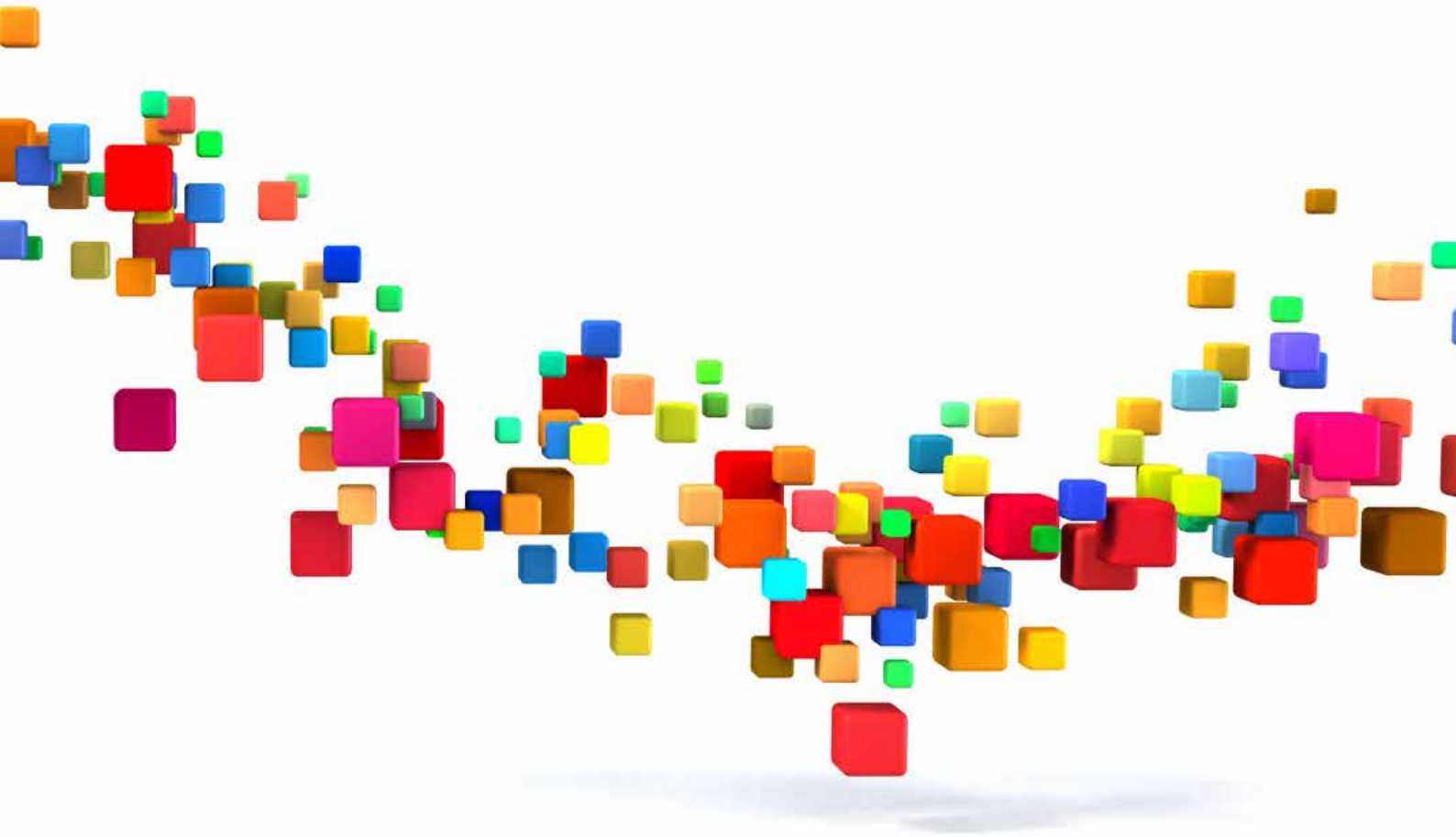


Blockkedjeteknik utifrån ett konkurrensperspektiv

Av Pontus Lindblom på uppdrag av Konkurrensverket

UPPDRAGSFORSKNINGSRAPPORT 2019:4

KONKURRENSVERKET
Swedish Competition Authority

Konkurrensverkets uppdragsforskningsrapport 2019:4
Utredare: Pontus Lindblom
ISSN-nr 1652-8069
Foto: Mostphotos

Förord

I Konkurrensverkets uppdrag ingår att främja forskning på konkurrens- och upphandlingsområdet. Konkurrensverket har därför gett dr Pontus Lindblom i uppdrag att, inom ramen för Konkurrensverkets uppdragsforskning, ge en översikt över blockkedjetekniken och dess tillämpningar samt genomföra en analys utifrån ett konkurrens-, tillsyns- och juridiskt perspektiv.

Blockkedjeteknik möjliggör ett flertal nya applikationer som inte tidigare varit möjliga. Tekniken kan användas som valutor, finansiella instrument och digitala äganderätter men även möjliggöra hantering av certifikat, licenser, digitala nycklar och identitetshandlingar. Blockkedjeteknik kan även möjliggöra för smarta kontrakt som kan användas för skapandet av smart egendom och applikationer för decentraliserad handel, decentraliserade databaser samt potentiellt i framtiden säker elektronisk röstning.

Utifrån ett konkurrens- och tillsynsperspektiv är det viktigt att förstå om blockkedjeteknik kan användas för konkurrenshämmande verksamhet, men också ifall denna teknik skulle kunna underlätta Konkurrensverkets tillsynsarbete. Blockkedjetekniken med dess tillämpningar är dock i ett tidigt utvecklingsstadium vilket gör att eventuella konsekvenser för konkurrensen är svåra att överblicka. Den här rapporten ger en ökad förståelse för nuvarande och framtida användningsområden för blockkedjetekniken och dess eventuella påverkan på konkurrensen.

Till projektet har det knutits en referensgrupp, som haft möjlighet att lämna synpunkter på utkast till slutrapport bestående av Peter Altman (RISE Victoria), Alexander Bottema (The MathWorks), Frida Gustavsson (Handelshögskolan vid Göteborgs universitet) samt Juho Lindman (Göteborgs universitet). Från Konkurrensverket har Björn Axelsson, Arvid Fredenberg, Louise Lundberg, Joakim Wallenklint och Alexander Weidstam deltagit.

Författaren ansvarar själv för alla slutsatser och bedömningar i rapporten.

Stockholm, maj 2019

Rikard Jermsten
Generaldirektör

Innehåll

Sammanfattning

Blockkedjeteknik är en nätverks- och databasstruktur som lanserades med kryptovalutan Bitcoin i januari 2009. Bitcoin bygger på mjukvara med öppen källkod för att skapa ett decentraliserat nätverk med en intern incitamentsstruktur som möjliggör ett säkert, globalt, transparent register som är öppet för alla att använda och som inga enskilda parter kontrollerar. Benämningen blockkedja kommer ifrån att transaktioner och information registreras löpande och irreversibelt i en ständigt växande kedja av kryptografiskt sammanlänkade och tidsstämplade datablock. Incitamentsstrukturen, som är essentiell för systemets funktion, skapas av en intern valuta som används för att utföra transaktioner och registrera information i blockkedjan. Den interna valutan skapas löpande som belöning till dem som väljer att bidra till processen att lägga till nya block med transaktioner till blockkedjan.

Eftersom blockkedjeteknik bygger på mjukvara med öppen källkod så har det växt fram ett ekosystem av hundratals olika system som bygger på Bitcoins ursprung–liga design med mer eller mindre omfattande modifieringar. Dessa system kan grovt indelas i öppna (publika) och stängda (privata) blockkedjor. De publika blockkedjorna är öppna för alla att använda, medan de privata blockkedjorna har skapats för användning inom ett företag, en myndighet eller ett konsortium av företag där tillåtelse från nätverkets skapare eller existerande medlemmar krävs för att delta.

Blockkedjeteknik bygger liksom de flesta uppfinningar på en lång historia av tidigare framsteg. De viktigaste byggstenarna för att möjliggöra blockkedjetekniken har skapats inom utvecklingen av internet, stark kryptering, öppen källkod, peer-to-peer fildelningsteknik och konceptet Proof-of-work . Proof-of-work är den mekanism som används i Bitcoin och de flesta publika blockkedjor för att möjliggöra en decentraliserad konsensus över en gemensam transaktionshistorik i ett publikt, tillståndsfritt, och censurresistent peer-to-peer-nätverk. Privata blockkedjor har inte ett inbyggt incitamentssystem med en intern valuta och Proof-of-work som krävs för att hålla systemet decentraliserat och säkert. Istället används identifierade anförtrodda parter för att uppnå konsensus över en gemensam transaktionshistorik.

Blockkedjeteknik möjliggör ett flertal nya applikationer som inte tidigare varit möjliga. Den interna valutan i decentraliserade publika blockkedjor möjliggör digital knapphet, digitala objekt som inte kan kopieras, men som kan överföras från person till person. Dessa kan användas som valutor, finansiella instrument och digitala äganderätter som kan hanteras utan mellanhänder eller anförtrodda tredjeparter. Blockkedjeteknik kan även möjliggöra permanent verifierbar dokumentering och hantering av certifikat, licenser, identitetshandlingar och digitala nycklar utan mellanhänder eller anförtrodda tredjeparter. Blockkedjeteknik möjliggör även smarta kontrakt som kan användas för skapandet av smart

egendom och applikationer för decentraliserad handel, decentraliserade databaser, samt potentiellt i framtiden säker elektronisk röstning och decentraliserade autonoma organisationer.

Konkurrenslagstiftning finns till för att hindra konkurrenshämmande verksamhet mellan företag och missbruk av en dominerande ställning på marknaden. Från Konkurrensverkets sida är det av intresse att förstå om blockkedjeteknik har potential att användas för att bedriva konkurrenshämmande verksamhet och om det finns risk att enstaka blockkedjor har potential att uppnå en marknadsdominerande ställning där denna ställning kan missbrukas.

Syftet med denna rapport är att ge en introduktion till blockkedjeteknikens framväxt, hur blockkedjetekniken fungerar och dess tillämpningar, samt beskriva blockkedjeteknik ur ett konkurrens-, tillsyns- och regulatoriskt perspektiv. Målgruppen för rapporten är främst personalen på Konkurrensverket, samt politiska beslutsfattare och personer som arbetar med konkurrens och tillsynsfrågor inom offentlig och privat sektor.

Slutsatserna som dras i denna rapport gällande konkurrensaspekter är att blockkedjeteknik är i ett tidigt stadium generellt och merparten av utvecklingen och tillämpningen av tekniken har skett inom publika blockkedjor och kryptovalutor. Publika blockkedjor har potential att förbättra konkurrensen på marknaden genom att ge allmän global tillgång till gemensam digital infrastruktur för ekonomiska transaktioner och hantering av data som inga enskilda parter kontrollerar. Privata blockkedjor, som inte är decentraliserade utan under kontroll av enskilda parter, kan inte erbjuda de unika nya användningsområden som publika decentraliserade blockkedjor möjliggör. Privata blockkedjor, som företag, banker och finansiella institut visat stort intresse för, är ännu på ett tidigt stadium av utveckling och konceptvalidering.

Huvuddelen av farhågorna kring konkurrensbegränsande verksamhet kopplat till blockkedjeteknik rör formerna för samarbeten mellan konkurrerande företag inom konsortier. Risker med konkurrenshämmande samarbeten mellan företag i utveckling och implementering av privata blockkedjor skulle kunna avhjälpas av att konkurrensmyndigheter ges insyn i privata blockkedjor som utvecklas inom konsortier av företag, antingen på frivillig väg eller via lagstiftning. Att tillämpa konkurrenslagstiftningen på konsortier av företag som samarbetar om utveckling och drift av privata blockkedjor på ett otillbörligt sätt borde inte vara mer problematiskt än vid andra former av samarbeten och kanaler för informationsdelning mellan företag. Tvärtom borde användningen av en blockkedja i konkurrenshämmande samarbeten kunna göra det lättare att säkra bevismaterial.

Det har föreslagits att koordinering och informationsutbyte med hjälp av blockkedjor och smarta kontrakt skulle kunna användas av företag för att upprätthålla karteller. Detta ger blockkedjor och smarta kontrakt varken tekniska eller praktiska

förutsättningar för idag och det är osannolikt att förutsättningarna för detta kommer att infinna sig inom överskådlig framtid.

Missbruk av en dominant ställning vore teoretiskt möjligt med en privat blockkedja, eftersom den är under kontroll av enskilda parter som kan missbruka den kontrollen. Men det förutsätter iså fall att en privat blockkedja kan uppnå en dominant ställning för att det konkurrensmässigt sätt skulle kunna bli ett problem. Det är inte möjligt att utöva missbruk av en dominant ställning med en decentraliserad publik blockkedja eftersom den är öppen för alla att använda under lika villkor och inte under någon enskild parts kontroll. Det vore teoretiskt möjligt att utöva missbruk av en dominant ställning med en publik blockkedja som inte är decentraliserad, utan under kontroll av enskilda parter. Men det förutsätter att en sådan blockkedja skulle kunna uppnå en dominant ställning i konkurrens med decentraliserade publika blockkedjor, vilket är osannolikt eftersom en publik blockkedja behöver vara decentraliserad för att kunna ge unika fördelar över en traditionell databas.

Summary

Blockchain technology is a network and database structure that was launched with the cryptocurrency Bitcoin in January 2009. Bitcoin is based on open source software to create a decentralized network with an internal incentive structure that enables a secure, global, transparent ledger, that is open for everyone to use and which no individual parties control. The term blockchain comes from the fact that transactions and information are recorded continuously and irreversibly in a constantly growing chain of cryptographically linked and time stamped data blocks. The incentive structure, which is essential for the functioning of the system, is created by an internal currency, which is used to perform transactions and record information in the blockchain. The internal currency is created continuously as a reward for those who choose to contribute to the process of adding new blocks of transactions to the blockchain.

Because blockchain technology is based on open source software, an ecosystem of hundreds of different systems have been developed based on Bitcoin's original design with more or less extensive modifications. These systems can be roughly divided into open (public) and closed (private) blockchains. The public blockchains are open for anyone to use, while the private blockchains have been created for use within a business, a government agency or consortium of companies, where permission from the network creator or existing members is required to participate.

Blockchain technology, like most inventions, builds on a long history of past progress. The most important building blocks for enabling blockchain technology have been created in the development of the internet, strong encryption, open source, peer-to-peer file sharing technology and the concept of Proof-of-work . Proof-of-work is the mechanism used in Bitcoin and most public blockchains to enable a decentralized consensus on a shared transaction history in a public, permissionless, and censorship-resistant peer-to-peer network. Private blockchains do not have a built-in incentive system with an internal currency and Proof-of-work which is required to keep the system decentralized and secure. Instead, identified trusted parties are used to reach consensus on a shared transaction history.

