presumtion för att dithörande Bitcoins ingår i konkursboet. Detsamma gäller Bitcoins som tillfaller gäldenären under konkursen, antingen genom att Bitcoin överförs till en nyckel som innehas av gäldenären eller att en ny nyckel mottas.

Att det inte rör sig om ett fysiskt föremål kan förstås göra besittningen svårupptäckt i det fall gäldenären inte är samarbetsvillig. Även om privata nycklar teoretiskt kan hållas helt i gäldenärens minne är det dock troligast att de finns nedskrivna i fysisk form eller finns lagrade på någon hårddisk. Den privata nyckeln tenderar alltså att ändå ha en sådan form att en konkursförvaltare kan påträffa den i sin inventering även om ingående åtgärder kan krävas för att komma åt skyddade och krypterade datafiler. Det kan också förväntas att pappersspåren är svårare att följa. Det finns inte någon betrodd intermediär att kontakta för att få ut kontoutdrag som kan visa på att det finns Bitcoin att hitta. Det troliga är att exempelvis inkomster i Bitcoin förvaras på en mängd unika nycklar som inte nödvändigtvis ingår i samma plånbok. Att vissa nycklar påträffas betyder inte att det inte finns fler. På samma sätt som det är svårt att veta om svarta pengar förekommit kontant utöver vad som syns på kontoutdrag är det svårt att veta om det finns Bitcoin-tillgångar som medvetet hålls utanför bokföringen och därtill skyddas av möjligheterna till anonymitet i systemet.

En annan fråga är om Bitcoin är sådan egendom som *kan utmätas*. Bitcoin ingår inte bland undantagen från utmätning i 5 kap. utsökningsbalken på grund av sin särart, även om Bitcoin på grund av andra omständigheter kan komma att uppfylla kriterierna för vissa undantag.

Min slutsats är att Bitcoin är sådan egendom som ingår i ett konkursbo och att innehav av privat nyckel utgör sådan besittning som ska utgöra presumtion för att egendomen tillhör gäldenären. Det finns inte heller någon generell anledning att undanta Bitcoin på grund av dess särart.

---

[136] Gäldenären är också skyldig att avlägga bouppteckningsed. Även andra med kännedom om relevanta förhållanden kan bli skyldiga att avlägga bouppteckningsed. Edgången är till för att personen ifråga ska intyga att bouppteckningen är korrekt, såvitt den personen vet, se 6 kap KonkL.

[137] Undantag görs i paragrafens andra stycke för skepp och luftfartyg som istället ska vara registrerade på gäldenären.

5.1.1.1 Svensk exekutionsbehörighet?

Bitcoin vill inte vara territoriellt bunden till någon stat. Systemet i sig är helt decentraliserat och har inget bakomliggande rättssubjekt som kan knytas till en viss stat. Själva Bitcoin-enheterna utgörs av en transaktionshistorik som är både decentraliserad och distribuerad över hela nätverket. Att exekutionsrättsligt ta ställning till om en viss Bitcoin-enhet finns här i landet eller om tillgången befinner sig utomlands är därför en fråga som ständigt kommer att besvaras både jakande och nekande. Detta vore rättssystematiskt besvärligt. Att låta den privata nyckeln utgöra den juridiskt relevanta tillgången medför därför, som jag ser det, exekutionsrättsliga fördelar. Om rättssystemet ser den privata nyckeln, snarare än själva Bitcoin-enheterna, som den relevanta resursen medger detta att tillgången kan knytas territoriellt till en viss stat; antingen där den privata nyckeln förvaras fysiskt eller den stat vars medborgare använder sitt eget minne för att lagra den privata nyckeln. Även om synsättet inte alltid medför att svaret ger svensk exekutionsbehörighet gör det åtminstone att frågan kan besvaras.

5.2 Borgenärsskydd – gränsdragning för prioritet

Liksom Elgebrant framhåller är kryptovalutor icke-fysik egendom som inte heller regleras genom något register på det sätt som exempelvis finansiella instrument gör. Det finns därför inga givna regler att falla tillbaka på i sakrättsliga konkurrenssituationer. Hur bedömningen av borgenärsskydd ska göras måste istället utgå ifrån allmänna sakrättsliga principer.[138] Att tillämpa allmänna regler på ett nytt egendomsslag leder ofrånkomligen till en situation där analogier blir ett nödvändigt underlag för bedömningen av borgenärsskyddet.

5.2.1.1 "Definitiv äganderätt"

I många rättsordningar räcker ett giltigt kontrakt för att ”överföra äganderätten”. I och med kontraktet blir köparen ägare, även i förhållande till säljarens borgenärer. I den svenska rättsordningen krävs i de allra flesta fall, utöver ett giltigt kontrakt, även ett sakrättsligt moment för att en köpare ska uppnå borgenärsskydd.[139] Som framgår ovan i avsnitt 4.1 ser jag svårigheter med att resonera kring Bitcoin och blockkedjor i en svensk kontext och samtidigt använda sig av äganderättsterminologin. Kanske faller Elgebrant in i en sådan terminologi därför att mycket av det som skrivits om kryptovalutor och blockkedjor är skrivet av jurister från andra rättsordningar eller teknikintresserade som tenderar att prata om äganderätt på ett mycket endimensionellt sätt.

Elgebrant skriver inledningsvis i sitt avsnitt om borgenärsskydd att ”En av de mest grundläggande frågorna som behöver utredas i en obeståndssituation är frågan om när *definitiv äganderätt* uppnås.”[140] Jag upplever terminologin som både svårhanterlig och missvisande. Själva problemet med att använda sig av begreppet ”äganderätt” blir här tydligt.

---

[138] Elgebrant, E. s 87.

[139] Det främsta undantaget till detta är konsumentköp, där köparen får sakrättsligt skydd redan vid avtalet. [140] Elgebrant, E. s 86, författarens kursivering.

De som förespråkar användandet av äganderätt som begrepp tenderar att hävda de pedagogiska fördelarna med att använda ett samlingsnamn för den situation då ett subjekt har samtliga möjliga rättigheter till ett visst objekt, ytterst möjligheten att överlåta eller förstöra egendomen. Vad är det då som äganderätten saknar när den, enligt Elgebrants terminologi, inte har uppnått statusen *definitiv*? Svaret är *prioritet*, det vill säga *bättre rätt i en konfliktsituation*. Jag vill därför omformulera frågan så att den använder en i min mening mer riktig och begriplig terminologi, nämligen att: En av de mest grundläggande frågorna som behöver utredas i en obeståndssituation är på vilka grunder en borgenär ska ges prioritet framför andra borgenärer för sitt anspråk.

Som jag ser det finns det en risk med att juridiska lösningar för Bitcoin och liknande tillgångar kan komma att konstrueras både utifrån ett osvenskt äganderättstänk och en stelbent syn på betydelsen av fysik form. Min inställning är att detta vore olyckligt och att effekten kan bli att lösningarna kan komma att bygga mer på teorier där äganderätt osynligt flyttas runt ute i etern än på de faktiska möjligheterna och riskerna i varje enskild situation.

5.2.1.2 Något om borgenärsskyddets grundläggande konfliktsituationer

Med borgenärsskydd menas ett sådant sakrättsligt skydd som till förmån för en borgenär hindrar gäldenären från att, i en obeståndssituation, använda sina kvarvarande tillgångar till att tillgodose övriga borgenärers anspråk utan att först ha tillgodosett den skyddade borgenärens intressen. Den som har borgenärsskydd ges alltså prioritet i förhållande till andra borgenärer.