Blockchain technology enables several new applications that have not been possible previously. The internal currency of decentralized public blockchains enables digital scarcity, digital objects that cannot be copied, but which can be transferred from person to person. These can be used as currencies, financial instruments and digital property rights that can be managed without intermediaries or trusted third parties. Blockchain technology can also enable permanent verifiable documentation and management of certificates, licenses, identity documents and digital keys without intermediaries or trusted third parties. Blockchain technology also enables smart contracts that can be used for the creation of smart property and applications for decentralized trading, decentralized databases, and potentially in the future secure electronic voting and decentralized autonomous organizations.

Competition law exists to prevent anti-competitive activities between companies and abuse of a dominant position on the market. For the Swedish Competition Authority, it is of interest to understand whether blockchain technology has the potential to be used to conduct anti-competitive activities and whether there is a risk that single block chains have the potential to achieve a market-dominant position where this position can be abused.

The purpose of this report is to give an introduction to the development of block-chain technology, explain how blockchain technology works and its applications, and to describe blockchain technology from a competition, oversight and regulatory perspective. The target group for the report is primarily the staff of the Swedish Competition Authority, as well as political decision makers and people who work with competition and oversight issues in the public and private sectors.

The conclusions drawn in this report on competition aspects are that blockchain technology is generally at an early stage, and most of the development and application of the technology has taken place in public blockchains and cryptocurrencies. Public blockchains have the potential to improve competition in the market by providing general global access to a shared digital infrastructure for financial transactions and data management which no individual parties control. Private blockchains, which are not decentralized but under the control of individual parties, cannot offer the unique new use cases that public decentralized block chains can enable. Private blockchains, which companies, banks and financial institutions have shown great interest in, are still at an early stage of development and concept validation.

Most of the concerns about anti-competitive activities linked to blockchain technology concern the forms of collaboration between competing companies within consortia. Risks with anti-competitive collaborations between companies in the development and implementation of private blockchains could be remedied if competition authorities are given insight into private blockchains that are developed within consortia of companies, either voluntarily or through legislation. Applying the competition law to consortia of companies that cooperate on the development and operation of private blockchains should not be more problematic than in other forms of collaboration and channels for information sharing between companies. On the contrary, the use of a blockchain in anticompetitive cooperation should make it easier to secure evidence.

It has been proposed that coordination and information exchange using blockchains and smart contracts could be used by companies to maintain cartels. Blockchains and smart contracts offer neither technical nor practical conditions for this today and it is unlikely that the conditions for this will emerge in the foreseeable future.

Abuse of a dominant position would be theoretically possible with a private blockchain, as it is under the control of individual parties who can abuse that control. But this assumes that a private blockchain can achieve a dominant position in order for this to become a problem. It is not possible to exercise abuse of a dominant position with a decentralized public blockchain since it is open for everyone to use under equal conditions, and not under the control of any single party. It would theoretically be possible to exercise abuse of a dominant position with a public blockchain that is not decentralized, but under the control of individual parties. But this presupposes that such a blockchain could achieve a dominant position in competition with decentralized public blockchains, which is unlikely because a public blockchain needs to be decentralized in order to provide unique advantages over a traditional database.

1 Inledning

Blockkedjeteknik har fått stor uppmärksamhet de senaste åren som tekniken bakom Bitcoin och andra kryptovalutor, men även företag, banker, finansiella institut och myndigheter har visat stort intresse för tekniken i syfte att effektivisera samt öka säkerheten och spårbarheten i datahantering och finansiella transaktioner.

En blockkedja är i vid mening ett transaktionsregister bestående av block med data som länkas samman kryptografiskt i kronologisk ordning och som upprätthålls och uppdateras av användare inom ett nätverk i enlighet med en konsensusmekanism som syftar till att säkerställa att alla användare är överens om en gemensam transaktionshistorik.

Blockkedjeteknik kan göra det möjligt för olika parter att på ett säkert sätt utföra och verifiera transaktioner i ett gemensamt register som finns replikerat hos varje användare av systemet så att samförstånd och tillit kan uppnås utan behov av mellanhänder. Det skulle kunna ge stora effektivitetsvinster jämfört med idag där varje verksamhet registrerar data och ekonomiska transaktioner i egna interna system och där mellanhänder är nödvändiga vid transaktioner.

Blockkedjesystem kan grovt indelas i privata och publika blockkedjor. Privata blockkedjor är stängda och kräver tillstånd för att användas från en centralt ansvarig part medan publika blockkedjor är öppna för alla att använda. Traditionella företag, finansiella institut, centralbanker och myndigheter har främst intresserat sig för privata blockkedjor eftersom de möjliggör mer flexibilitet för anpassning och kontroll, och möjlighet till högre kapacitet och lägre energianvändning än publika blockkedjor.

I denna rapport vill vi belysa syftet och skillnaderna mellan dessa olika typer av blockkedjesystem och hur de jämför sig i ett konkurrens- och tillsynsperspektiv, samt analysera vilka av dessa system som kan ha potential att uppnå marknadsdominerande ställningar och möjlighet för bedrivande av konkurrenshämmande verksamheter.

Bitcoins blockkedja kommer att användas som det primära exemplet i denna rapport för att beskriva hur blockkedjor fungerar. Anledningen till detta är flera, dels att den är originalet, dels att den utgör den hittills mest framgångsrika och renodlade tillämpningen av tekniken och dels att den har den högsta graden av decentralisering och säkerhet.

När nya innovationer växer fram uppkommer ofta en ny terminologi och blockkedjeteknik är inte något undantag. Det mesta av denna terminologi kopplad till blockkedjeteknik har ännu inte nått någon konsensus vad gäller svensk översättning. Den engelska terminologin kommer att användas vid de tillfällen där någon

bra svensk översättning inte finns tillgänglig. I bilaga 1 hittas en ordlista som förklarar begrepp som används i rapporten.

Kunskapen om vad blockkedjeteknik är samt dess användningsområden och begränsningar är generellt låg och det cirkulerar många missuppfattningar gällande blockkedjeteknikens förutsättningar och begränsningar vilket vi vill belysa och redogöra för i denna rapport, för att klargöra hur tekniken kan komma att påverka konkurrens, tillsyns och juridiska frågor.

Denna rapport tar upp blockkedjeteknikens historiska rötter, hur blockkedjetekniken fungerar och dess tillämpningar, samt beskriver blockkedjeteknik ur ett konkurrens-, tillsyns- och regulatoriskt perspektiv.

2 Blockkedjeteknikens framväxt

Blockkedjetekniken beskrevs först i artikeln "Bitcoin: A Peer-to-Peer Electronic Cash System" undertecknad pseudonymen Satoshi Nakamoto i november 2008 (Nakamoto, 2008). Mjukvaruprotokollet som artikeln beskriver startades sedan upp i januari 2009 och är vad som idag är känt som Bitcoin. Det första arbetet på en kryptografiskt säkrad kedja av datablock beskrevs dock redan 1991 av Stuart Haber och W. Scott Stornetta då de ville utveckla en mekanism för säker tidsstämpling av digitala dokument som inte kunde manipuleras (Haber & Stornetta, 1991).

Vad Bitcoin möjliggjorde för första gången var en decentraliserad digital valuta. Ett system för att skapa unika digitala enheter som inte kan kopieras eller dubbelspenderas och som inte behöver någon anförtrodd central part. Då mjukvaran som Bitcoin är skriven i är öppen källkod har hundratals varianter av alternativa blockkedjor med egna interna valutor skapats. Bitcoin är dock i egenskap av att vara först och alla nätverkseffekter som det ger, dominerande i form av marknadsvärde, användarbas, säkerhet, utvecklingsresurser och infrastruktur. Det är ett i högsta grad levande projekt vars källkod och funktioner successivt förbättras och byggs ut.

I denna del beskrivs historien och filosofin bakom Bitcoinblockkedjan och vilka tekniska framsteg som gjorde det möjligt att lansera den i januari 2009. Därefter beskrivs den fortsatta utvecklingen av nya blockkedjor, skillnaden mellan publika och privata blockkedjor, samt fenomenet Initial Coin Offerings.

2.1 Blockkedjans byggstenar

Blockedjetekniken bygger liksom de flesta uppfinningar på en lång historia av tidigare framsteg. De viktigaste byggstenarna för att möjliggöra blockkedjetekniken har skapats inom utvecklingen av internet, stark kryptering, öppen källkod, peer-to-peer fildelningsteknik och konceptet Proof-of-work .

2.1.1 Internet

Internet är ett öppet globalt decentraliserat kommunikationsnätverk. Grunden till Internet började utvecklas på 60-talet i samband med datorernas utveckling (Kleinrock, 2010). Internet är ett nätverk av datorer som kopplas samman genom öppna standardiserade kommunikationsprotokoll. Öppna standardiserade kommunikationsprotokoll är förutsättningen för internets decentraliserade struktur. Några avgörande milstolpar var: Packet-Switching (1961), ASCII (1963), ARPANET (1969), TCP/IP (1982), SMTP (1982), WWW (1989), HTML (1993) och XML (1996).

Kommunikationsprotokoll för överföring av värde, vilket blockkedjetekniken möjliggör, kan ses som en ny viktig del till internets utveckling. Det är ett öppet Internet där datorer i hela världen kan kommunicera med varandra som möjliggör att digitala, decentraliserade blockkedjor kan existera. Decentraliserade system måste byggas på en decentraliserad grundstruktur, vilket internet utgör.

2.1.2 Kryptering

I samband med datorernas och internets utveckling i början av 1970-talet så gick kryptering från att främst användas inom militära organisationer och underrättelseorganisationer till att bli tillgänglig för allmänheten. Det möjliggjorde för privata aktörer att delta i utvecklingen av krypteringstekniken. 1975 skapade och publicerade det privata företaget IBM en symmetrisk krypteringsalgoritm, kallad Data Encryption Standard (DES), som fick global spridning efter att DES utsågs till en officiell krypteringsstandard i USA 1977 (Smid & Branstad, 1988). Vid symmetrisk kryptering används samma nyckel för både kryptering och dekryptering. Det innebär att symmetrisk kryptering kräver att krypteringsnyckeln först överlämnas säkert mellan parterna som sedan vill kunna kommunicera privat.

1976 publicerades konceptet för asymmetrisk kryptering av kryptografiforskarna Whitfield Diffie och Martin Hellman på MIT (Diffie & Hellman, 1976). Deras artikel "New Directions in Cryptography" revolutionerade kryptografin då det med asymmetrisk kryptering blev möjligt att kommunicera krypterat och säkert utan att först behöva utbyta hemliga krypteringsnycklar med varandra. Asymmetrisk kryptering vidareutvecklades sedan och optimerades av kryptografiforskarna Ron Rivest, Adi Shamir, och Leonard Adleman på MIT (Rivest, Shamir, & Adleman, 1978). Deras krypteringsalgoritm, kallad RSA, utgjorde ett effektivt och säkert sätt att generera nyckelpar med hjälp av stora primtal.

1985 gjordes en vidareutveckling av asymmetrisk kryptering där matematik på elliptiska kurvor används för att generera par av kryptonycklar på ett mer effektivt och mindre minneskrävande sätt (Miller, 1986). Det är denna typ av kryptografi som Bitcoin och andra blockkedjor använder sig av för att hantera transaktioner.

Vid asymmetrisk kryptering genereras två matematiskt kopplade kryptonycklar, en publik kryptonyckel som används för att kryptera meddelanden och en privat kryptonyckel som kan dekryptera meddelanden som krypterats med tillhörande publika nyckel. För att skicka ett privat meddelande som endast mottagaren kan öppna så krypteras meddelandet med mottagarens publika nyckel. Det innebär att endast mottagaren som har tillhörande privata nyckel kan dekryptera och läsa meddelandet i klartext.

Då den privata och publika nyckeln är varandras inverser så är det även möjligt att gå andra vägen och detta är principen för att skapa en digital signatur. Ett meddelande som signeras med en avsändares privata nyckel kan verifieras av alla som har tillgång till avsändarens publika nyckel. Detta säkerställer även att meddelandet inte har manipulerats, eftersom en signatur är matematiskt bunden till det meddelande som det ursprungligen gjordes med och minsta lilla modifiering av meddelandet skulle göra att verifieringen av signaturen misslyckas.

2.1.3 Öppen källkod

Utveckling av mjukvara genom öppen källkod tog fart i början på 80-talet. Öppen källkod betyder att instruktionerna för att konstruera ett datorprogram är publikt och fritt att använda, läsa, kopiera, modifiera och vidaredistribuera. Det gör det möjligt för människor att samarbeta fritt och decentraliserat i utvecklingen av mjukvara. Eftersom källkoden är publik kan koden för all öppen mjukvara granskas och det är möjligt för människor att försäkra sig om att mjukvaran gör det som den är tänkt att göra och inte innehåller några säkerhetsbrister eller illvillig kod som syftar till att göra det möjligt att spionera på användaren eller stjäla information.

1983 startades GNU-projektet av programmeraren Richard Stallman på MIT med syfte att bygga ett operativsystem med fri och öppen källkod (Stallman, 1985). Målet med projektet var att skapa ett operativsystem där människor skulle få rätt att studera, ändra och förbättra programmet. Richard Stallman grundade även "Free Software Foundation" (FSF) 1985, vilket är en stiftelse som arbetar för användandet och produktion av fri programvara. Sedan mitten av 1990-talet har FSF även arbetat med juridiska frågor rörande fri och öppen källkod. 1989 publicerade Richard Stallman under FSF:s flagg "GNU General Public License" (GPL), vilket är en upphovsrättslicens för fri programvara. 1991 lanserades operativsystemet Linux av programmeraren Linus Torvalds som anammade principen om fri programvara och öppen källkod (Torvalds, 1991). Linux bygger på en central del från GNU-projektet och en Linuxkärna med öppen källkod som tillsammans utgör ett komplett, fungerande operativsystem. GNU/Linux-projektet var till en början något enskilda entusiaster arbetade med, men numera deltar också ett stort antal globala företag i utvecklingen av projektet.

1998 skapades organisationen "Open Source Initiative" (OSI) som är ett organ för utbildning, förvaltning och förespråkande av öppen källkod. Det gjordes i samband med att företaget bakom Netscape beslutade att släppa källkoden till den populära webbläsaren fri. Initiativtagarna förstod att uppmärksamheten kring Netscape-projektet hade skapat en möjlighet att utbilda och förespråka fördelarna med en öppen utvecklingsprocess för programvara.

2008 lanserades GitHub som blivit världens största plattform för att hantera källkod för öppna mjukvaruprojekt. GitHub är en versionshanteringsplattform som håller reda på varje ändring som görs av källkoden i ett mjukvaruprojekt och vem det är som gör varje ändring. De som äger ett projekt på GitHub bestämmer vilka ändringar som ska tillåtas föras in i deras projekt, men det är fritt och enkelt att kopiera ett redan existerande mjukvaruprojekt och fortsätta utvecklingen åt ett annat håll i en ny förgrening (eng. fork) av det ursprungliga projektet.

Arbetet med att utveckla olika blockkedjor sker mestadels på Github. Det är under kravet om öppen och fri tillgång till källkoden som Bitcoin lanserades och den öppna koden och det publika kollaborativa utvecklingsarbetet är en av grundpelarna till Bitcoins säkerhet och decentralisering.

2.1.4 Peer-to-peer fildelningsteknik

Peer-to-peer fildelningsteknik utvecklades runt milleniumskiftet (Lua m.fl., 2005). Genom implementationer som Napster (1999), Gnutella (2000) och BitTorrent (2001) har den kanske blivit mest känd som ett verktyg för piratkopiering av musik och film. I Peer-to-peer nätverk är alla datorer likvärdiga noder som agerar som både server och klient till de andra datorerna i nätverket. Det möjliggör en decentraliserad organisation för delande av information utan hierarkier.

Peer-to-peer fildelningsteknik är en av de nödvändiga komponenterna för att kunna bygga decentraliserade publika blockkedjor som inte har någon central punkt från vilket systemet kan kontrolleras.

2.1.5 Proof-of-work

Proof-of-work är ett matematiskt bevis som är dyrt och tidskrävande att producera genom att det kräver omfattande beräkningar att framställa, men det är sedan trivialt att verifiera att ett producerat bevis är äkta och ett bevis på att motsvarande mängd resurser har förbrukats. Proof-of-work uppfanns som en mekanism för att förhindra spam av skräppost och som en allmän mekanism för att begränsa åtkomst för delade resurser i datornätverk (Back, 2002; Dwork & Naor, 1993).

I Bitcoin används Proof-of-work för att göra det artificiellt dyrt att lägga till ett nytt block med transaktioner till blockkedjan och därigenom reglera hur den delade databasen kan uppdateras. Samtidigt utgör Proof-of-work en mekanism för att randomisera vem i nätverket som skapar nästa block, reglerar den genomsnittliga tiden mellan blocken, samt ger en objektivt verifierbar punkt för koordination och konsensus över transaktionshistoriken. Proof-of-work är en nödvändig del av Bitcoin för att garantera blockkedjans säkerhet, integritet och decentralisering, vilket i sin tur ger blockkedjan egenskapen att den blir socialt skalbar i betydelsen att ett mycket stort antal människor kan använda den för att utföra transaktioner och organisera sig med minimalt krav på tillit till varandra (Szabo, 2017).

Nick Szabo har utvecklat konceptet “unforgable costliness” (oförfalskbar dyrhet) som en generalisering av Proof-of-work konceptet så som det används i datornätverk (Szabo, 2002, 2005a). Szabo hävdar att detta koncept genom mänsklighetens historia utgjort grunden för mänskliga institutioner och är fundamentalt för den mänskliga civilisationen och för pengar. Genom historien har människor använt pengar i form av samlarföremål (t.ex. sällsynta snäckor), i form av sällsynta råvaror (t.ex. guld och silver), eller idag i form av fiatpengar vars oförfalskbara dyrhet upprätthålls genom att artificiellt begränsa skapandet av nya pengar.

2.2 Blockkedjans filosofiska rötter

Bitcoin och blockkedjetekniken föddes ur Cypherpunkrörelsen, en aktiviströrelse som förespråkar användning av stark krypteringsteknik och integritetsfrämjande teknologier för att möjliggöra personlig integritet i den digitala tidsåldern, i vilken alla våra kommunikationer allt enklare kan övervakas och lagras. Cypherpunks anser att personlig integritet är en grundläggande mänsklig rättighet, inklusive privatliv från myndigheter.

Det var förmodligen till stor del uppfinnaren och kryptografiexperten David Chaums tidiga och omfattande arbete med kryptografiska protokoll och arbete med att skapa ett system för anonyma digitala pengar under det tidiga 80-talet som lade grunden till Cypherpunkrörelsen. Chaums avhandling "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" från University of California, Berkley 1981, har även lagt grunden till dagens forskning om anonymitet vid kommunikation på Internet (Chaum, 1981). 1982 utvecklade han Ecash, ett emittentbaserat system för anonyma digitala pengar, som han lanserade via sitt företag Digicash (Chaum, 1983). 1985 publicerade han “Security Without Identification: Transaction Systems to Make Big Brother Obsolete” där han ingående beskriver farorna med ett massövervakningssamhälle som möjliggörs med digital teknik och centrala hierarkiska organisationer, samt hur den utvecklingen kan motverkas genom krypterad anonym kommunikation, digitala signaturer och anonyma digitala kontanter (Chaum, 1985).

1988 publicerade ingenjören och seniora datavetaren på företaget Intel, Timothy C. May manifestet "The Crypto Anarchist Manifesto" som först definierade grunderna till Cypherpunkrörelsen (May, 1988). I manifestet presenterade May fundamenten för kryptoanarkism, vilket innefattar krypterade digitala transaktioner med fullständig anonymitet, yttrandefrihet och fri handel.

Den officiella delen av Cypherpunkrörelsen grundades av Timothy C. May tillsammans med programmerings- och kryptografiexperterna, Eric Hughes och John Gilmore hösten 1992 (Levy m.fl., 1993). De bildade en liten grupp av integritets- och kryptografi-intresserade individer som träffades en gång per månad på John Gilmores San Francisco Bay Area-baserade företag Cygnus Solutions för att disku-

tera utvecklingen och farorna med ett framväxande övervakningssamhälle. Gruppen breddades senare genom att en mailinglista (The Cypherpunk electronic mailing list) skapades där alla som var intresserade av att bygga verktyg för att främja personlig integritet kunde delta och diskutera.

Ett grundläggande motto för Cypherpunkrörelsen är "Cypherpunks write code" som myntades av Eric Hughes i "A Cypherpunk's Manifesto" som han publicerade några månader efter att rörelsen bildats (Hughes, 1993). Det betyder att Cypherpunks primära uppgift anses vara att skapa mjukvara för kryptering och försvar av personlig integritet. I manifestet påtalades även vikten av att sprida mjukvaran och källkoden öppet så att andra cypherpunks har möjlighet att lära av den, attackera den och förbättra den.

Bland framträdande medlemmar i Cypherpunk rörelsen kan nämnas Philip Zimmermann som 1991 utvecklade krypteringsprotokollet PGP (Zimmermann, 1991), Bram Cohen som 2001 skapade fildelningsprotokollet BitTorrent, Jacob Appelbaum som 2002 utvecklade anonymiseringsnätverket Tor, Julian Assange som 2006 grundade Wikileaks och Moxie Marlinspike som 2014 lanserade den krypterade chattappen Signal.

Cypherpunkrörelsen har under årens lopp utvecklat flera försök till att skapa digitala anonyma valutor. 1997 utvecklade Adam Back Hascash som en mekanism för att förhindra spam av skräppost (Back, 2002). Hashcash bygger på konceptet Proof-of-work som är en central byggsten i Bitcoin och flera andra kryptovalutor. 1998 föreslog Wei Dai b-pmoney, ett protokoll för ett distribuerat kryptovalutasystem där den monetära basen produceras via Proof-of-work i ett auktionssystem, och där transaktionshistoriken innehas av alla deltagare som ett offentligt register (Dai, 1998). 1998 utvecklade även Nick Szabo ett koncept han kallade Bit gold för skapandet av en kryptovaluta där mynten skapades genom Proof-of-work i en tidsstämplad kedja och registrerades i ett offentligt register (Szabo, 2005b). Bit gold implementerades aldrig men kan på många sätt ses som en direkt föregångare till Bitcoin. Ytterligare en design av kryptovaluta publicerades inom Cypherpunkrörelsen av Hal Finney 2004 som använde mynt skapade genom Proof-of-work men där en central server behövdes för att förhindra att samma mynt spenderades mer än en gång (Finney, 2004).

Alla dessa tidigare försök till att skapa anonyma digitala valutor gav viktiga pusselbitar till att skapa en decentraliserad, digital kryptovaluta, men det skulle dröja ytterligare ett antal år innan alla pusselbitarna var på plats.

I november 2008 mitt under den stora finanskrisen publicerades artikeln "Bitcoin: A Peer-to-Peer Electronic Cash System" undertecknad pseudonymen "Satoshi Nakamoto" (Nakamoto, 2008). Den anonyme skaparen (eller skaparna) av Bitcoin blev först med att hitta en lösning för hur dubbelspendering kan undvikas i ett decentraliserat elektroniskt betalningsnätverk. Ett problem som fram tills dess gjort det omöjligt att skapa en elektronisk valuta utan en central anförtrodd tredjepart som verifierar att de digitala mynten inte kopieras och används flera gånger.

I Bitcoins whitepaper adresserar Satoshi bland annat problemet med att det nuvarande finansiella systemet kräver användandet av anförtrodda tredjeparter som mellanhänder i ekonomiska transaktioner, och i det första blocket i Bitcoins blockkedja präntade Satoshi in en dagsaktuell referens från London-baserade tidningen The Times, och vad som kan tolkas som en kritik av det rådande ekonomiska systemet "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

2.3 Hur nya blockkedjor skapas

Det går att programmera nya blockkedjor från grunden utifrån de allmänna principer som Bitcoin demonstrerade men det vanligaste sättet att skapa en ny blockkedja och kryptovaluta har varit att kopiera Bitcoins öppna källkod och därefter göra modifieringar och lansera den som en ny kryptovaluta.

Den första nya blockkedjan som lanserades efter det att Bitcoin skapades och aktiverades i januari 2009 var Namecoin. Namecoin skapades i april 2011 och denna blockkedja var en kopia av Bitcoins öppna källkod där sedan extra funktionalitet lagts till för att Namecoin skulle kunna fungera som ett decentraliserat register för domännamn på på internet. Namecoin skapades för att erbjuda ett decentraliserat och ocensurerbart alternativ till det domännamnsystem som används på internet, vilket administreras av "Internet Corporation for Assigned Names and Numbers" (ICANN), en icke vinstdrivande organisation baserad i Kalifornien.

Från 2011 och framåt har ett stort antal nya blockkedjor och kryptovalutor skapats, där de flesta bygger på förgreningar av Bitcoins öppna källkod, men där vissa även utvecklats från grunden med ny kod. 2013 fanns ett tiotal kryptovalutor listade på webbsidan Coinmarketcap, i februari 2019 fanns där över 2000.[1]

Det är även möjligt att skapa en ny kryptovaluta genom att göra en avsiktlig eller oavsiktlig förgrening av en befintlig blockkedja genom en så kallad hard fork (Se Kapitel 3.5.2). Vid en hard fork skapas en ny kryptovaluta som delar blockkedja och transaktionshistorik bakåt i tiden med den ursprungliga blockkedjan men inte framåt. En hard fork initieras genom att en andel av noderna i nätverket bestämmer sig för att köra en ny version av blockkedjeprotokollet som uppdaterats på ett sådant sätt att det inte är bakåtkompatibelt med de andra noderna i nätverket. Ett exempel på det skedde på Ethereums blockkedja där Ethereum Classic skapades i juli 2016 genom att en majoritet av noder i Ethereums nätverk uppdaterade till en icke-bakåtkompatibel version av Ethereums blockkedjeprotokoll. I augusti 2017 skapades även den nya kryptovalutan Bitcoin Cash på detta sätt som en avknoppning från Bitcoins blockkedja.

[1] https://coinmarketcap.com/historical/

2.4 Publika och privata blockkedjor

Syftet med Bitcoin var att skapa en decentraliserad, öppen, digital valuta som inga enskilda parter kan kontrollera eller manipulera. Publika blockkedjor är helt öppna för alla att delta i utan att fråga någon om lov. Det enda som behövs är en dator och en internetuppkoppling för att delta som en nod i nätverket och kommunicera med övriga noder, för att utföra transaktioner, upprätthålla en synkroniserad kopia av den gemensamma transaktionshistoriken, hjälpa till att upprätthålla protokollets konsensusregler och validera transaktioner. Vem som helst kan använda öppna blockkedjor för att utföra transaktioner och läsa av transaktionshistoriken.

Istället för att behöva använda en anförtrodd central part för att förhindra dubbelspendering så använder Bitcoin Proof-of-work för att verifiera transaktioner. Proof-of-work möjliggör decentraliserat konsensus över en gemensam transaktionshistorik i ett publikt, tillståndsfritt, och censurresistent peer-to-peer-nätverk (Poelstra, 2015).

Den grundläggande datastrukturen hos blockkedjor med block av data som länkas samman kryptografiskt i kronologisk ordning, men utan inbyggt incitamentssystem med Proof-of-work och en intern valuta för att hålla systemet decentraliserat och säkert, kan potentiellt även användas för att ge ökad dataintegritet och transparens för data som delas mellan betrodda parter i interna nätverk.

Privata blockkedjor är blockkedjor som skapats för användning inom ett företag, en myndighet, eller ett konsortium av företag där tillåtelse från nätverkets skapare eller existerande medlemmar krävs för att delta (Jayachandran, 2017). Privata blockkedjor kan utgöra ett alternativ till traditionella replikerade databaser när samarbetspartners och konkurrenter behöver samarbeta med en gemensam transaktionsinfrastruktur. Privata blockkedjor möjliggör mer flexibilitet för anpassning och kontroll, och möjlighet till högre kapacitet och lägre energianvändning än de publika blockkedjorna och privata blockkedjor kan byggas så att olika deltagare kan ges olika befogenhet att skriva och läsa data i blockkedjan.

Med privata blockkedjor är det, till skillnad från publika blockkedjor, möjligt för enskilda organisationer eller ett konsortium av företag att upprätthålla kontroll över driften av nätverket, vilket kan vara ett krav i reglerade finansiella marknader för att möjliggöra en tydlig roll och ansvarsfördelning (Lemieux, 2016).

Banker och finansiella institut har visat stort intresse för privata blockkedjor som ett system för effektivare transaktioner och registreringar av finansiella avtal, samt utfärdande och hantering av digitala tillgångar och finansiella instrument. Ett annat område där en privat blockkedja kan vara ett alternativ som företag visat intresse för är att spåra varor i en logistik- eller värdekedja som kan innefatta flera mellanhänder och olika företag.

Hyperledger är en paraplyorganisation som startades 2016 av "The Linux Foundation" för utveckling av privata blockkedjor och distribuerad databasteknik med öppen källkod för tillämpningar inom företag och organisationer. Vid starten ingick 30 medlemmar vilket inkluderade flera stora teknikföretag (IBM, Intel, Fujitsu, Hitachi m.fl.), finansiella institut (J.P. Morgan, CME Group, Deutsche Börse Group, Wells Fargo, SWIFT m.fl.) och blockkedjeföretag (Blockchain, Digital Asset Holdings, Guardtime, R3, Symbiont m.fl.). Sedan dess har antalet medlemsföretag utökats till över 200.