I huvudsak handlar det om två varianter av konfliktsituation. I den ena har borgenären förvärvat eller tagit säkerhet i viss egendom som gäldenären ursprungligen hade bättre rätt till. Borgenären härleder alltså sin rätt från gäldenären och har det yngre anspråket. Anspråket handlar då om att få behålla sin yngre rätt till egendomen framför att egendomen dras in i konkursen och används till att tillgodose övriga borgenärers anspråk (nedan kallat *borgenärsskyddsfallen*). Typfallet är att en köpare har betalat i förskott men ännu inte hämtat egendomen.

I det andra typfallet är det istället den skyddade borgenären som har det äldre anspråket till viss egendom som av en eller annan anledning ser ut att ingå i konkursboet. Anspråket handlar då om att göra gällande sin äldre rätt till egendomen och därigenom få rätt att få ut egendomen ur konkursboet innan konkursförvaltaren tillgodoser övriga borgenärers anspråk (nedan kallat *separationsrättsfallen*). Vanligt förekommande fall är då gäldenären innehar något som tredje man kan ha bättre rätt till är exempelvis vid saklån, deposition, hyra och försäljning med återtagandeförbehåll.

I båda fallen handlar det för borgenären att visa att dess anspråk är sakrättsligt skyddat eftersom sakrätter gäller mot tredje man, del vill säga det kvarvarande borgenärskollektiv som saknar sakrättsligt skydd för sina anspråk. Den juridiska definitionen av tredje man är en fysisk eller juridisk person som berörs av ett rättsförhållande utan att vara part i det samma. I ovan beskrivna konflikttyper är detta fallet för de övriga borgenärerna, vars

möjlighet till betalning är beroende av huruvida borgenärsskydd ska anses uppnått i rättsförhållandet mellan gäldenären och den borgenär som vill göra en viss sakrätt gällande.

Möjligheten för en gäldenär att erbjuda sakrättsligt skydd för en borgenärs anspråk är av central betydelse för kreditväsendet och omsättningen. Mot intresset för kreditgivare att ta fullgod säkerhet och köparens intresse av att hen får det hen betalt för står det övriga borgenärskollektivets intresse att få utdelning på riktiga villkor, det vill säga att ingen särskild borgenär får prioriteras på oriktiga grunder. Det är främst i gränsdragningen mellan dessa motstående intressen som de sakrättsliga momenten har sin funktion.

De krav som genom sakrättsliga moment uppställs för att borgenärsskydd ska uppstå tar främst sikte på att minska risken för skentransaktioner och efterkonstruktioner. Med skentransaktioner menas att en genomförd transaktion inte varit allvarligt menad och med efterhandskonstruktion att någon oriktigt påstår att överlåtelse eller pantsättning av egendom ägt rum. En annan typ av bedrägerier går ut på att hävda att besutten egendom tillhör någon annan. Att förhindra dessa former av borgenärsskyddsbedrägerier är det sakrättsliga momentets främsta syfte råder det enighet om i litteratur och praxis.[141]

I borgenärsskyddsfallen är det sakrättsliga momentet ofta den springande punkten i bedömningen av om borgenärsskydd uppnåtts. I separationsrättsfallen handlar det istället om att visa att den aktuella egendomen uppnår kravet på specialitet och att förfoganderätten varit begränsad på sådant sätt att påståendet att egendomen tillhör annan, trotts att den är i gäldenärens besittning, är trovärdig.

5.2.2 Borgenärsskyddsfallen

För att erhålla borgenärsskydd för ett förvärv krävs i regel att parterna har ett giltigt avtal, att de uppfyllt ett sakrättsligt moment och att transaktionen är skyddad från återvinning. Frågan blir därför om dessa bedömningar påverkas av Bitcoins särart som egendomsslag och vilka analogier eller andra metoder som i så fall bör komma ifråga för att överbrygga avsaknaden på uttrycklig särreglering.

Som jag ser det finns ingen anledning att bedöma frågan om giltigt avtal på något särskilt sätt i fråga om Bitcoin. Inte heller bedömningen av återvinningsskydd föranleder någon annorlunda bedömning än för andra egendomsslag.[142] Det som främst behöver diskuteras här är vilket sakrättsligt moment, om något, som kan uppfyllas på lämpligt vis av Bitcoin. Traditionsprincipen utgör själva grunden,[143] medan varianterna publikation och denuntiation uppkommit som praktiska lösningar på situationer då tradition inte ansetts möjligt eller i vart fall praktiskt olämpligt. Väljer man att använda sig av en klassisk föreställning om fysiska

---

[141] Se Myrdal, S. (2002). *Borgenärsskyddet – Om principerna för skyddet mot överlåtarens och pantsättarens borgenärer.* Stockholm: Norstedts Juridik
samt bl.a NJA 1979 s 591, NJA 1985 s 159, NJA 1987 s 3, NJA 1988 s 257 och NJA 1995 s 367.

[142] En annan sak är att återvinning rent praktiskt försvåras. Jag återkommer till detta nedan i avsnitt 5.3.3.1.

[143] Att så är fallet anses framgå *e contrario* av Lag (1845:50 s.1) om handel med lösöre som köparen låter i säljarens vård kvarbliva.

egenskaper kan tradition verka svåruppnåeligt,[144] vilket i sin tur kan leda tanken över till publikation och denuntiation. Som jag ser det kan det vara bedrägligt för tanken även om det finns anledning att inte helt avfärda dessa möjligheter.

5.2.2.1 Publikation

Även om blockkedjan i sig kan utgöra en förträfflig plattform att använda för att distribuera exempelvis ett ägarregister på ett säkert sätt, utgör en transaktion i en blockkedja ingalunda någon publikation i sig så länge som det saknas uttryckliga registerregler för det egendomsslag vars transaktioner är tänkta att publiceras på ett sätt som kan tillfredsställa borgenärsintresset. Några sådana registerregler finns inte för Bitcoin och möjligheterna till anonymitet innebär att protokollet inte ens teoretiskt är lämpat att i sig användas för något sådant ändamål.

Jag ser dock teoretiskt inget hinder för att publikation kan användas som sakrättsligt moment genom registrering i enlighet med lösöresköplagen.[145] För att med tillräcklig tydlighet kunna utpeka vad som är lösöret i fråga torde detta dock fordra att det rör sig om överlåtelse av en viss privat nyckel snarare än om Bitcoins i sig, exempelvis sådana fysiska ”mynt” och ”sedlar” som nämnts ovan i avsnitt 3.4.1. Förteckningen av det köpta bör då innehålla uppgifter om den publika nyckeln så att allmänheten förstår att överföringar signerade med hjälp av den överlåtna privata nyckeln bara kommer att stå sig rättsligt om den angivna köparen ligger bakom transaktionen. I praktiken har jag dock svårt att se hur ett sådant upplägg alls skulle kunna vara användbart eller fördelaktigt.

5.2.2.2 Denuntiation

En eventuell användning av denuntiation som sakrättsligt moment stödjer sig analogivis på 31 § 1 st. skuldebrevslagen.[146] Enligt Elgebrant är en sådan analogilösning utesluten på grund av att det inte finns något rättssubjekt i Bitcoin-systemet som kan inta gäldenärspositionen och denuntieras i lagrummets mening.[147] Det kategoriska avfärdandet bygger dock på att det nödvändigtvis skulle vara Bitcoin-systemet som i situationen analogivis intar gäldenärspositionen. Detta varken kan eller behöver vara fallet. Bristen på rättssubjekt att denuntiera inom Bitcoin-systemet innebär, som jag ser det, endast att denuntiation inte kan utgöra det grundläggande sakrättsliga momentet för Bitcoin i alla lägen. Det finns inget som hindrar att exempelvis en fysisk representation av en privat nyckel som befinner sig hos tredje man kan överlåtas genom att parterna denuntierar tredje man om överlåtelsen. Det finns självfallet heller inget som hindrar att denuntiation används för att överlåta ett enkelt skuldebrev som avser betalning i Bitcoin istället för exempelvis svenska kronor, det vill säga en direkt tillämpning av 31 § 1 st. skuldebrevslagen.[148]

---

144 I vart fall i sin renaste form, d.v.s. utan användandet av teoretiska modeller kring rådighetsavskärande.
145 Lag (1845:50 s.1) om handel med lösöre som köparen låter i säljarens vård kvarbliva.
146 Zetterström, S. (2016). Sakrättens fyra huvudfall (4 uppl.). Uppsala: Iustus, s 88.
147 Elgebrant, E. s 104.
148 Exempelvis kan A som lånat ut Bitcoin till B, denuntiera B att istället för att återbetala skulden till A betala den till C. I ett sådant fall utgör denuntiationen till B sakrättsligt moment mellan A och C.