De två första blockkedjeprojekten som blev inkluderade i Hyperledger var "Fabric" som utvecklats av IBM och Digital Asset Holdings, samt "Sawtooth" som utvecklats av Intel. Därefter har ett antal ytterliggare blockkedjeprojekt och verktyg för blockkedjor inkluderats i Hyperledger. Blockkedjan Hyperledger Fabric har stöd för privata kanaler för att göra konfidentiella transaktioner mellan parter på blockkedjan och ett av de andra blockkedjeprojekten, "Hyperledger Indy" är särskilt byggt för att hantera identiteter och är byggt för att vara kompatibelt med dataskyddsförordningen (GDPR).

Hyperledger Fabric har använts av bland annat Walmart i ett pilotprojekt med IBM för att spåra ursprung och hantering av olika livsmedelsprodukter i ett projekt kallat "IBM Food Trust". Detta är ett exempel på "Blockchain as a service" där den privata blockkedjan körs på IBM:s molntjänst och verifierade användare registrerar data i blockkedjan och läser av data via en vanlig webbläsare. Varje användare har inte en egen kopia av blockkedjan och de deltar inte i valideringen av transaktioner eller konsensusmekanismen för blockkedjan. IBM har även bildat ett joint venture företag tillsammans med Maersk, som är världens största rederi, för att digitalisera och effektivisera spårbarhet och hantering av distributionskedjor för containerfrakt i ett system kallat TradeLens baserat på Hyperledger Fabric. Målet med TradeLens är att skapa en plattform byggd på öppna standarder som kan användas av hela det globala ekosystemet som är involverat i containerfrakt. Men intresset har varit svalt från andra rederier att ansluta sig till TradeLens och fem av Maersk's största konkurrenter (CMA CGM, Cosco, Evergreen Marine, OOCL och Yang Ming) har bildat ett konsortium för att gemensamt ta fram en konkurrerande öppen standard baserad på blockkedjeteknik, kallad Global Shipping Business Network (GSBN).

Företaget R3 har fått mycket uppmärksamhet för deras blockkedjekonsortium för banker och finansiella institut som utvecklat den blockkedje-inspirerade plattformen Corda. Men när Corda lanserades i april 2016 skrev R3:s "Chief Technology Officer" Richard Gendal Brown om varför de valt att inte bygga en blockkedja och vad skillnaden mellan Corda och en blockkedja är (Brown, 2016). Corda är byggd för att hantera finansiella avtal mellan banker och finansiella institut. Varje avtal registreras i systemet så att det endast är de ingående parterna som registrerar informationen och regulatoriska myndigheter kan enkelt ges insyn. All data sparas inte i en global databas som i en blockkedja och konsensus uppnås på nivån av varje enskild överenskommelse mellan parterna, inte på nivån av systemet som

helhet. Med denna design delas ingen potentiellt känslig information med utomstående tredjeparter. R3 leder ett konsortium med över 200 finansiella institut, banker, branschorganisationer och fintech-företag.

Privata blockkedjors säkerhet behöver liksom traditionella, centraliserade och delade databaser baseras på att kontrollera vilka som har åtkomst till dem, vilket innebär sårbarhet både från attacker från insiders och yttre hackare. En stor fördel med publika blockkedjor är att dess säkerhet inte är baserad på åtkomstkontroll. Det gör också att nya applikationer kan byggas på publika blockkedjor utan att behöva fråga någon om lov.

Publika blockkedjor som finns tillgängliga för alla via internet, måste för att överleva växa sig starkare och mer motståndskraftiga med tiden, då de konstant är utsatta för olika attackvektorer som protokollet behöver uppdateras för att kunna stå emot. Det finns många exempel på publika blockkedjor som på grund av bristande säkerhet, för få användare och bristande decentralisering dukat under. Privata blockkedjor utsätts inte för samma evolutionära tryck eftersom de hålls i en skyddad nätverksmiljö där endast betrodda identifierade användare är tänkta att interagera med blockkedjan.

Publika blockkedjor kan liknas vid öppna nätverk av typen "internet" som vem som helst kan använda och ansluta sig till, och privata blockkedjor kan liknas vid slutna nätverk av typen "intranet" med en sluten grupp av användare för interna syften, exempelvis inom ett företag, en myndighet eller branschorganisation. Se Tabell 1 för en översikt av typiska skillnader mellan publika och privata blockkedjor.

Tabell 1 Typiska skillnader mellan publika och privata blockkedjor

	Publik blockkedja	**Privat blockkedja**
Åtkomst	Öppen, tillståndsfri	Stängd, kräver tillstånd
Kapacitet	Låg, begränsad	Hög, flexibel
Säkerhet	Proof-of-work /Proof-of-Stake	Åtkomstkontroll
Identitet	Anonym, pseudonym	Identifierade deltagare
Energiförbrukning	Hög*	Låg
Validering	Decentraliserad	Anförtrodda parter

*för Proof-of-work

2.5 Initial Coin Offerings

En Initial Coin Offering (ICO) är en finansieringsmodell som baseras på skapandet av en ny kryptovaluta för att få in investeringar till ett projekt (Li & Mann, 2018). I en ICO säljs en andel av alla mynt (eng. tokens) i en nyskapad kryptovaluta till spekulanter och investerare för annan kryptovaluta och ibland även fiatvaluta. Det kan ske som en öppen crowdfunding där alla som vill kan delta eller till en sluten grupp av privata investerare, eller en kombination av de båda i flera steg.

Mastercoin var det första projektet som lanserades genom en ICO i juli 2013 och projektet fick in ca 5000 bitcoin vilket då motsvarade ca 500 000 dollar. I juli 2014 lanserades Ethereum genom en ICO där skaparna av Ethereum fick in ca 31 000 bitcoin till ett värde av ca 18 miljoner dollar.

Syftet med en ICO är att få in pengar för att utveckla en ny form av blockkedja eller plattform där oftast användningen av den när den väl är utvecklad, enbart ska kunna ske genom den nyskapade kryptovalutan. Tanken är att de funktioner som blockkedjan eller plattformen erbjuder när den väl är lanserad ska ge en efterfrågan på dess interna valuta så att värdet av valutan stiger.

I slutet av 2015 lanserades en standard kallad ERC-20 för att lansera nya kryptovalutor i form av smarta kontrakt på blockkedjan Ethereum. Detta har bidragit till att mängden ICO:s ökat lavinartat då det har gjort det väldigt enkelt att skapa en ny valuta för denna typ av crowdfunding. Enligt statistisk sammanställt av Coindesk genomfördes 343 ICO:s år 2017 som finansierades med sammanlagt 5 482 miljoner dollar och 2018 hade denna siffra ökat till 650 genomförda ICO:s som sammanlagt finansierades med 16 718 miljoner dollar.[2]

Att lansera en ICO har varit ett populärt sätt för nystartade företag och organisationer inom kryptovaluta- och blockkedje-ekosystemet att få in kapital utan att behöva gå genom traditionella kanaler av riskkapitalister, banker och börser. Det har även använts som ett sätt att kringgå regleringar kring hur företag kan ta in kapital från investerare (Zetzsche m.fl., 2018). I vissa prospekt framhålls det för potentiella investerare att köp av den nya kryptovalutan inte kommer med några garantier eller rättigheter för köparen och att mynten inte ska ses som en investering eller någon form av valuta eller värdepapper. En studie publicerad i maj 2018 visade att endast 44% av företagen som finansierar sig via en ICO överlever i mer än 4 månader (Benedetti & Kostovetsky, 2018).

[2] https://www.coindesk.com/ico-tracker

Den rättsliga ställningen för ICO:s är fortfarande oklar inom de flesta länder inklusive Sverige och andra EU-länder. I ett examensarbete från juridiska fakulteten på Uppsala universitet 2018 undersöks den legala statusen för ICO:s i svensk rätt (Sadeghi Gazani, 2018). Slutsatsen är att ICO-mynt kan utgöra värdepapper i den allmänna meningen att de utgör en handling vars ägande eller innehav medför eller utgör ett bevis för en rätt till prestation av egendom eller tjänst, eller kan användas som betalningsmedel för vissa bestämda varor eller ändamål. Dock passar ICO:s inte in på definitionen av ett finansiellt instrument eller någon definierad typ av värdepapper enligt rådande lagstiftning i form av värdepappermarknadslagen (2007:528) eller direktiv 2014/65/EU om marknader för finansiella instrument.

I USA har U.S. Securities and Exchange Commission (SEC), som utövar tillsyn över handel med värdepapper, uttalat sig att alla ICO-mynt definieras som värdepapper förutsatt att de uppfyller kriterierna i Howey-testet, vilket specificerar att det ska röra sig om en investering av pengar i ett gemensamt företag med en rimlig förväntan på vinst härledd ur andras arbete.

En distinktion som kan göras är den mellan security tokens och utility tokens. Security tokens är att betrakta som ett värdepapper enligt SEC och Howey-testet, medans utility tokens är mer att betrakta som en kupong som kan bytas mot en bestämd vara eller tjänst. SEC menar att alla ICO:s som de undersökt har varit säljande av security tokens trots att de ofta marknadsfört sig som utility tokens. För att klargöra vad som gäller har SEC sammanställt en guide för att informera om ICO:s. SEC har även tagit fram riktlinjer för hur en laglig ICO kan genomföras i form av vad de kallar en Security Token Offering (STO) (Bevilacqua, Levites, & Rahmati, 2018).

3 Hur blockkedjeteknik fungerar

Bitcoins blockkedja kommer att användas i detta kapitel för att förklara grunderna för hur blockkedjor fungerar. Anledningen till detta är flera, dels att den är originalet, dels att den utgör den hittills mest framgångsrika och renodlade tillämpningen av tekniken och dels att den har den högsta graden av decentralisering och säkerhet.

Publika blockkedjor bygger på mjukvara med öppen källkod för att skapa ett decentraliserat nätverk med en intern incitamentsstruktur som möjliggör ett säkert, globalt, transparent register som är öppet för alla att använda och som ingen styr över. I detta speciella register, kallat en blockkedja kan transaktioner och information registreras irreversibelt i en ständigt växande kedja av tidsstämplade transaktionsblock. Incitamentsstrukturen för att hålla transaktionshistoriken säker och nätverket decentraliserat skapas av en intern valuta som används för att utföra transaktioner och registrera information i registret och som skapas löpande som belöning till dem som väljer att bidra till processen att lägga till nya block med transaktioner till blockkedjan.

Privata blockkedjor har inte ett inbyggt incitamentssystem med en intern valuta och Proof-of-work som krävs för att hålla systemet decentraliserat och säkert. Istället används identifierade anförtrodda parter för att uppnå konsensus. I privata blockkedjor är vanligtvis inte heller alla användare likvärdiga deltagare med samma befogenheter att skriva och läsa data i blockkedjan.

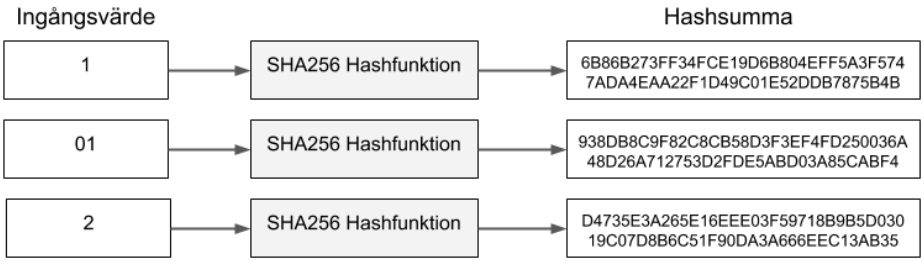
3.1 Blockkedjans struktur

En blockkedja är ett gemensamt register som delas av alla deltagare i ett nätverk som kör mjukvaran för ett kompatibelt blockkedjeprotokoll. En fullständig kopia av en blockkedja innehåller varje transaktion som någonsin utförts och med denna information går det att se exempelvis hur många enheter av blockkedjans interna valuta som tillhört varje adress vid varje tidpunkt i historien.

För att alla ska vara överens om en gemensam historia över alla transaktioner så låses de kryptografiskt i en kronologisk kedja av transaktionsblock genom en process som kallas ”mining” och som i Bitcoins blockkedja är baserad på Proof-of-work . Med Proof-of-work menas att en viss mängd arbete i form av beräkningar behöver utföras i genomsnitt för att lägga till ett nytt block med transaktioner till blockkedjan. Enligt protokollets regler så är det alltid den blockkedja som genererats genom mest Proof-of-work som gäller som ett majoritetsbeslut för den aktuella transaktionshistoriken, vilket ger en objektivt verifierbar mekanism för koordination och konsensus.

För att förstå hur blockkedjan fungerar krävs förståelse för hashfunktioner. En matematisk hashfunktion har egenskapen att när ett ingångsvärde matas in i funktionen så matas det alltid ut ett utgångsvärde av en fix längd. En kryptografisk hashfunktion har dessutom egenskapen att den är irreversibel. Det innebär att det är praktiskt omöjligt att reversera funktionen, det vill säga att räkna ut vilket värde som matades in i funktionen baserat på värdet som fås ut. Det enda sättet att få fram vilket värde som matats in i en kryptografisk hashfunktion baserat på dess utgångsvärde (hashsumman) är att prova alla möjliga ingångsvärden tills det värde hittas som producerar rätt hashsumma. Principen illustreras i Figur 1.

Figur 1 Principen för en kryptografisk hashfunktion



Förenklat exempel:

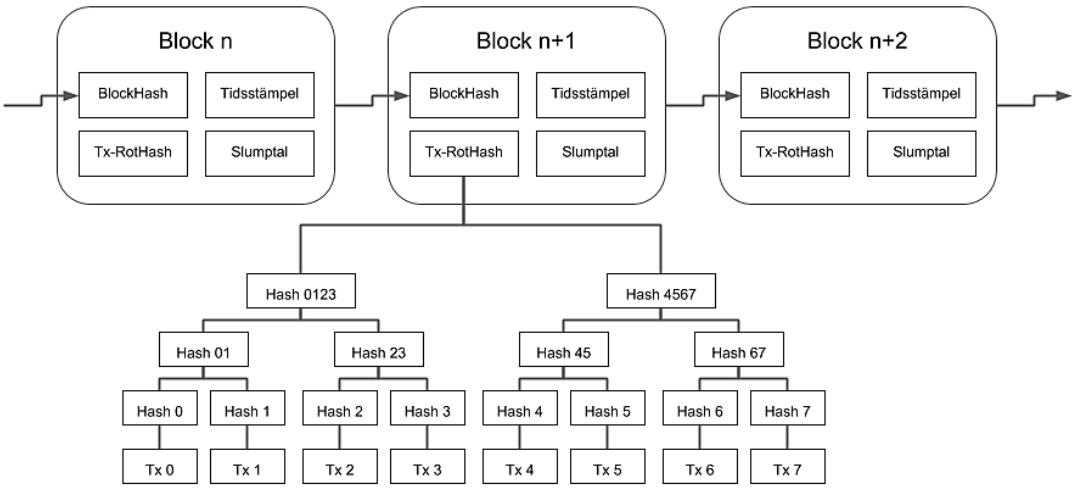
F(**?**) = 365 - Vilket ingångsvärde till funktionen ger hashsumman 365?

F(**5**) = 43 - fel gissning, försök igen...
F(**6**) = 300 - fel gissning, försök igen...
F(**7**) = 67 - fel gissning, försök igen...
...
…

För en stark kryptografisk hashfunktion bör det ta längre tid än universums livslängd att prova sig fram till rätt ingångsvärde. Hashsumman kan därmed fungera som ett digitalt fingeravtryck som kan användas som unik verifiering av det värde som matats in.

Genom mining processen försöker alla miners i Bitcoin-nätverket kontinuerligt att packa ihop alla nya transaktioner som sker i block. Transaktionerna i varje block hashas ihop i en trädstruktur (Merkle-träd) till en transaktions-rothash, vilket är ett sätt att skapa en effektiv och säker verifiering av innehållet i stora datastrukturer, namngivet efter dess uppfinnare Ralph Merkle (Merkle, 1988). Varje block innehåller dessutom en tidsstämpel, ett slumptal och en hash av all data i det föregående blocket (Figur 2).

Figur 2 Blockkedjans struktur



All dessa data för ett föreslaget nytt block matar miners in i en kryptografisk hash-funktion (i Bitcoin används den kryptografiska hashfunktionen SHA-256) och om resultatet understiger ett bestämt gränsvärde (kallat svårighetsgraden) så läggs blocket till blockkedjan som ett giltigt block. Om resultatet överstiger gränsvärdet som avgör svårighetsgraden får miners prova nya val av slumptalet, eller ändra andra variabla ingångsvärden för det föreslagna blocket, tills de hittar en godkänd lösning. Svårigheten sätts automatiskt så att all datorkraft som miners bidrar med till nätverket i snitt lyckas lösa ett nytt block var 10:e minut. Vilken enskild miner som lyckas lösa ett block styrs av slumpen, men miners med större andel av den totala beräkningskraften i nätverket har en större chans att hitta lösningen för ett block. Detta kan liknas med ett lotteri där chansen att vinna ökar med andelen av lotter som innehas. Dock är det fortfarande slumpen som styr så vidare en individ inte köpt upp samtliga lotter.

Genom att låta slumpen avgöra vem i nätverket som kommer att verifiera nästa block med transaktioner så gör det att ingen enskild part kan kontrollera vilka transaktioner som registreras. Detta innebär att ett robust, decentraliserat konsensus kan uppnås och ingen kan censurera transaktioner i nätverket eller manipulera blockkedjans transaktionshistorik så länge majoriteten av all beräkningskraft inte försöker attackera nätverket (Garay & Kiayias, 2014; Miller & LaViola, 2014). Om en enskild aktör har över 50% av beräkningskraften i nätverket så kan de reversera transaktioner som de själva skickar, hindra alla eller ett urval av andras transaktioner från att bekräftas och hindra andra miningaktörer från att generera block som kommer med i den giltiga kedjan (med mest Proof-of-work), men de kan inte stjäla andras pengar eller ändra reglerna för protokollet.

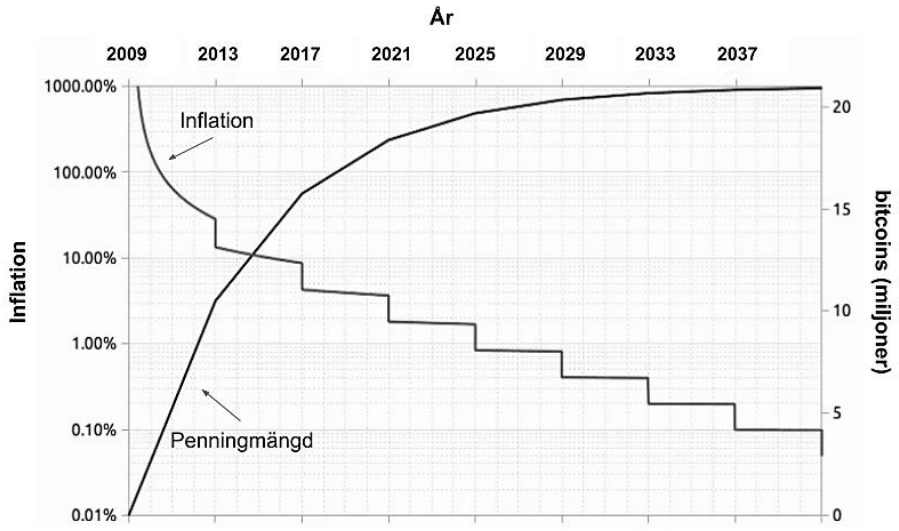
Genom att varje block i blockkedjan refererar till det tidigare blocket på ett sätt som unikt identifierar det tidigare blocket så kopplas alla blocken ihop i en ständigt växande ihoplänkad kedja som går tillbaka till det första blocket.

Den miner som lyckas hitta Proof-of-work lösningen till ett block belönas med ett visst antal nyskapade enheter av den interna valutan (bitcoin) samt även transaktionsavgifter. Dessa utgör de ekonomiska incitamenten för att miners ska vara villiga att spendera beräkningskraft för att verifiera nya transaktioner och säkra transaktionshistoriken.

De nya enheterna av den interna valutan som skapas med varje nytt block utgör mekanismen för att över tid distribuera den monetära basen i systemet utan någon central utgivare. Den monetära basen skapas och fördelas över tid som belöning till miners i förhållande till hur stor andel beräkningskraft som de bidrar med under fri, global konkurrens utan några artificiella hinder för nya aktörer.

Alla i dagsläget existerande enheter av den interna valutan har skapats som belöning till miners för beräknade lösningar till transaktionsblock i blockkedjan. I Bitcoinblockkedjan var belöningen 50 bitcoin per block från början, men vart 210 000:e block (ca vart fjärde år) halveras belöningen. Ökningstakten (inflationen) av bitcoin var därmed hög i början men halveras vart fjärde år och totala antalet bitcoin kommer inte att överstiga 21 miljoner (Figur 3). Varje bitcoin är i sin tur delbar i 100 miljoner delar, där den minsta enheten 0,00000001 bitcoin kallas 1 Satoshi.

Figur 3 Bitcoins penningpolitik



Bitcoins design möjliggjorde för första gången digital knapphet (eng. digital scarcity). Googles tidigare verkställande direktör Eric Schmidt har beskrivit detta i följande ordalag:

> *"Bitcoin is a remarkable crypto-graphic achievement and the ability to create something which is not 'duplicable' in the digital world has enormous value. It's very hard to do and it's incredibly useful for many computer applications. The Bitcoin architecture, literally the ability to having these ledgers that can't be replicated is an amazing advancement. A lot of businesses will be built on top of that."*

Antalet transaktioner som kan få plats i ett block är begränsat genom att varje transaktion kräver att en viss mängd data lagras. Storleken på blocken är begränsad för att inte blockkedjan ska växa sig så stor att det blir för kostsamt för vanliga användare att köra en fristående nod i nätverket, vilket skulle kompromissa decentralisering och säkerhet.

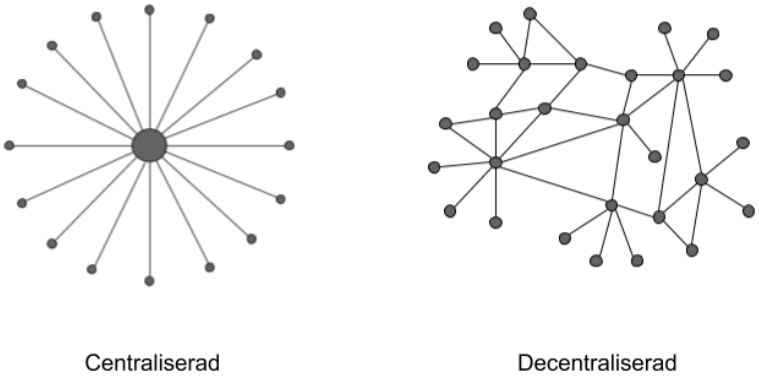
Ett nytt block i Bitcoin skapas var tionde minut i snitt och om det görs fler transaktioner än vad det finns utrymme för i ett block så är det den frivilligt inkluderade transaktionsavgiften som avgör om transaktionen inkluderas i nästkommande block. Miners har som incitament att välja de transaktioner som inkluderar högst transaktionsavgift i första hand eftersom de tilldelas transaktionsavgifterna för alla transaktioner i block som de lyckas lösa. Vid fulla block uppstår det därmed en fri marknad där de transaktioner som inkluderat en tillräckligt hög transaktionsavgift ges högst prioritet. Om en transaktion med för låg transaktionsavgift skickas kan den ersättas med en högre transaktionsavgift så att den registreras i ett block inom önskat tidsintervall.

3.2 Nätverkets struktur

En blockkedjas nätverk utgörs av alla noder som kör ett kompatibelt protokoll som följer samma regler. Nya noder kan i publika blockkedjor ansluta sig till nätverket genom att ansluta till ett slumpmässigt urval av andra noder. Denna mekanism etablerar ett tätt sammankopplat randomiserat nätverk där meddelanden snabbt sprids till alla noder (Decker & Wattenhofer, 2013; Karp m.fl., 2000).

Alla noder i Bitcoins nätverk och i nätverken för de flesta publika blockkedjor utgör likvärdiga parter till varandra och ingen nod har större befogenheter eller makt än någon annan. Nätverket av sammankopplade noder utgör en decentraliserad platt organisation utan hierarkier, där noder skickar meddelanden och vidarebefordrar meddelanden till alla andra noder som de är anslutna till (Figur 4).

Figur 4 Decentraliserad nätverksstruktur utan hierarkier (till höger)



Noder behöver inte vara identifierade eftersom meddelanden inte skickas till någon särskild plats utan endast levereras efter bästa förmåga. Noder kan lämna och återansluta till nätverket som de vill och acceptera den blockkedja med mest Proof-of-work som bevis på vad som hänt medans de varit bortkopplade.

Denna decentraliserade platta organisation av deltagare utan hierarkier i nätverket gäller vanligtvis inte i privata blockkedjor där olika deltagare kan ges olika uppgifter och befogenheter.

3.3 Konsensusalgoritmens funktion

Proof-of-work möjliggör decentraliserat konsensus (Poelstra, 2015). Ett decentraliserat konsensus är ett globalt samförstånd mellan många ömsesidigt misstroende parter som inte litar på varandra och som inte behöver ha varit närvarande när systemet skapades.

Den anonyme skaparen (eller skaparna) av Bitcoin var först med att hitta en lösning för hur dubbelspendering (dvs. att samma elektroniska mynt kan spenderas flera gånger) kan undvikas i ett decentraliserat elektroniskt betalningsnätverk där inga parter behöver lita på varandra. Bitcoin var med andra ord först med att använda Proof-of-work för att lösa det datorvetenskapliga problemet "Byzantine Generals' Problem" som handlar om hur flera olika deltagare i ett osäkert kommunikationsnätverk kan koordinera sig med varandra och uppnå konsensus på ett säkert sätt (Lamport, Shostak, & Pease, 1982; Miller & LaViola, 2014).

Lösningen består i att alla transaktioner annonseras ut publikt till alla deltagare (noder) i nätverket. För att alla sedan ska vara överens om en gemensam historia över alla transaktioner så låses de kryptografiskt i en kronologisk kedja av transak-

tionsblock (blockkedjan) genom en process som kallas Proof-of-work . Den blockkedja som genererats genom mest Proof-of-work som gäller som ett majoritetsbeslut för den aktuella transaktionshistoriken.

Decentraliserat konsensus är ett svårt problem till skillnad från ett traditionellt konsensus som etableras genom validering av en eller flera anförtrodda identifierade parter. Decentraliserat konsensus kräver att de som validerar transaktioner inte behöver vara identifierade, att de kan förändras över tid, samt utan kostnad gå med i eller lämna systemet. Decentraliserat konsensus kan åstadkommas genom att valideringen innefattar beräkningen av en enkel oberoende matematisk funktion många gånger, så att utföra denna beräkning under dubbelt så lång tid är ekvivalent med att utföra den parallellt med dubbelt så mycket beräkningskraft. Detta är grunden för Proof-of-work .

Bitcoin-mining fungerar genom en hash-baserad Proof-of-work algoritm kallad hashcash (Back, 2002). Hashfunktionen som används (SHA-256) är en verkligt slumpmässig funktion vilket gör att det enda sättet att producera en giltig Proof-of-work signatur är att utföra nya oberoende beräkningar om och om igen med nya värden tills en giltig lösning hittas som uppfyller kravet i Bitcoin-protokollet för att lägga ett nytt block med transaktioner till blockkedjan. Att utföra beräkningar kräver enligt fysikens lagar arbete genom att energi förbrukas och därmed också att det tar en viss tid att utföra beräkningarna (Landauer, 1961).

Från början kunde Bitcoin-mining ske med processorn i vanliga datorer av vanliga användare, men i takt med att konkurrensen hårdnat har mining blivit en allt mer specialiserad industri med specialiserad hårdvara för att kunna göra så många beräkningar som möjligt till så låg energikostnad som möjligt.

För att få en jämnare utbetalning från mining över tid sker mining i pooler där deltagarna aggregerar sin beräkningskraft och delar på belöningen när poolen hittar lösningen till ett block. Om miners med låg andel av den totala beräkningskraften i nätverket agerade självständigt skulle det kunna ta månader och år innan de hittar lösningen till ett block, vilket blir svårt att matcha med löpande utgifter i form av el och underhåll.

Proof-of-work är en mycket energikrävande konsensusmekanism. Enligt en analys förbrukades ca 0.1% av världsproduktionen av elektricitet till mining av Bitcoin i januari 2018 (Bevand, 2018). Som jämförelse uppskattas all nätverksinfrastruktur och alla datacenter i världen (exklusive Bitcoin) förbruka ca 2% av världsproduktionen av elektricitet (Koomey, 2018). Andelen förnybar energi som används för mining av Bitcoin har dock beräknats uppgå till minst 78% (Bendiksen m.fl., 2018). Det kan förklaras av att billig elektricitet är ett avgörande kriterier för att kunna bedriva lönsam miningverksamhet och därför förläggs miningverksamhet med fördel i områden med överkapacitet av genererad elektricitet i form av framförallt vattenkraft som annars skulle gå till spillo.