5.2.2.3 Tradition

Till skillnad från Elgebrant utesluter jag inte möjligheten att anse att en transaktion i blockkedjan kan anses som en fullgod besittningsförändring även om den äger rum i det digitala istället för det fysiska rummet.[149] [150] Mitt resonemang kan dock tyckas systematiskt motsägelsefullt. Jag har tidigare hävdat att den privata nyckeln ska ses som det juridiskt relevanta och besittningsbara. För att konstruera ett effektivt sakrättsligt moment utifrån Bitcoins särart bör det emellertid inte vara besittningen till den privata nyckeln som ska övergå, eftersom detta oftast medför risk att överlåtaren behåller en kopia av den privata nyckeln och därmed inte avskärs från sin rådighet.[151] I fråga om sakrättsligt moment är det istället Bitcoin-enheterna som måste överföras till en privat nyckel som överlåtaren inte har tillgång till. Som jag ser det är det dock fortfarande den privata nyckeln som är relevant ur besiktningssynpunkt.

Genom en fullständig transaktion i blockkedjan blir den nyckel som överlåtaren besitter värdelös medan den nyckel mottagaren besitter tillskrivs det överförda värdet. Konstruktionen skiljer sig förvisso från en klassisk, fysisk besittningsövergång men blir, som jag ser det, en pragmatisk lösning som de facto uppnår samma slutresultat. Det finns därför inget behov att teoretisera i termer av rådighetsavskärande. Den digitala besittningsövergången bör, som jag ser det, utgöra ett fullgott sakrättsligt moment.

5.2.3 Separationsrättsfallen

Separationsrättsfallen gäller, som nämnts ovan, den situation när en borgenär med ett äldre anspråk än gäldenären vill göra detta gällande trots att egendomen ser ut att ingå i konkursboet. Anspråket handlar då om att göra gällande sin äldre rätt till egendomen och därigenom få rätt att få ut egendomen ur konkursboet innan konkursförvaltaren tillgodoser övriga borgenärers anspråk.

5.2.3.1 Specialitet

Huruvida en borgenär ges separationsrätt avgörs främst av *specialitetsprincipen*. Att något har *specialitet* innebär att egendomen är identifierbar och går att särskilja från gäldenärens förmögenhetsmassa i övrigt. För detta har det betydelse att dess ursprungliga identitet är intakt, det vill säga att saken i fråga inte bearbetats, sammanfogats eller sammanblandats med annan egendom på sådant sätt att den ursprungliga egendomen inte längre går att särskilja.

---

[149] Elgebrant, E. s 104.

[150] Se ovan förda resonemang om digital besittning i avsnitt 4.3.3.

[151] Med undantag för exempelvis sådana säkra ”mynt” och ”sedlar” som nämns i avsnitt 3.4.1 och liknande säkra lösningar på problemet. I sådana fall finns det, som jag ser det, inget hinder för att se det som en vanlig besittningsförändring i det fysiska rummet.

5.2.3.2 Är Bitcoin fungibel egendom?

Det som främst blir aktuellt i Bitcoin-fallet är sammanblandning med andra Bitcoins. Problemet med sammanblandning hör ihop med att egendom är fungibel, det vill säga inte uppvisar några särdrag och därför är utbytbar. Pengar, spannmål, guld och bensin är klassiska exempel på fungibel egendom. Då Elgebrant behandlar separationsrätt inleder han kategoriskt med meningen ”Kryptovalutor utgör alltid fungibel egendom”.[152] Han stödjer detta på att det avgörande bedömningsmomentet är vad som normalt sätt är köparens syfte med överlåtelsen, vilket han menar är att få generisk, fungibel egendom.

Jag vill här ifrågasätta om det verkligen är så enkelt. Fungibiliteten är en av de aspekter som diskuterats flitigt i Bitcoin-världen och något som ofta tas upp som en utmaning för valutan.[153] Fungibilitet är en central egenskap hos välfungerande valutor eftersom det säkerställer det man intuitivt ser som självklart, nämligen att en svensk krona är lika mycket värd som en annan svensk krona eller att en Bitcoin är lika mycket värd som en annan Bitcoin. Guld är ett bra exempel på utpräglat fungibel egendom. Ett kilo guld är ett kilo guld är ett kilo guld.[154]

Till skillnad från ett kilo guld har varje Bitcoin en spårbar historik,[155] vilket beskrivits ovan i avsnitt 3.3. Även om en viss Bitcoin är *lika mycket* som en annan Bitcoin så kan de två ha olika historik, vilken blir identitetsskapande för dem. Anledningen till att detta anses problematiskt för Bitcoin som valuta är att spårbarheten kan leda till att Bitcoin blir *olika mycket värda.* En ny Bitcoin, som ännu inte har någon historik[156] eller en Bitcoin som blandats i en s.k. *mixing service* så att dess historik inte längre är spårbar[157] kan i vissa sammanhang bli mer värda, medan Bitcoin vars historik smutsats ner av att de ingått i illegala transaktioner kan bli mindre värda. Legitima företag som förmedlar Bitcoin-köp är i regel skyldiga under nationell lagstiftning att utföra kontroller som är ämnade att motverka penningtvätt. Eftersom Bitcoin har en historik som går att följa väljer många aktörer att granska historiken i flera led tillbaka för att försäkra sig om att de inte handlar med Bitcoin som är smutsig för att den tidigare associerats med transaktioner inom kriminell verksamhet, ofta kallade *tainted coins*. En sådan nedsmutsning kan också påverka värdet och göra en viss Bitcoin mindre gångbar på den totala Bitcoin-marknaden. Att göra spåren svårare att följa, trots att tekniken

---

[152] Elgebrant, E. s 96.

[153] Se bl.a. Donnelly, J. C. (9 oktober 2016). *Bitcoin Fungibility: The Most Important Feature?* Hämtat från Decentralize Today: https://decentralize.today/bitcoin-fungibility-the-most-important-feature-of-bitcoin-4b87a381f21a den 6 januari 2018;
Olsson, D. (5 november 2017). *Fungibility – why Bitcoin or Ether aren't the most democratic currencies yet*. Hämtat från dickolsson.com: https://dickolsson.com/what-is-fungible-currency/ den 6 januari 2018 och
The Merkle. (21 mars 2017). *What Is Bitcoin Fungibility?* Hämtat från themerkle.com: https://themerkle.com/what-is-bitcoin-fungibility/ den 6 januari 2018.

[154] Men är en konto-krona lika mycket värd som en mynt-krona? Om man med värde menar gångbarhet och köpkraft torde detta vara situationsberoende.

[155] Om inte möda lagts på att genom olika tekniker sudda ut spåren så att de inte längre går att följa.

[156] Ang. hur nya Bitcoin skapas, se avsnitt 3.3.4.3.