En alternativ konsensusalgoritm som används av vissa kryptovalutor är proof-of-stake. Proof-of-stake innebär att noder som kontrollerar en andel av den interna valutan får delta i processen att lägga nya block med transaktioner till blockkedjan istället för noder som utför beräkningar. Ett argument som framförs för proof-of-stake är att det skulle vara mer kostsamt att ta kontroll över blockkedjan genom att anskaffa över 50% av den interna valutan än att anskaffa mer än 50% av den totala beräkningskraften i nätverket. Ett annat argument som framförs för proof-of-stake är att det är mer miljövänligt och effektivt eftersom det inte innebär något förbrukande av externa fysiska resurser. De användare som låser upp valuta i en blockkedja har chans att få lägga till nästa block med transaktioner till blockkedjan i proportion till hur stor andel av den interna valutan de kontrollerar och skapandet av nya block belönas med vanligtvis med nyskapad intern valuta och transaktionsavgifter på motsvarande sätt som Proof-of-work .

Det har dock visats att proof-of-stake inte är tillräckligt för att uppnå decentraliserat konsensus för att skapa en decentraliserad blockkedja och kryptovaluta (Poelstra, 2015). Det beror på att det inte finns någon extern kostnad för att skapa alternativa historiker över systemets interna tillstånd vilket avgör fördelningen av den interna valutan. En nod som kopplar bort sig från nätverket under en tid eller ansluter för första gången har inget sätt att skilja på en riktig transaktionshistorik och en simulerad sådan utan att sätta sin tillit till en anförtrodd tredjepart (Daian, Pass, & Shi, 2016). Det har därför dokumenterats en lång rad av attacker som proof-of-stake är känsligt för (BitFury Group, 2015).

Historiken i en blockkedja som byggs genom Proof-of-work blir säkrare med tiden då det för varje nytt block som läggs till krävs mer arbete för att skriva om transaktionshistoriken. För en blockkedja som byggs med proof-of-stake så kan det argumenteras att historiken istället blir mindre säker med tiden eftersom det finns fler tidpunkter i historien varifrån privata nycklar kan återanvändas för att skapa alternativa kedjor. En annan aspekt är att i proof-of-stake så blir de rika gradvis rikare utan att behöva arbeta för det eller ta någon risk, eftersom de med fler mynt i systemet har en högre sannolikhet att få belöningen för att lägga nya block till kedjan, vilket med tiden leder till en ökad centralisering.

I privata blockkedjor där alla parter är identifierade behöver varken Proof-of-work eller proof-of-stake användas för att nå konsensus utan istället kan alla deltagarna i nätverket, eller utvalda noder, beroende på implementering, rösta om att lägga till block med nya transaktioner till blockkedjan (Goya, 2017). Det finns även olika former av hybrider, exempelvis blockkedjor som är öppna för alla att göra transaktioner på, men där valideringen av transaktioner är centraliserad och sker genom röstning av anförtrodda parter.

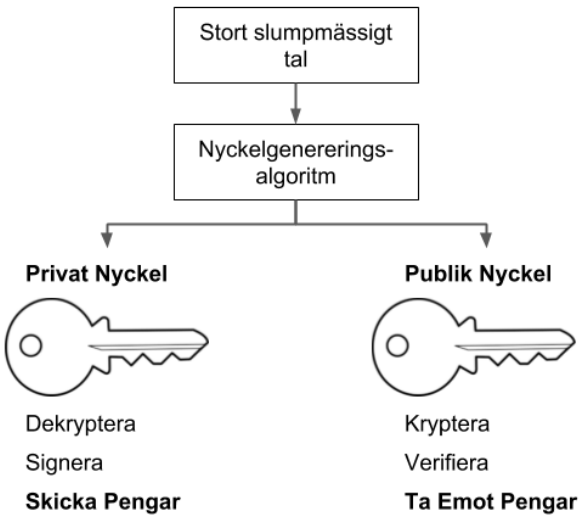
3.4 Intern valuta och transaktioner

Bitcoins blockkedja innehåller datablock med transaktioner som består av kryptografiskt signerade meddelanden. I blockkedjan finns det inga inbyggda koncept för användare, konton, kontobalanser eller identiteter, dessa existerar bara i den mån som de kan härledas från transaktionerna i blockkedjan.

Varje transaktion består av en lista av indata med saldon från mottagna transaktioner och en lista med utdata med saldon till adresser som pengarna ska skickas till. En "plånbok" för att hantera tillgångar på blockkedjan i sin enklaste form består av en privat och en publik kryptonyckel som är matematiskt sammanlänkade genom asymmetrisk kryptering baserat på matematik för elliptiska kurvor.

En privat nyckel i Bitcoin är ett heltal mellan 1 och ca 10^77 (2^256, eller 256 bits), denna siffra körs sedan i en matematisk funktion kallad Elliptic Curve Digital Signature Algorithm med de parametrar som beskrivs av standarden secp256k1 för att generera motsvarande publika nyckel. Den publika nyckeln används för att generera en adress för att kunna ta emot pengar och den privata nyckeln används för att kunna skicka pengar (Figur 5).

Figur 5 Asymmetrisk kryptering för att skicka och ta emot blockkedjans interna valuta



För att skicka en transaktion behöver indata som används i transaktionen signeras med den privata nyckel som hör till den publika nyckel som pengarna i föregående led skickades till. Varje transaktion blir på detta sätt direkt sammanlänkad till tidigare transaktioner ända tillbaka till det block i blockkedjan där pengarna skapades från första början som belöning till en miner för att ha hittat en Proof-of-work lösning för att skapa det blocket. Detta gör att alla mynt i systemet blir unika eftersom de kan länkas tillbaka till ett specifikt block där de skapades och det är även detta som garanterar den begränsade valutamängden i systemet.

I varje transaktion som utförs behöver saldot för listan av indata till transaktionen vara större än eller lika stort som listan av utdata med adresser dit pengarna ska skickas. Om saldot för ingående värden är större än saldot för utgående värden tolkas mellanskillnaden som en transaktionsavgift som går till den miner som lyckas skapa det block som transaktionen inkluderas i. Att äga en kryptovaluta som bitcoin innebär endast ensam kontroll över de kryptonycklar som behövs för att skicka en viss mängd bitcoin som tidigare tagits emot på den distribuerade blockkedjan som finns representerad på tusentals datorer över hela världen.

Transaktioner kan skapas och skickas på olika sätt. För den enklaste formen av transaktioner behöver endast en giltig kryptografisk signatur tillhandahållas genom en privat nyckel. Mer avancerade transaktioner kan utföras genom att transaktionen innehåller ett skript (en lista med instruktioner) som utgör ett smart kontrakt som specificerar under vilka villkor pengarna flyttas.

En enkel form av ett smart kontrakt är en multisignatur-transaktion där signering av M av N privata nycklar krävs för att auktorisera en transaktion.[3] Den vanligaste formen är av typen 2 av 3 privata nycklar. Multisignatur-transaktioner är användbara för att säkra konton och för tre-parts-transaktioner (eng. escrow), där exempelvis köparen håller en privat nyckel, säljaren håller en privat nyckel och en tredjepart håller en tredje privat nyckel. Om både köparen och säljaren är nöjda kan de enkelt signera transaktionen med deras respektive nycklar och det blir inget behov av en tredjepart. Om en tvist uppstår mellan köparen och säljaren kan den tredje parten gå in och medla och agera skiljedomare i tvisten genom att signera en transaktion med den tredje privata nyckeln. Antingen tillsammans med köparens eller säljarens nyckel. Alltså antingen till köparens eller säljarens favör, eller en procentuell fördelning dem emellan.

3.5 Hur blockkedjor uppgraderas

Liksom all form av mjukvara så behöver mjukvaran för blockkedjeprotokoll uppdateras med jämna mellanrum för att täppa till säkerhetsluckor, optimera dess funktion och för att lägga till nya funktioner. Konsensusreglerna är den mest kritiska delen av mjukvaran som avgör vilka transaktioner och block som anses giltiga. Varje användare av nätverket behöver följa samma konsensusregler för att vara överens om en gemensam blockkedja.

Blockkedjor kan uppgraderas genom att mjukvaran som enskilda noder använder förändras på ett bakåtkompatibelt eller ett icke-bakåtkompatibelt sätt. För att uppgradera nätverket på ett icke-bakåtkompatibelt sätt så krävs det i princip enhällighet bland alla användare för att resultatet inte ska bli att blockkedjan delas upp i två separata nätverk. Av den anledningen och ur säkerhetssynpunkt så är bakåtkompatibla uppgraderingar att föredra. Följande terminologi används för dessa två klasser av uppgraderingar av blockkedjeprotokoll.

[3] https://en.bitcoin.it/wiki/Multisignature

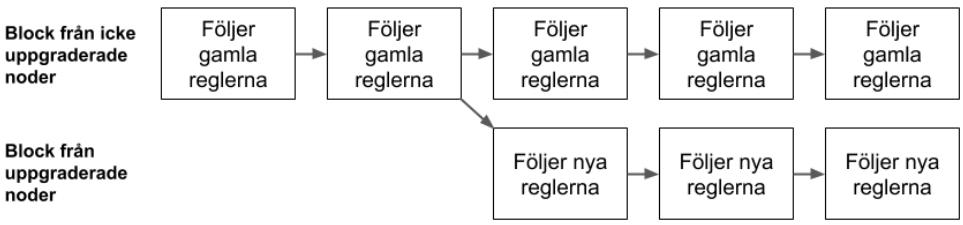
3.5.1 Soft fork

En soft fork är en förändring i protokollet som innebär att konsensusreglerna görs striktare. Det innebär att en viss sorts transaktion eller block som tidigare ansågs giltig blir ogiltig med de nya reglerna. En soft fork är bakåtkompatibel med tidigare versioner av protokollet eftersom alla transaktioner och block som produceras med de nya reglerna är tillåtna även enligt de gamla reglerna. Det betyder att noder som uppgraderar till den nya mjukvaran och de som är kvar på äldre versioner av mjukvaran fortfarande är kompatibla och del av samma nätverk och samma blockkedja. För att de nya reglerna i en soft fork ska aktiveras krävs det att de antas av en majoritet av miners, så att blockkedjan med mest Proof-of-work följer de nya striktare reglerna.

3.5.2 Hard fork

En hard fork är en förändring i protokollet som innebär att konsensusreglerna görs mindre strikta. Det innebär att en viss typ av transaktion eller block som anses ogiltig med de gamla reglerna görs giltig med de nya reglerna. En hard fork är inte bakåtkompatibel med tidigare versioner av protokollet. Det betyder att alla användare och miners behöver uppgradera till de nya reglerna för att inte nätverket och blockkedjan ska delas upp i två separata versioner bestående av de användare som är kvar på de gamla reglerna respektive de användare som bytt till mjukvaran med de nya reglerna. Om det finns användare som vill ha kvar de gamla reglerna och det även finns användare som vill följa de nya reglerna så blir resultatet att de går skilda vägar i varsin blockkedja som delar en gemensam historia bakåt i tiden (Figur 6).

Figur 6 **Vid en hard fork avvisar icke uppgraderade noder block från uppgraderade noder vilket leder till att noder med de nya reglerna fortsätter som en separat blockkedja**



3.6 Transparens och anonymitet

I publika blockkedjor kan alla se alla transaktioner som någonsin har skett. Alla kan se från vilken adress och till vilken adress blockkedjans interna valuta har skickats, det belopp som skickats samt tidpunkten för transaktionen. Vilka personer, företag eller organisationer som äger olika adresser behöver dock inte vara publikt och nya adresser kan genereras och användas för varje ny transaktion.

Om det kommit till kännedom att en viss individ äger en viss adress, så går det att i blockkedjan se alla transaktioner som utförts med den adressen. Om det är känt att en eller flera adresser hör till en viss individ så går det ofta även att ta reda på andra adresser som den individen kontrollerar med hög sannolikhet. Det senare bygger på antaganden för hur plånboksmjukvara hanterar transaktioner och återanvändning av adresser. I en demonstration av dessa tekniker så kunde 70% av en viss bitcoinplånboks adresser hittas givet kännedom om endast en av dess adresser (Nick, 2016).

Det finns flera företag som specialiserat sig på att bygga verktyg för att analysera blockkedjor i syfte att hjälpa myndigheter med brottsbekämpning och hjälpa företag att följa regleringar kring penningtvätt, kundkännedom och att göra riskbedömningar. Några exempel på sådana företag är Chainalysis, Coinalytics och Elliptic.

På grund av detta är det i praktiken mycket svårare att göra anonyma transaktioner med bitcoin än med vanliga fysiska kontanter. Kontanter är en anonym betalningsform som gör det möjligt att utföra privata transaktioner peer-to-peer utan inblandning eller behov av en mellanhand eller tredjepart som får insyn i alla transaktioner och som kan missbruka den makten. Utan kontanter så finns det inget sätt att utföra transaktioner som inte övervakas och kräver tillstånd från en tredje part.

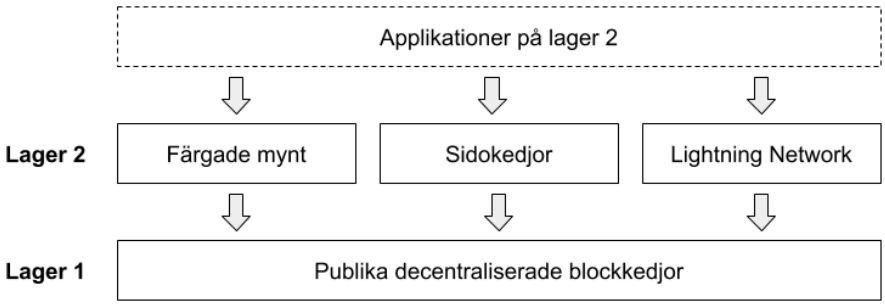
Flera kryptovalutor har skapats och är under utveckling för att kunna ge mer privata transaktioner än Bitcoin. Några exempel på sådana är Monero, Zcash, Grin och Beam. Det är även möjligt att uppgraderingar implementeras i Bitcoin i framtiden som kan göra mer privata transaktioner möjliga. Spårbarheten av bitcointransaktioner kan också minskas genom att använda mixingtjänster där transaktioner formas som blandar bitcoin från olika användare, vilket bryter den direkta kopplingen mellan sändare och mottagare. Ett annat sätt att bryta spårbarheten är att växla bitcoin till en mer privat kryptovaluta och sedan växla tillbaka.

Kryptovalutor kan även användas för att uppnå en ekonomisk transparens som inte går att uppnå i det vanliga finansiella systemet, med full spårbarhet. Detta skulle exempelvis kunna användas för att följa hur varje skattekrona spenderas i den offentliga sektorn eller hur pengar som samlas in av biståndsorganisationer används.

3.7 Lager ovanpå blockkedjor

Precis som Internet är uppbyggt genom lager på lager av olika protokoll så är det även möjligt att bygga olika lager av nya protokoll och applikationer ovanpå blockkedjor. På så sätt kan nya användningsområden skapas och kapaciteten skalas upp utan att kompromissa på blockkedjans decentralisering och säkerhet. Detta innebär att blockkedjan används som ett undre lager där säkerheten för transaktionssystem och decentraliserade applikationer i de övre lagren kan förankras (Figur 7).