[157] Detta kan liknas vid penningtvätt.

bygger på en öppen huvudbok, är något som utvecklare arbetar på för att stärka Bitcoins fungibilitet.[158]

5.2.3.3 Möjligheter till separationsrätt för Bitcoin

På grund av de ovan nämnda bristerna i Bitcoins fungibilitet, torde det vara möjligt att med hjälp av viss efterforskning uppnå specialitet och på den grunden ge separationsrätt till Bitcoin även då inga särskilda åtgärder vidtagits. För att förvissa sig om att separationsrätten inte går förlorad ser jag det dock som fördelaktigt att hantera medlen i enlighet med *Lag (1944:181) om redovisningsmedel*, som i min mening bör vara tillämplig.

Grundtanken inom Bitcoin-systemet är att nya nycklar används för varje transaktion och det finns heller inte några svårigheter med att hantera Bitcoin på det sättet. Detta medför i praktiken att man med enkelhet exempelvis kan föra separata klientmedelskonton för varje transaktion. Eftersom nycklarna i sig inte behöver vara kopplade till någon fysisk eller juridisk person bör huvudmannen kräva att den som mottar medlen gör en anteckning om att den mottagande nyckeln är öronmärkt för huvudmannens medel.

För separationsrätt krävs i vanlig ordning även att mottagaren/gäldenären inte ska ha haft förfoganderätt över tillgångarna. Om så varit fallet avgörs av de villkor som huvudmannen och mottagaren/gäldenären uppställt för sina mellanhavanden.[159]

5.2.4 Möjligheter till pantsättning av Bitcoin

5.2.4.1 Handpantsättning

Som jag argumenterat för ovan i avsnitt 5.2.2 är tradition av Bitcoin möjlig genom att nyckeln anses vara det för besittningsbegreppet relevanta även om det inte är nyckeln i sig som traderas. Väljs en sådan tankekonstruktion möter handpanträtten inga större svårigheter. För att uppnå önskvärd publicitet för överlåtelsen kan det vara lämpligt att låta nycklarna ha en fysisk manifestation i form av en pappersplånbok eller liknande[160] och förstöra överlåtarens nyckel efter överlåtelsen så att denna inte kan ge sken av att fortsatt vara en värdebärare. Ett annat alternativ är att använda sig av sådana ”mynt” och ”sedlar” som nämnts ovan i avsnitt 3.4.1.

Det finns, som jag ser det, inte heller något som hindrar att sekundärpantsättning genom denuntiation av primärpanthavaren kan användas även vid pantsättning av Bitcoin. Med tanke på Bitcoins möjligheter att fördela egendomen fritt över ett obegränsat antal nycklar

---

158 Det ska här påpekas att den som får en smutsig Bitcoin inte på något vis själv behöver ha varit inblandad i något oegentligt, på samma sätt som man inte kan veta om någon i något skede köpt droger för just den hundralapp man har i plånboken.

159 I de fall gäldenären haft förfoganderätt krävs istället returrisk. Jag kommer inte att behandla detta närmare inom ramen för mitt arbete.

160 Mer om pappersplånböcker finns att läsa ovan i avsnitt 3.4.1.

förefaller det dock som en onödigt komplicerad och för sekundärpanthavaren osäker lösning att nöja sig med ett överhypotek som primärpantshavarens har kontroll över. Med Bitcoin är det enkelt att anpassa pantens storlek efter behov och låta alla panthavare ha primärpant i sin egen nyckel.

I enlighet med vad som tidigare nämnts om publikation ovan i avsnitt 5.2.2 bör en analog tillämpning av lösöresköplagen och benämningen ”köp” i säkerhetsöverlåtelseavtalet, kunna utgöra sakrättsligt moment vid en säkerhetsöverlåtelse av Bitcoin. Dock känns det otroligt att detta skulle få någon praktisk betydelse.

5.2.4.2 Pantsättning av Bitcoin hos tredje man

Som jag ser det finns inget hinder mot att analogivis använda sig av *Lag (1936:88) om pantsättning av lös egendom som innehas av tredje man* och använda sig av denuntiation som sakrättsligt moment. På grund av de praktiska möjligheterna att istället få till stånd en handpantsättning (må vara genom att instruera tredje man att utföra en transaktion i blockkedjan och därefter förstöra sin nyckel för att undvika att ge sken av att den fortfarande utgör en värdebärare) ser jag dock liten praktisk betydelse av en sådan möjlighet.

5.2.4.3 Bitcoin – en god säkerhet?

Med tanke på att Bitcoin i dagsläget har ett mycket kraftigt fluktuerande värde bör Bitcoin i alla lägen ses som en riskfylld och spekulativ säkerhet.

5.2.5 Möjlighet till escrow-liknande arrangemang utan tredje part

Andra tänkbara konstruktioner som Bitcoin rentav underlättar är möjligheten till escrow-liknande arrangemang där parterna kan välja att tillfälligt låsa vissa Bitcoin mellan sig genom att dela upp den privata nyckeln och avtala om att överlåtaren ska överlämna sin del av den privata nyckeln först efter att vissa villkor uppfyllts av mottagaren eller liknande. På så vis kan överlåtaren, utan att själv ha möjlighet att disponera aktuella Bitcoins, ändå ha viss säkerhet för att utöva påtryckning på sin motpart.

5.2.6 Något om förhållandet till företagshypoteksunderlaget

I *Lag (2008:990) om företagshypotek* framgår i andra kapitlet 1 § 2 st. vad som inte ska anses omfattas. Att Bitcoin skulle utgöra finansiella instrument enligt p. 2 är uteslutet.[161] Bitcoin kan inte heller vara föremål för inteckning enligt p. 3 eftersom inteckning kräver registerregler. Inte heller bör Bitcoin undantas under p. 4 eftersom det ovan konstaterats att Bitcoin såväl kan utmätas som ingå i en konkurs.[162] Det som återstår att bedöma är om Bitcoin ska räknas som kassa- och bankmedel enligt p.1. Eftersom Bitcoin inte är knutna till någon bank är bankmedel uteslutna. Med kassamedel avses normalt alla medel som i affärsverksamheten typiskt sett uppfattas som likvida medel. Även om så ofta torde vara fallet, är det inte självklart att alltid betrakta Bitcoin som likvida medel. Som jag diskuterat

[161] Se ovan i avsnitt 4.2.1.
[162] Se ovan i avsnitt 5.1.1.

ovan i avsnitt 4.2.4 finns det anledning att i många sammanhang överväga om Bitcoin snarare är att betrakta som en handelsvara, vilken i regel hade ingått i företagshypoteksunderlaget. Möjligheten att snabbt kunna omvandla Bitcoin till traditionellt kassamedel talar dock för att Bitcoin ändå kan komma att rymmas under undantaget även om det i den aktuella verksamheten snarare hanteras som en handelsvara.

5.3 Borgenärers skydd mot gäldenärens obehöriga förfoganden

5.3.1 En konflikt mellan motstående logiker

När Elgebrant väljer att fokusera på Bitcoins icke-fysiska natur och drar paralleller till annan icke-fysisk egendom framstår det faktum att Bitcoin är icke-fysisk som det centrala. Som att den fysiska formen, eller bristen på sådan, skulle vara den väsentliga skillnaden som gör Bitcoin svår att kontrollera juridiskt.

De stora juridiska svårigheterna som jag ser, framförallt i en obeståndssituation, handlar i grunden inte om bristen på fysisk form utan om motsättningar i förhållande till Bitcoin-systemet. Det handlar dels om systemets decentraliserade struktur som medför att det aldrig går att gå ”över huvudet” på en gäldenär som inte vill samarbete. Dels om att möjligheten till anonymitet skapar bevissvårigheter som i ett sådant läge där gäldenären väljer att inte samarbeta gör det svårare att sätta press på gäldenären genom hot om straffrättsliga sanktioner.