Figur 7 Lager ovanpå blockkedjor



Med en säker publik decentraliserad blockkedja som första lager så går det att bygga säkra decentraliserade lager ovanpå. Det går däremot inte att bygga säkra lager ovanpå en osäker grund, eller decentraliserade applikationer på en centraliserad grund.

3.7.1 Färgade mynt

I Bitcoins blockkedja och andra blockkedjor finns det utrymme för en viss mängd metadata som kan inkluderas med varje transaktion. Genom dessa metadata kan enskilda enheter av den interna valutan öronmärkas och innehålla logik för att associeras med nya protokoll för utgivning och transaktioner i andra tillgångar, exempelvis aktier, obligationer, råvaror, fastigheter, fiatvalutor och olika former av värdekuponger (Rosenfeld, 2012). Den generella termen för detta är "Colored Coins"[4]. Färgade mynt hanteras av protokoll som tolkar bifogad metadata, skriver ny metadata och utför definierade operationer i enlighet med reglerna för det överliggande protokollet. Exempel på öppna protokoll som utvecklats för detta är Counterparty, Omni Layer och EPOBC som utvecklats av det svenska företaget ChromaWay. Olika former av tillgångar kan med dessa system utfärdas av olika utgivare, där transaktioner med dessa tillgångar sedan sker genom blockkedjan.

[4] https://en.bitcoin.it/wiki/Colored_Coins

3.7.2 Sidokedjor

Ett annat sätt att utöka en blockkedjas funktionalitet är genom Sidokedjor (Back m.fl., 2014). Sidokedjor är blockkedjor som är kopplade till och kompatibla med huvudblockkedjan så att tillgångar kan flyttas mellan dem. Genom sidokedjor kan nya funktioner introduceras utan att kompromissa med säkerheten för huvudkedjan. Uppstår problem på en sidokedja så är skadorna begränsade till de tillgångar som flyttats dit från huvudkedjan. Liquid är en sidokedja som utvecklats av företaget Blockstream för att snabbt, anonymt och säkert flytta större summor av bitcoin mellan börser (Dilley m.fl., 2016). Liquid lanserades och togs i bruk av 23 kryptovalutabörser i oktober 2018. RSK är namnet på en annan sidokedja till Bitcoin som håller på att utvecklas i syfte att kunna utföra lika avancerade smarta kontrakt med Bitcoin som är möjligt på Ethereums blockkedja (Lerner, 2015).

3.7.3 Betalningskanaler

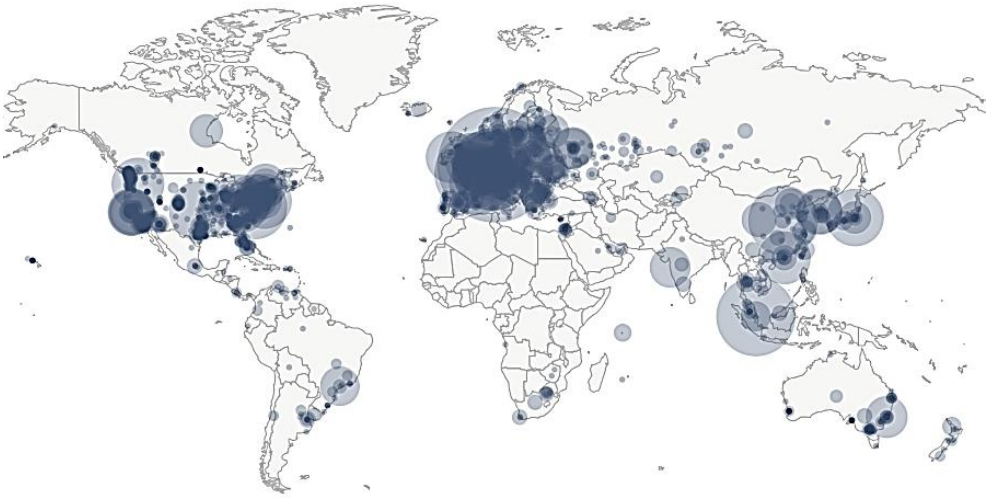
Betalningskanaler är en annan typ av lager där ett stort antal transaktioner kan ske på ett kryptografiskt säkert sätt mellan två parter utanför blockkedjan. Varje ny transaktion mellan parterna uppdaterar saldot mellan dem och ersätter det föregående. Det är först när en betalningskanal stängs av endera parten som balansen av dessa transaktioner registreras på blockkedjan. Genom att koppla ihop ett nätverk av denna typ av betalningskanaler med hjälp av smarta kontrakt, som säkerställer att mellanliggande noder inte kan stjäla pengar som de förmedlar, så blir det möjligt för varje användare i nätverket att kryptografiskt säkert och snabbt skicka pengar till varje annan användare till en mycket låg kostnad, vilket möjliggör omedelbara mikrobetalningar. För detta syfte har Lightning Network utvecklats för att skapa ett betalningsnätverk ovanpå Bitcoins blockkedja (Poon & Dryja, 2016). Lightning Network protokollet finns i flera olika implementationer som utvecklas av olika företag efter en gemensam standard och användningen och utvecklingen av Lightning Network har växt kraftigt sedan de första implementationerna lanserades i början av 2018. Lightning Network kan möjliggöra en i princip obegränsad transaktionskapacitet.

3.8 Decentralisering och säkerhet

Säkerheten hos publika blockkedjor bygger på att inga enskilda parter kan ta kontroll över dem. Det krävs att det inte finns några anförtrodda tredjeparter involverade i systemet vilka skulle kunna utgöra säkerhetshål, samt orsaka skada för systemet som helhet. Anförtrodda tredjeparter utgör alltid en källa till säkerhetsrisk genom att de kan bli kompromissade inifrån av en insider eller utifrån av hackare som tar sig in med rent tekniska medel eller via social manipulation (Szabo, 2001). Det är viktigt att decentraliseringen och säkerheten består i takt med att nätverket uppgraderas, antalet användare växer och nya sätt att attackera systemet upptäcks.

Ett mått på decentralisering är hur många oberoende noder som finns i nätverket. Endast genom att köra en egen nod är det möjligt att använda en blockkedja utan att behöva lita på någon annan. För att möjliggöra högsta möjliga decentralisering i denna dimension är det viktigt att det inte kostar varje användare för mycket att köra en egen nod. Om det kräver mycket resurser och är dyrt att köra en egen nod för att vara en oberoende medlem i nätverket, så blir resultatet att endast stora aktörer kommer att ha den möjligheten. Kostnader för att köra en egen full nod är framförallt kostnaden för att lagra och ständigt hålla sig uppdaterad med hela blockkedjan i form av kostnaden för lagringsutrymme och nätverksbandbredd. Det är därför viktigt att storleken på blockkedjan inte växer i för snabb takt. Bitcoins blockkedja var ca 200 Gb i total storlek i februari 2019 och växer med ca 50 Gb per år. Antalet noder som accepterar inkommande anslutningar i Bitcoins nätverk var samma tid ca 10 500 (Figur 8). Antalet noder kan ses som en funktion av efterfrågan på att validera transaktioner självständigt i förhållande till kostnaden för att driva en nod.

Figur 8 Geografisk koncentration av Bitcoin-noder i februari 2019

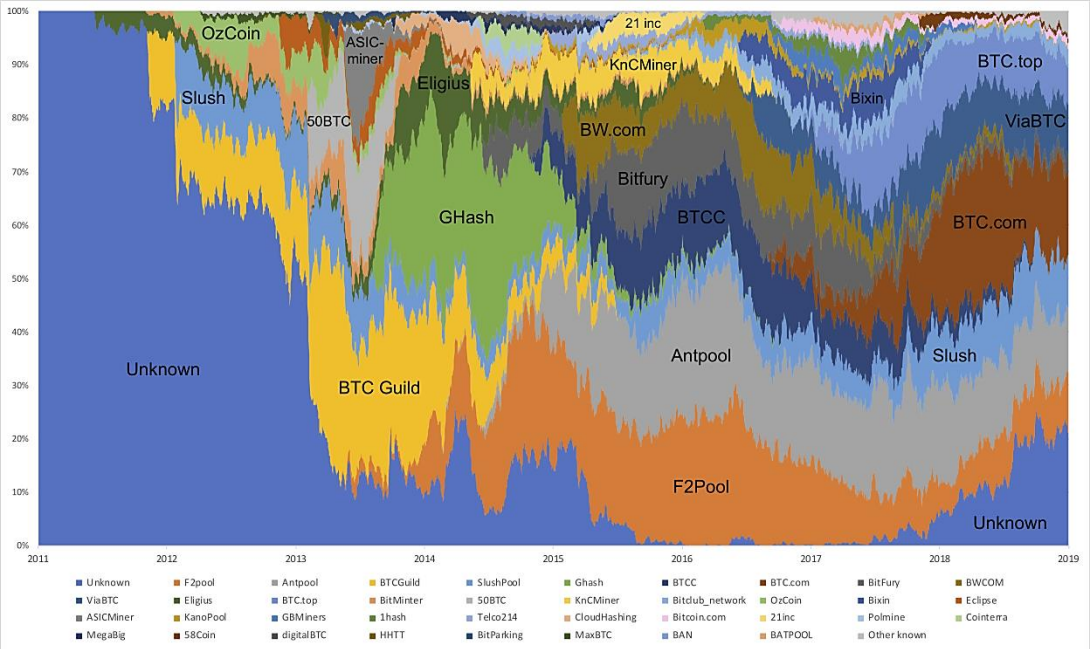


Källa: https://bitnodes.earn.com/

Ett annat mått på decentralisering är koncentrationen av miningverksamhet och hur den förändras över tid. Om en miner har över 50% av beräkningskraften i nätverket så är de i en position där de kan reversera transaktioner som de själva skickar, hindra alla eller ett urval av andras transaktioner från att bekräftas och hindra andra miningaktörer från att generera block som kommer med i den giltiga kedjan (med mest Proof-of-work), men de kan inte stjäla andras pengar eller ändra reglerna för protokollet. Miners har samtidigt starka ekonomiska incitament att inte försöka attackera nätverket eftersom det skulle skada deras möjligheter att göra en vinst på de omfattande investeringar i infrastruktur som de genomfört. Detta behöver dock inte gälla mindre och osäkrare kryptovalutor som använder samma typ av Proof-of-work algoritm som en större och säkrare kryptovaluta. Incitament kan då finnas för miners att attackera den mindre kryptovalutan, samtidigt som de kan ha fortsatt nytta av sina infrastrukturinvesteringar genom mining av den större kryptovalutan.

En sammanställning av marknadsandelen för miningpooler på Bitcoin från 2011 till 2019 visar att omsättningen bland miningaktörer är hög och att det är svårt för enskilda aktörer att behålla en stark ställning under någon längre tid, vilket tyder på en fungerande konkurrens (Figur 9).

Figur 9 Marknadsandel för miningpooler på Bitcoin från 2011 till 2019



Källa: https://coinmetrics.io/miningpool-mapping/

Ett ytterligare mått på decentralisering är hur decentraliserad utvecklingen av mjukvaran är. Som ett öppet och fritt mjukvaruprojekt så sker utvecklingen av Bitcoin genom att varje individ som bidrar till projektet arbetar med de saker som de själva tycker är viktiga och det finns inga centrala projektledare som styr utvecklingen. All diskussion och utveckling sker i öppna kanaler. Det avgörande för om ett bidrag uppskattas och godkänns av de övriga utvecklarna är kvaliteten på kod, kodgranskning, tester och dokumentation för att säkerställa att föreslagna uppgraderingar är säkra och positiva för protokollets funktion och utvecklingen sker på GitHub som är den största plattformen i världen för utveckling av mjukvara med öppen källkod.

Metoden för uppgradering av protokollet är också viktig för decentraliseringen. Att uppgradera på ett sätt som är bakåtkompatibelt med tidigare versioner av protokollet garanterar att ingen behöver känna press att uppgradera till en mjukvara som de inte känner sig bekväm med. Det betyder att utvecklarna inte får någon privilegierad ställning eller makt att förändra reglerna i protokollet. Genom att endast uppgradera genom soft forks så innebär det att alla användares noder förblir kompatibla även om de kör olika versioner av mjukvaran. Varje användare kan fritt välja vilken version av mjukvaran bland olika soft forks de vill köra och om de uppgraderar till en ny version och ångrar sig så kan de enkelt byta tillbaka till en äldre version utan att någon skada är skedd. Vid uppgradering genom hard forks

blir alla användare tvungna att unisont uppgradera eller unisont avvisa den nya mjukvaran för att inte riskera att nätverket och blockkedjan delas i två. Uppgradering genom hard forks kan därför sägas ge utvecklare mer makt, vilket kan ge mer centraliserad kontroll. Att uppgradera genom hard forks kan också vara mycket mer riskabelt eftersom det introducerar nya regler som inte varit tillåtna tidigare. Med soft forks kan det inte bli någon plötslig obehaglig överraskning eftersom systemet är skyddat enligt samma gamla regler som det tidigare överlevt genom.

Slutligen är komplexitet ofta en fiende till säkerhet. Mer komplex mjukvara med längre kod kan ha fler komponenter som kan interagera med varandra på oförutsedda sätt, kan innehålla fler sårbarheter och blir svårare att analysera (McGraw, 2004).

3.9 Blockkedjeteknikens begränsningar

Blockkedjeteknik tenderar att framställas som en universallösning av dess förespråkare, men det är viktigt att vara medveten om dess begränsningar.

För att en blockkedja ska kunna möjliggöra funktioner utöver en vanlig databas så krävs det att den är decentraliserad. Det vill säga att alla kan använda den på lika villkor och vara överens om blockkedjans tillstånd och innehåll utan behov av en central anförtrodd part. Decentralisering krävs för att det inte ska finnas någon enskild svag punkt genom vilken databasen kan skadas, kontrolleras eller korrumperas. Decentralisering krävs för att det endast ska gå att lägga till data och inte ta bort tidigare inmatad data, och för att transaktioner och registrering av data inte ska kunna hindras eller censureras av någon. Detta i sin tur möjliggör säkert ägande och kontroll av digitala tillgångar i blockkedjan av enskilda parter utan motpartsrisk och övriga unika tillämpningar.

Kostnaderna för att skapa ett system med dessa egenskaper är dock höga. Det innebär att utvecklingen och uppdateringen av mjukvaran som behöver köras för att delta som en nod i nätverket måste göras ytterst noggrant och konservativt för att inte buggar ska introduceras som kan äventyra databasens integritet och alla dess användares digitala tillgångar. Alla uppgraderingar för systemet behöver anammas frivilligt av alla deltagare, då det inte finns någon central part som kan tvinga användare att köra en viss version av protokollet. Alla uppdateringar behöver vara bakåtkompatibla för att inte riskera att nätverket splittras, vilket gör det betydligt mer komplicerat att introducera nya funktioner och gör att det tar lång tid att testa och utveckla uppgraderingar.