Vid en konkurs förordnas en utomstående förvaltare som har till uppgift att fördela konkursegendom i enlighet med statens insolvensrättsliga regelverk. Här finns en potentiell konfliktyta. Dels motsätter sig Bitcoin all form av toppstyrning. Dessutom vill Bitcoin ligga utanför statlig kontroll och förbli oberoende av jurisdiktioner. Förvaltarens roll är i min uppfattning precis en sådan *administratör* eller *betrodd intermediär* som systemet vill utesluta från åtkomst. Jag återkommer till detta nedan i avsnitt 5.3.2.

Utöver att eliminera behovet av en betrodd intermediär är en av de viktigaste (eller kanske den viktigaste?) egenskapen för många användare, möjligheten att legitimera sig mot systemet utan att identifiera sig såsom fysisk eller juridisk person. Detta kan dels skapa praktiska svårigheter för konkursförvaltningen, dels skapa betydande bevissvårigheter vid ett eventuellt åtal. För många gäldenärer är hotet om straffsanktioner säkerligen ett effektivt påtryckningsmedel enbart genom det psykologiska motståndet mot att göra något brottsligt. För andra gäldenärer torde effektiviteten vara i hög grad beroende av risken att bli påkommen, risken att bli dömd och straffets kännbarhet i förhållande till den potentiella vinningen om så inte blir fallet. Här uppstår ytterligare en konfliktyta med Bitcoin och dess bakomliggande ideologier. Jag återkommer till detta nedan i avsnitt 5.3.3.

Ett ytterligare problem som inte bygger på motsättningen mellan Bitcoin och konkursinstitutet är att Bitcoins struktur gör att varje användare själv ansvarar för sin egen säkerhet. Som påtalats i avsnitt 3.4.3 kan stora värden gå förlorade på grund av mänskliga

misstag eller bristande skydd mot dataintrång. Till skillnad från bank-fallet finns här ingen att kontakta för att få ut uppgifter om var medlen tagit vägen. Det är därför svårt att hitta något rättssubjekt att rikta anspråk mot om oturen är framme. Detta ställer också höga krav på konkursförvaltarens förståelse för tekniken och vilka säkerhetsåtgärder som bör tas för att inte riskera att stora värden går förlorade genom misstag vid säkerställandet av exekutionsunderlaget eller efter det att förvaltaren tagit över kontrollen. Kort om detta finns nedan i avsnitt 5.3.4.

5.3.2 Säkerställande av exekutionsunderlaget

Enligt 3 kap. 1 § Konkurslagen[163] får, sedan beslut om konkurs meddelats, gäldenären inte längre råda över egendom som tillhör konkursboet. Ett första steg för konkursförvaltaren är därför att säkerställa exekutionsunderlaget.

Banktillgodohavanden säkerställs genom att banken kontaktas och får reda på att gäldenären inte längre får råda över bankmedlen eftersom dessa nu ingår i konkursboet och därför ska stå under konkursförvaltarens kontroll. Banken är därmed rättsligt hindrad från att utge medel till gäldenären. Bitcoin har inget bakomliggande rättssubjekt och det finns därför inget subjekt som kan försättas i ond tro angående gäldenärens rätt att disponera de Bitcoin som gäldenären kontrollerar genom innehav av privata nycklar. Detta ligger i själva grundidén bakom Bitcoin och användandet av publik-nyckel-kryptografi. Ingen (enligt Bitcoin-protokollet) utomstående ska ha möjlighet att disponera Bitcoin på någon annans nyckel. Det finns inga betrodda administratörer med övergripande åtkomst.

Konsekvensen blir att Bitcoin *de facto* kontrolleras helt enligt protokollets syn på ägande eller bättre rätt.[164] Gentemot protokollet är innehavaren av en privat nyckel alltid den ”riktiga” ägaren. Detta hör ihop med anonymiteten. Om inget rättssubjekt kopplats till den publika adressen och innehavaren använt sig av ytterligare åtgärder för att förbli anonym finns det inget alternativt sätt att bevisa sin behörighet gentemot systemet. Det är alltså omöjligt att inneha en privat nyckel men vara obehörig enligt systemet eftersom möjligheten att använda den privata nyckeln, i brist på koppling till fysisk eller juridisk person, är det enda kravet för behörighet. Förvaltaren kan därför behöva förmå gäldenären som innehar en privat nyckel att samarbeta.

Detta är inte unikt för Bitcoin som egendomsslag. En jämförelse med bank-fallet är främst relevant därför att det annars är lätt att se just bankmedel som det egendomslag som bär mest likheter med Bitcoin. Min uppfattning är att det, särskilt i konkurssituationer, snarare finns anledning att uppmärksamma skillnaderna. Stora delar av ett konkursbo kan vara under gäldenärens kontroll på ett sådant sätt att det krävs samarbete från gäldenärens sida för att säkerställa exekutionsunderlaget. Det går inte alltid att räkna med att en gäldenär är

163 Konkurslag (1987:672).

164 Att någon kan ha stulit en privat nyckel eller lurat någon att skicka Bitcoin till en publik nyckel som kontrolleras av en annan än den mottagare som avsändaren avsett är en annan sak som inte kommer att behandlas inom ramen för detta arbete.

samarbetsvillig. Ytterst kan konkursförvaltaren använda sig av hot om straffrättsliga sanktioner, framförallt genom brottsbalkens elfte kapitel om brott mot borgenärer.[165]

I korthet kan situationen beskrivas så att en konkursförvaltare har två möjliga scenarion vid säkerställande av exekutionsunderlaget. Antingen är egendom som ska säkerställas sådan att detta kan ske utan samverkan från gäldenärens sida. Detta är ofta fallet med icke-fysiska tillgångar såsom kontopengar, immaterialrätter och finansiella instrument där det finns en tredje part som kan underrättas med den verkan att rådighet över egendomen övergår från gäldenären till konkursförvaltaren. Scenariot är gynnsamt för borgenärskollektivet. Dels är säkerställandet oberoende av gäldenärens samarbetsvilja, dels tenderar säkerställandet att vara effektivt på så sätt att det inte föranleder några extraordinära kostnader för konkursförvaltningen.

Det andra scenariot är att egendomen är sådan att konkursförvaltaren måste förmå gäldenären att samarbeta och överlämna egendomen till förvaltaren (om den inte kan beslagtas). För borgenärskollektivet finns här en risk att gäldenären inte är samarbetsvillig och att hot om straffsanktioner i förlängningen leder till både kostsamma och utdragna processer. Om det generella bevisläget för konkursförvaltningen är dåligt kan det tänkas att incitamenten att försöka undandra tillgångar ökar samtidigt som förutsättningarna för konkursförvaltningen att återfå medel som undandragits minskar.

Det enda säkra sättet att säkerställa att tillgångar bestående av Bitcoin blir kvar i konkursboet och kontrolleras av konkursförvaltaren är att genomföra en transaktion i blockkedjan till en ny publik nyckel vars privata nyckel konkursförvaltaren, och inte gäldenären, förfogar över. För att få tillgång till den privata nyckeln krävs ofta samarbete från gäldenärens sida. Möjligen kan datorer samlas in och privata nycklar tas fram av tekniska experter, men är gäldenären tekniskt kunnig torde de privata nycklarna vara väl skyddade från åtkomst från utomstående. Dessutom kan en privat nyckel lika gärna förvaras på en lapp i gäldenärens innerficka eller rent av i dennes minne. På många sätt kommer ett säkerställande av Bitcoin snarare påminna om säkerställandet av lösa, fysiska saker än icke-fysiska såsom bankmedel.

5.3.3 Betydelsen av anonymitet och bevissvårigheter

Eftersom gäldenärens samarbetsvilja ytterst kan komma att vila på hot om straffsanktioner och effektiviteten i dessa hot är beroende av åklagarens möjlighet att visa att något oegentligt ägt rum, är det centralt för påtryckningsmedlens effektivitet att obehöriga förfoganden går att bevisa. Här finns, som jag ser det, betydande svårigheter.

På grund av möjligheterna till anonymitet går det att se till att den publika nyckeln är det enda som går att få fram om mottagaren. Hur kan man då bevisa att någon som hävdar att den på grund av ett skrivfel, av misstag sickat Bitcoin till fel adress, inte själv innehar det nyckelpar som Bitcoins ”felaktigt” har skickats till? Hur bevisar man att någon inte tappat bort eller glömt sin privata nyckel om denne hävdar det? Jag vill mena att det går att ljuga

[165] Brottsbalk (1962:700).

om missöden på ett sätt som är svårt att motbevisa och samtidigt, på ett svårligen spårbart sätt, ha kvar tillgången.

Som jag diskuterat ovan i olika sammanhang bär Bitcoin snarast likhet med kontanter, vilka har sådana egenskaper att de ofta användas för affärer som parter av någon anledning vill hålla utanför böckerna. En skillnad som jag ser som problematisk i förhållande till kontanter är dels att det vid Bitcoin-transaktioner inte krävs någon logistik för att överföra mycket stora värden, dels att en uppdiktad historia enligt ovan ändå måste anses relativt sannolik. Att någon gjort ett litet skrivfel då hen manuellt försökt fylla i en lång rad slumpvisa tecken (en publik nyckel) känns ju mycket mer sannolikt än att någon skulle ha råkat ge en stor summa kontanter till fel person. Att exempelvis en hårddisk kraschat eller en pappersplånbok förkommit förefaller också mer sannolikt än att någon av misstag skulle ha tappat bort eller råkat förstöra en stor mängd kontanter.

Dessa farhågor är förvisso rent spekulativa, men jag vill ändå hävda att det finns anledning att fundera över och problematisera med vilken enkelhet det potentiellt går att ljuga om Bitcoin-innehav och komma undan med det.

5.3.3.1 Påverkan på möjligheten till effektiv återvinning

Även om det går att visa att en transaktion ägt rum och att den är av sådan art att den ska återvinnas kan det bli praktiskt omöjligt att få till stånd en återvinning. Anledningen är att gäldenären och betalningsmottagaren kan ha vidtagit sådana åtgärder att transaktionen blir mycket svår (och i vissa fall omöjlig) att spåra till en fysisk eller juridisk person. Det finns helt enkelt inget subjekt att rikta sitt krav på återvinning mot. Konkursförvaltaren blir då helt beroende av att få uppgifter från gäldenären om vem som mottagit Bitcoin. Eftersom gäldenärens samarbetsvilja ytterst kan komma att vila på hot om straffsanktioner och effektiviteten i dessa hot till stor del måste basera sig på det generella bevisläget, är min slutsats att återvinningsbara transaktioner i praktiken kan komma att bli mycket svåra att återvinna om man har att göra med en bedräglig gäldenär.

5.3.4 Konkursförvaltarens ansvar och något om försäkring

I 17 kap. 1 § 1 st. konkurslagen sägs att ”En förvaltare skall ersätta de skador som han vid fullgörande av sitt uppdrag uppsåtligen eller av oaktsamhet tillfogar boet, en konkursborgenär eller gäldenären […]”. Som bland annat utvecklats ovan i avsnitt 3.4.3 kan små misstag innebära att stora värden går förlorade. Ett litet skrivfel vid överföringen som ska säkerställa exekutionsunderlaget kan få medlen att hamna i händerna på någon annan vars identitet inte alltid kan spåras. Det samma gäller om medel stjäls genom hacking på plånboksnivå. En hårdvarukrasch kan också göra att nycklar och de medel som knutits till dem för alltid är förlorade. Det är inte svårt att se hur en konkursförvaltare utan närmare kunskap om Bitcoins särart skulle kunna råka ut för missöden på grund av en oförsiktighet som bottnar i okunskap om riskerna. Det är svårt att sia om vilken kunskapsnivå som kan förväntas av en konkursförvaltare på ett så pass nytt och säreget område. I lagrummet anges att ”[…]Skadeståndet kan jämkas efter vad som är skäligt med hänsyn till handlingens

beskaffenhet, skadans storlek och omständigheterna i övrigt." Det ter sig rimligt att tänka sig att en förvaltare kan tänkas undgå ansvar där värden gått förlorade på grund av teknisk okunskap även om motsvarande förlust inte ansetts ursäktlig om undvikandet av riskerna inte krävde någon specialkompetens.

Även om förvaltaren inte skulle bli ersättningsskyldig är det självfallet alltid viktigt att minimera riskerna för onödiga förluster. Viktigt att tänka på är framförallt att säkerställandet av Bitcoin ska ske genom en transaktion i blockkedjan och att transaktionen bör ske till en nyckel som förvaras på ett säkert sätt. Om en online-plånbok används,[166] (vilket kan vara den enklaste och snabbast lösningen för en förvaltare som inte är förberedd på situationen) är det en god ide att ta reda på hur företaget förvarar Bitcoin och om de är försäkrade.

[166] Online-plånböcker beskrivs ovan under avsnitt 3.4.1.

6 NÅGRA AVSLUTANDE REFLEKTIONER

Som jag visat är det lätt hänt att hamna i tankebanor där den fysiska formen blir avgörande. Sådana tankebanor leder, som jag ser det, till (miss)uppfattningen att det framförallt skulle vara bristen på fysisk form som gör Bitcoin juridiskt svårhanterlig. Jag har med detta arbete velat utmana synen på det fysiska som en avgörande faktor, framförallt för kryptovalutan Bitcoin som jag menar, på grund av sin materiella integritet, ger anledning att tala om en ny möjlighet; *digital besittning*.

Det jag har velat problematisera är den krock av ideologisk-systematiskt motstående logiker som jag anser uppstår mellan å ena sidan Bitcoin-protokollet och å andra sidan konkursinstitutet. Konkursinstitutet har inte varit föremål för den oro och det missnöje som föranledde framväxten av cypherpunk-rörelsens ideologiska visioner eller utformningen av Bitcoin-protokollet, men konkurssituationen består just av den sortens relationer som Bitcoin-systemet motsätter sig. Min uppfattning är att detta potentiellt leder till problematiska konfliktytor. Även om Cypherpunk-rörelsen inte uttryckligen förklarat krig mot konkursinstitutet blir konflikten en ofrånkomlig bieffekt.

Genom en ökad kunskap och förståelse för Bitcoin, såväl som ideologiskt som tekniskt och förmögenhetsrättsligt fenomen, blir juristen bättre rustad att tackla de nya utmaningar som kan uppkomma i denna systemkrock. En ökad kunskap leder förhoppningsvis också till att den nya teknikens spännande egenskaper kan användas konstruktivt i det juridiska arbetet.

Något som varit påtagligt under mitt arbete är att uppfattningen om Bitcoin tycks dela människor i de som är *för* och de som är *emot*. De som ser Bitcoin som ett fantastiskt framsteg som möjliggör en verkligt rättvis ekonomi och de som ser det som ett ont påfund vars främsta syfte är att underlätta skumraskaffärer. På frågan om jag personligen anser att Bitcoin är något bra eller dåligt, blir mitt svar det för jurister så klassiska ”det beror på”.

Framförallt är Bitcoin oerhört *intressant*.

KÄLLFÖRTECKNING

Litteratur

Arnesdotter, I. (1996). *Moderna betalningsmetoder*. Stockholm: Nerienius & Santérus.

Elgebrant, E. (2016). *Kryptovalutor, Särskild rättsverkan vid innehav av bitcoins och andra liknande betalningsmedel*. Stockholm: Wolters Kluwer Sverige AB.

Göranson, U. (2011). Besittning och rådighet – är det samma sak? i G. Lambertz, S. Lindskog, & M. Möller, *Festskrift till Torgny Håstad* (ss. 209-224). Uppsala: Iustus.

Hohfeld, W. N. (1913). Some Fundamental Legal Conceptions as Applied in Judicial Reasoning. *The Yale Law Journal*, 16-59.

Lindskog, S. (2014). *Betalning, Om kongruent infriande av penningskulder och andra betalningsrättsliga frågor*. Stockholm: Norstedts Juridik.

Myrdal, S. (2002). *Borgenärsskyddet – Om principerna för skyddet mot överlåtarens och pantsättarens borgenärer*. Stockholm: Norstedts Juridik.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tillgänglig för nedladdning från https://bitcoin.org/bitcoin.pdf.

Warnolf, A. (2007). *Egendomlig egendom - Argument för en minskad fokusering på fysiska egenskaper. (Examensuppsats)*. . Lund: Juridiska fakulteten vid Lunds universitet.

Zetterström, S. (2016). *Sakrättens fyra huvudfall* (4 uppl.). Uppsala: Iustus.

Internetkällor

Birch, D. (4 april 2017). *Legal, tender and legal tender*. Hämtat från Consult Hyperion: http://www.chyp.com/legal-tender-and-legal-tender/ den 19 december 2017.

Bitcoin Wiki. (u.d.). *Bitcoin Wiki*. Hämtat från https://en.bitcoin.it/wiki/Main_Page

bitcoin.se. (4 augusti 2012). *Bitcoin som sedlar eller mynt*. Hämtat från bitcoin.se: https://www.bitcoin.se/2012/08/04/bitcoin-som-sedlar-eller-mynt/ den 10 februari 2018.

Bloomberg. (29 november 2017). *Goldman's Jeff Currie Says Bitcoin Is a Commodity*. Hämtat från Bloomberg: https://www.bloomberg.com/news/videos/2017-11-29/goldman-s-jeff-currie-says-bitcoin-is-a-commodity-video den 30 november 2017.

Boaz, D. (1 januari 1999). *Key Concepts of Libertarianism*. Hämtat från Cato Institute: https://www.cato.org/publications/commentary/key-concepts-libertarianism den 16 december 2017.

Clinch, M. (18 september 2015). *Bitcoin now classed as a commodity in the US*. Hämtat från CNBC: https://www.cnbc.com/2015/09/18/bitcoin-now-classed-as-a-commodity-in-the-us.html den 3 december 2017.

CuriousInventor. (YouTube-kanal) https://www.youtube.com/channel/UCOGrxFj_j7PZRQM63OFCwmA

De, N. (3 november 2017). *Finance Bigwig Mohamed El-Erian Says Bitcoin Is a Commodity* . Hämtat från Coindesk: https://www.coindesk.com/allianz-chief-economic-advisor-says-bitcoin-is-a-commodity/ den 12 november 2017.

Donnelly, J. C. (9 oktober 2016). *Bitcoin Fungibility: The Most Important Feature?* Hämtat från Decentralize Today: https://decentralize.today/bitcoin-fungibility-the-most-important-feature-of-bitcoin-4b87a381f21a den 6 januari 2018.

fieatleak.com. (u.d.). *Watch the world's currencies flow to bitcoin in realtime*. Hämtat från fiatleak.com: http://fiatleak.com/

Forbes. (u.d.). *Think of bitcoin as a commodity, not a currency*. Hämtat från Forbes: https://www.forbes.com/pictures/efei45mhdf/think-of-bitcoin-as-a-commodity-not-a-currency/#4d3802ca1664 den 1 december 2017.

Greenhalgh, H. (21 september 2016). *Blockchain, Asset managers quick to adopt blockchain* . Hämtat från Financial Times: https://www.ft.com/content/ee6d8454-7f27-11e6-bc52-0c7211ef3198 den 12 december 2017.

Hecht, A. (11 december 2017). *Basic Facts You Should Know About Bitcoin* . Hämtat från The balance: https://www.thebalance.com/is-bitcoin-a-commodity-4126544 den 14 december 2017.

Huges, E. (9 mars 1993). *A Cypherpunk's Manifesto*. Hämtat från activism.net: https://www.activism.net/cypherpunk/manifesto.html den 12 december 2017.

Investopedia. (u.d.). *Double-Spending*. Hämtat från Investopedia: https://www.investopedia.com/terms/d/doublespending.asp den 16 december 2017.

Investopedia. (u.d.). *Investopedia*. Hämtat från Fiat Money: https://www.investopedia.com/terms/f/fiatmoney.asp den 25 november 2017.

Ivan on Tech. (YouTube-kanal) https://www.youtube.com/channel/UCrYmtJBtLdtm2ov84ulV-yg

Ivan on Tech. (den 22 september 2017). *Difference between COIN, TOKEN and PROTOCOL - Programmer explains*. Hämtat från YouTube: https://www.youtube.com/watch?v=pcilyT3fh-0 den 30 januari 2018.

Lantmäteriet. (24 augusti 2016). *Lantmäteriet har tittat på blockkedjetekniken*. Hämtat från Lantmäteriet: https://www.lantmateriet.se/sv/Nyheter-pa-Lantmateriet/lantmateriet-har-tittat-pa-blockkedjetekniken/ den 4 december 2017.

Lee, Y. N. (2 november 2017). *Bitcoin is a commodity, not a currency, Allianz's Mohamed El-Erian says*. Hämtat från CNBC: https://www.cnbc.com/2017/11/02/allianz-chief-economic-advisor-mohamed-el-erian-on-bitcoin-at-barclays-asia-forum.html den 3 december 2017.

Leonard, S. (21 juni 2017). *The Internet of Value: What It Means and How It Benefits Everyone.* Hämtat från ripple.com: https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/ den 27 september 2017.

Levy, S. (1 februari 1993). *Crypto Rebels*. Hämtat från Wired: https://www.wired.com/1993/02/crypto-rebels/ den 28 oktober 2017.

Libertarian Party. (u.d.). *Bitcoin*. Hämtat från Libertarian Party: https://www.lp.org/donate/bitcoin/ den 17 december 2017.

Marr, B. (21 september 2017). *14 Things Everyone Should Know About Blockchains*. Hämtat från Forbes: https://www.forbes.com/sites/bernardmarr/2017/09/21/14-things-everyone-should-know-about-blockchains/#4097154252a7 den 12 december 2017.

Morris, D. Z. (3 december 2017). *Here's What Bitcoin's Smartest Skeptics are Telling Investors*. Hämtat från Fortune: http://fortune.com/2017/12/03/heres-what-bitcoins-smartest-skeptics-are-telling-investors/ den 11 december 2017.

O'Connor, N. (25 november 2017). *Is bitcoin a fiat currency?* Hämtat från Capital & Conflict: https://www.capitalandconflict.com/investing-in-bitcoin/bitcoin-fiat-currency/ den 30 november 2017.

Olsson, D. (5 november 2017). *Fungibility – why Bitcoin or Ether aren't the most democratic currencies yet*. Hämtat från dickolsson.com: https://dickolsson.com/what-is-fungible-currency/ den 6 januari 2018.

OpenPGP. (u.d.). *OpenPGP, Email encryption. For all operating systems. Standing the test of time.* . Hämtat från openpgp.org: https://www.openpgp.org/ den 27 november 2017.

Redman, J. (16 januari 2017). *Do Satoshi's Libertarian Statements from the Past Matter Anymore?* Hämtat från bitcoin.com: https://news.bitcoin.com/satoshis-libertarian-statements-past-matter-anymore/ den 12 december 2017.

Reiff, N. (den 12 december 2017). *Can Bitcoin Be Hacked?* Hämtat från Investopedia: https://www.investopedia.com/articles/investing/032615/can-bitcoin-be-hacked.asp den 26 december 2017.

Törnwall, M. (13 november 2017). *Digitalt inbördeskrig sänker bitcoin: "Valutan kommer dö"* . Hämtat från SvD Näringsliv: https://www.svd.se/digitalt-inbordeskrig-sanker-bitcoin-valutan-kommer-dov den 4 december 2017.

The Economist. (9 maj 2015). *Blockchain, The next big thing*. Hämtat från The Economist: https://www.economist.com/news/special-report/21650295-or-it-next-big-thing den 12 december 2017.

The Merkle. (21 mars 2017). *What Is Bitcoin Fungibility?* Hämtat från themerkle.com: https://themerkle.com/what-is-bitcoin-fungibility/ den 6 januari 2018.

Trustnodes. (21 september 2017). *Bitcoin Millionaires Announce Plans to Form a Libertarian Country*. Hämtat från trustnodes.com: http://www.trustnodes.com/2017/09/21/bitcoin-millionaires-announce-plans-form-libertarian-country den 12 december 2017.

Wallenberg, B. (26 april 2017). *Dagens Industri, Digital*. Hämtat från Spotify köper blockkedjebolag: https://digital.di.se/artikel/spotify-koper-blockkedjebolag den 12 december 2017.

Wikipedia. (2 december 2017). *Cypherpunk*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Cypherpunk den 14 december 2017.

Wikipedia. (23 oktober 2017). *Eric Hughes (cypherpunk)*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Eric_Hughes_(cypherpunk) den 15 december 2017.

Wikipedia. (u.d.). *Legality of bitcoin by country or territory*. Hämtat från Wikipedia: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory den 1 december 2017.

Yaw-Owusu, F. (1 november 2017). *Cryptocurrencies, Blockchain: Moving from the Internet of Information to the Internet of Value*. Hämtat från The Market Mogul: https://themarketmogul.com/blockchain-information-internet-value/ den 12 december 2017.

Zhao, W. (25 oktober 2017). *Bitcoin Is a Commodity Not a Currency, Says South Korean Central Bank Chief* . Hämtat från Coindesk: https://www.coindesk.com/bitcoin-commodity-not-currency-says-south-korean-central-bank-chief/ den 12 november 2017.

Zimmerman, P. (1 juni 1991). *Why I Wrote PGP*. Hämtat från philzimmermann.com: https://philzimmermann.com/EN/essays/index.html den 2 december 2017.

Svenska författningar

Lag (1845:50 s.1) om handel med lösöre som köparen låter i säljarens vård kvarbliva

Lag (1936:81) om skuldebrev

Lag (1936:88) om pantsättning av lös egendom som innehas av tredje man

Lag (1944:181) om redovisningsmedel

Brottsbalk (1962:700)

Jordabalk (1970:994)

Utsökningsbalk (1981:774)

Konkurslag (1987:672)

Lagen (1988:1385) om Sveriges riksbank

Lag (2008:990) om företagshypotek

EU-rätt

Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (MiFID II)

Rådets direktiv 2006/112/EG av den 28 november 2006 om ett gemensamt system för mervärdesskatt

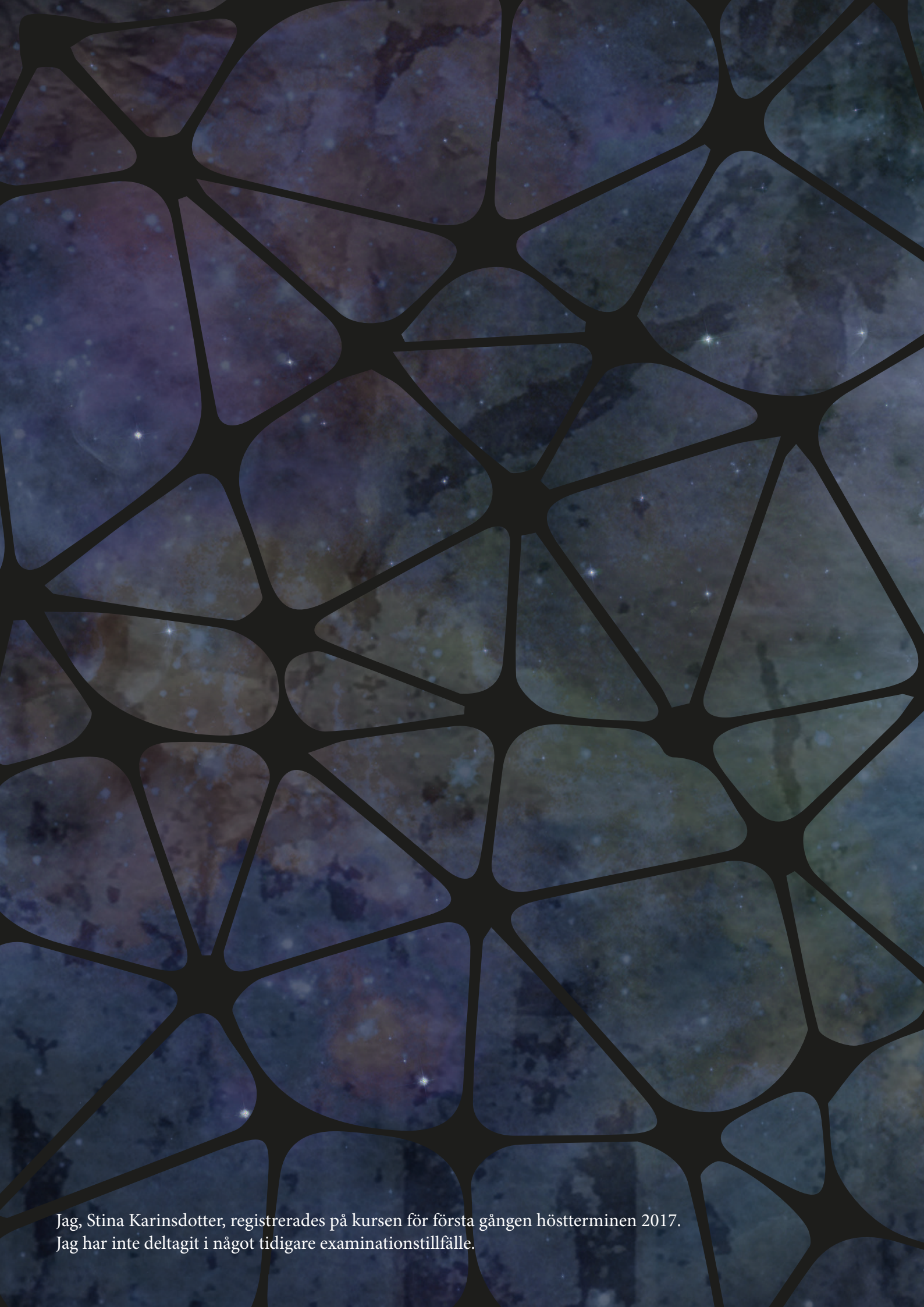
RÄTTSFALLSREGISTER

NJA

NJA 1979 s 591
NJA 1984 s 456
NJA 1984 s 656
NJA 1985 s 159
NJA 1987 s 3
NJA 1988 s 257
NJA 1994 s 480
NJA 1995 s 367
NJA 2007 s 413
NJA 2009 s 182
NJA 2009 s 500
NJA 2011 s 5

EU-domstolen

Mål C-264/14 (Skatteverket v. David Hedqvist)



Jag, Stina Karinsdotter, registrerades på kursen för första gången höstterminen 2017.
Jag har inte deltagit i något tidigare examinationstillfälle.