En fungerande incitamentsstruktur behöver finnas för att se till att användare av systemet inte har möjlighet att missbruka eller korrumpera den gemensamma databasen. Det får exempelvis inte vara för billigt att lägga in stora mängder data i blockkedjan som sedan alla noder behöver lagra och hålla i minnet för all framtid. Det får inte heller vara för dyrt att registrera nya transaktioner och data i blockkedjan, för då kommer mycket få att vilja använda den. Det finns ingen möjlighet att stänga ute enskilda användare om de hittar sätt att använda blockkedjan som orsakar skada för resten av dess användare. Protokollet måste vara opartiskt och genomdriva de regler som definieras av programvaran.

Kostnaderna för att upprätthålla en decentraliserad blockkedja är betydligt högre än för traditionella databaser och dessa kostnader behöver motiveras av motsvarande unika nytta som inte går att åstadkomma med en traditionell databas, framförallt censurresistans genom decentralisering så att inga enskilda parter kan utöva kontroll över systemet som helhet.

Att skala upp kapaciteten är betydligt svårare i en decentraliserad blockkedjedatabas än i ett traditionellt centraliserat system. Det beror på att samma uppsättning data behöver lagras och uppdateras på tusentals ställen istället för på en enda plats. Varje enskild nod behöver kontinuerligt betala kostnaderna för överföring, verifiering och lagring av all data i blockkedjan, istället för att denna kostnad betalas en gång i en traditionell centraliserad databas. Att reducera denna kostnad genom att ha ett färre antal noder i nätverket är inte ett alternativ eftersom varje användare behöver köra sin egen nod för att kunna använda systemet utan att förlita sig på någon tredjepart.

Decentraliserade system är svåra och dyra att upprätthålla, svåra att uppgradera och svåra att skala upp kapaciteten i. Så varför framhävs blockkedjeteknik som lösningen för så många problem? Blockkedjeteknik tenderar att användas som ett sätt att sälja in uppgraderingar av föråldrade IT-system hos företag och banker, men de system som säljs in som blockkedjeteknik är i själva verket inte decentraliserade och kan därmed inte erbjuda ett decentraliserat systems egenskaper. Ett andra skäl kan vara att benämningen blockkedjeteknik ger sken av att företag befinner sig i framkant gällande teknikutveckling.

De enda egentliga användningsområden där blockkedjeteknikens begränsningar kan försvaras är där decentralisering och eliminering av centrala punkter av sårbarhet och kontroll överväger kostnaderna. De flesta industrier kräver nya funktioner eller uppgraderingar och friheten att byta och expandera vid behov. Eftersom blockkedjor är svåra att uppgradera, svåra att ändra och svåra att skala, har de flesta industrier begränsad användning för blockkedjor för deras specifika ändamål. Många implementationer som kallar sig blockkedjor försöker göra det omöjliga i att skapa säkerheten i ett decentraliserat system men med kontrollen och flexibiliteten som i ett centraliserat system. Resultatet kan då bli en kombination av kostnaderna och svårigheterna för ett decentraliserat system i kombination med sårbarheterna hos ett centraliserat system.Ett användningsområde där en decentraliserad blockkedjas svårighet att förändra, stabilitet och förutsägbarhet är en fördel är för applikationen pengar. Avsaknad av central kontroll och avsaknad av möjligheten att förändra penningpolitiken är en fördel för ett monetärt system och en valuta. En intern valuta och Proof-of-work verkar även vara nödvändigt för att skapa ett fungerande incitamentssystem för att hålla en blockkedja säker och decentraliserad. Med en sådan blockkedja som grund kan sedan även andra applikationer än valuta byggas ovanpå där behovet av en anförtrodd tredjepart kan uteslutas.

4 Användningsområden för blockkedjeteknik

Blockkedjeteknik möjliggör ett flertal nya applikationer som inte tidigare varit möjliga. Blockedjors interna valuta kan möjliggöra digital knapphet, digitala objekt som inte kan kopieras, men som kan överföras från person till person. Dessa kan användas som valutor, finansiella instrument och digitala äganderätter som kan hanteras utan mellanhänder eller anförtrodda tredjeparter.

Genom att blockkedjeteknik använder asymmetrisk kryptering för att hantera transaktioner och att varje block med transaktioner är tidsstämplat, samt permanent lagrat så möjliggörs permanent verifierbar dokumentering och hantering av certifikat, licenser, identitetshandlingar och digitala nycklar.

Blockkedjeteknik möjliggör även smarta kontrakt som kan användas för smarta ägodelar och decentraliserade applikationer för decentraliserad handel, decentraliserade databaser, samt potentiellt säker elektronisk röstning och decentraliserade autonoma organisationer.

4.1 Alternativ valuta

Blockkedjetekniken skapades för att möjliggöra Bitcoin som världens första decentraliserade digitala kontantsystem. Bitcoin är både en valuta och betalsystem samtidigt vilket möjliggör peer-to-peer betalningar över elektroniska kommunikationskanaler utan mellanhänder.

Kontanter i form av mynt, sedlar och bitcoin är vad som på engelska kallas “bearer instruments”. Det betyder att innehavaren är ägaren och om de överförs till en annan innehavare så överförs ägandet i samma stund. Kontanter har även ett värde i sig själv och de är inte samtidigt någon annans skuld, till skillnad från krediter. Vid kontant betalning behöver inte den som betalar lämna ut någon känslig information till mottagaren eftersom kontanterna i sig själva har ett värde. Vid betalning med betalkort så dras pengar från ett konto hos en bank. Känslig information för kontot behöver därför lämnas ut till kortterminalen som i sin tur avgör hur mycket pengar som ska dras från kontot. Det gör att kortbetalningar kan bli utsatta för stöld och bedrägerier med kontouppgifter.

Kontanter i form av sedlar var från början skuldebrev, exempelvis som bevis på att en bank var skyldig innehavaren av skuldsedeln pengar i form av guld eller silver. Fram till 1971 hade amerikanska dollar som sista nationella valuta i världen kvar denna ursprungliga funktion. Detta upphörde då Richard Nixon genom “Executive Order 11615” avskaffade konvertabiliteten mellan dollarsedlar och guld som hade gällt med 35 dollar för 1 uns guld sedan Bretton Woods avtalet 1944. Efter 1971 har det enbart funnits fiatvalutor i världen utan koppling till någon knapp fysisk resurs. Inga nationella valutor kan längre växlas in till en fast mängd guld. I

realiteten är alltså sedelns historiska funktion avskaffad i världen sedan 1971 och vi befinner oss i ett nytt monetärt paradigm sedan dess. Avskaffandet av kopplingen mellan pengar och en knapp fysisk resurs (som guld) har inneburit att världens centralbanker är fria att trycka så mycket nya pengar som de anser är lämpligt. Detta kan i värsta fall leda till hyperinflation där en valuta förlorar i princip all sin köpkraft till följd av att en centralbank trycker allt för mycket nya pengar. Mellan 1920 och 2008 har över 50 fall av hyperinflation dokumenterats i olika länder vilket definieras som en allmän konsumentprisökning på minst 50% per månad (Hanke & Krus, 2012). Dessa hyperinflationer har enbart varit möjliga genom en central politisk kontroll över mängden pengar.

Bitcoin och de flesta kryptovalutor har en strikt reglerad inflation och total penningmängd som regleras enligt konsensusreglerna i protokollet. Den strikta penningmängden, möjlighet att skicka pengar över hela världen omedelbart till låg kostnad utan mellanhänder, samt omöjligheten att censurera transaktioner kan med tiden göra att dem till ett konkurrenskraftigt alternativ till nationella valutor. I exempelvis Venezuela där hyperinflation nu råder kan kryptovalutor erbjuda en livlina, men även i länder som Zimbabwe, Iran, Sudan och Argentina lider befolkningen nu av mycket hög inflation.

4.2 Permanent verifierbar dokumentering

För fysiska dokument finns det olika sätt att tidsstämpla dokument med mer eller mindre beviskraft och legitimitet. Ett simpelt sätt kan vara skicka ett brev till sig själv och lämna det oöppnat, vilket kan tjäna som ett bevis på att det förslutna brevet existerade före det datum som kuvertet poststämplades. Ett mer rättsligt hållbart sätt kan vara få ett fysiskt dokument intygat av en notarius publicus. För digitala dokument är det betydligt svårare att bevisa att ett visst dokument existerat i en viss form vid en viss tidpunkt och det är enklare att manipulera utan att det lämnar några spår.

Säker och verifierbar tidsstämpling av digitala dokument kan lösas med en decentraliserad publik blockkedja. Eftersom transaktioner på Bitcoins blockkedja är tidsstämplade och permanent lagrade så kan de användas för att bevisa att ett visst digitalt dokument (exempelvis text, bild, ljud, video) existerade vid en bestämd tidpunkt i historien (Clark & Essex, 2012).

Vid tidsstämpling av ett digitalt dokument på en blockkedja så registreras en hash av dokumentet som data i en transaktion på blockkedjan. En hash utgör ett digitalt fingeravtryck som unikt identifierar ett digitalt dokument. För att senare bevisa att ett existerande digitalt dokument funnits vid en tidigare tidpunkt i historien jämförs dokumentets hash med det som finns registrerat i blockkedjan.

I många situationer finns det ett behov av att intyga det datum ett dokument skapades eller senast modifierades. Vid exempelvis patenttvister kan det vara avgörande att kunna verifiera datumet som en uppfinnare först dokumenterade en patenterbar idé, för att fastställa dess företräde framför konkurrerande patentanspråk. Permanent verifierbar dokumentering av digitala dokument skulle även kunna revolutionera exempelvis myndigheters möjlighet till tillsyn och övervakning av bokföring hos företag om lagar stiftades som krävde att bokföringsposter gällande ekonomiska transaktioner eller någon annan typ av process kontinuerligt registreras och tidsstämplas i en decentraliserad och oföränderlig blockkedja.

OpenTimestamps är ett protokoll med öppen källkod utvecklat av Peter Todd som gör det möjligt att tidsstämpla ett obegränsat antal digitala dokument i en enda Bitcointransaktion (Todd, 2016). Genom Merkle-träd-strukturer uppnås en obegränsad skalbarhet. För att validera konceptet så användes OpenTimestamp-protokollet i maj 2017 för att tidsstämpla alla 750 miljoner dokument som existerar i databasen Internet Archive, i en enda Bitcointransaktion. Om någon av dessa enskilda dokument i Internet Archive skulle tas bort eller manipuleras så skulle detta nu gå att upptäcka med hjälp av data sparat i Bitcoins blockkedja. Chainpoint är ett annat öppet protokoll som fungerar enligt samma princip som OpenTimestamps men som skiljer sig i implementationen (Vaughan, Bukowski, & Wilkinson, 2016).

Blockkedjor kan möjliggöra en bokföringsteknisk innovation som kallas trippel bokföring (Grigg, 2005). Trippel bokföring kan ge lika pålitlig bokföring mellan företag, organisationer och myndigheter som dubbel bokföring möjliggör inom enskilda företag, genom att alla transaktioner utöver att bokföras hos parterna till transaktionen även registreras i en blockkedja som agerar som en neutral tredjepart (De Oliveira m.fl., 2017). Ett sådant system skulle även kunna ge automatiserad bokföring och revision, vilken skulle kunna delges tillsynsmyndigheter och andra intressenter i realtid.

4.3 Certifikat och licenser

Permanent verifierbar dokumentering kan användas för att registrera dokument i form av certifikat och licenser. Genom att registrera certifikat och licenser i en publik blockkedja med permanent lagrade och tidsstämplade transaktioner så blir det möjligt att snabbt och oberoende verifiera dess äkthet oavsett var i världen man befinner sig och oavsett om den institution som utfärdade certifikatet eller licensen fortfarande existerar.

Universitetet i Nicosia på Cypern blev 2014 det första universitetet i världen som registrerade akademiska certifikat i en blockkedja och de var också första universitet i världen att erbjuda en kurs i kryptovalutor. De beskriver utförligt den process de använde för att registrera certifikaten på kursens hemsida samt hur äktheten av ett utfärdat certifikat kan verifieras. I korthet gick det till så att ett index-dokument i form av en pdf skapades som innehöll en SHA-256 hash av varje enskilt certifikat som utfärdats till elever som slutfört kursen “DFIN-511 Introduction to Digital

Currency". Därefter gjordes en SHA-256 hash av index-dokumentet som inkluderades som data i en bitcoin-transaktion. För att göra det möjligt att verifiera ett enskilt certifikats äkthet helt oberoende, endast med hjälp av Bitcoins blockkedja och en pdf av index-dokumentet, så inkluderades även ett tidsintervall i index-dokumentet i vilket det skulle inkluderas i en bitcoin-transaktion. Universitetet höll samtidigt tyst om vad de höll på med tills index-dokumentets hash registrerats i en bitcoin-transaktion och tidsintervallet löpt ut. Därigenom har ingen haft möjlighet att registrera alternativa index-dokument i Bitcoins blockkedja under den tidsperioden. Universitetet har sedan spridit index-dokumentet och publicerat dess hash för att det enkelt ska gå att få tag på utan att kontakta universitetet.

MIT Media Lab har utvecklat ett mer avancerat system för att registrera certifikat på Bitcoins blockkedja som även gör det möjligt för utfärdaren eller mottagaren av ett certifikat att indikera att certifikatet ska anses vara återkallat och inte längre giltigt, genom att göra en ny speciell bitcoin-transaktion.[5] Blockcerts är ytterligare ett projekt som utvecklat en öppen standard för att skapa, utfärda, visa och verifiera certifikat på blockkedjor.[6]

4.4 Identitetshandlingar

Publika blockkedjor kan användas som en allmänt tillgänglig publik och decentraliserad infrastruktur för hantering av krypteringsnycklar. Publika nycklar kan kopplas till enskilda individer, företag, organisationer och myndigheter, och dessa kan sedan använda tillhörande privata nyckel för att attestera olika uppgifter.

"Decentralized Identity Foundation" är en samarbetsorganisation med 56 medlemsföretag som arbetar med att utveckla öppna standarder för hantering av decentraliserade identifierare som ska kunna förankras i och vara kompatibla med olika blockkedjor. [7] "Self Sovereign Identity" (SSI) är ett begrepp som används för att benämna verifierbara suveräna identiteter som är helt under deras ägares kontroll, oberoende av något centraliserat register, identitetsleverantör eller certifikatmyndighet. "Decentralized Identifiers" (DID) är en öppen standard som utvecklats för SSI. Till dessa decentraliserade identiteter, hanterade genom blockkedjor, kan sedan olika certifikat, licenser och referenser kopplas. "World Wide Web Consortium" (W3C) som är det internationella standardiseringsorganet för protokoll på webben har en "W3C Credentials Community Group" som arbetar med att utforska och ta fram standardiserade protokoll för hantering av decentraliserade identiteter.[8] Ett av flera alternativ som denna grupp arbetar med är "Bitcoin Reference" (BTCR), vilket är ett protokoll som utvecklats för hantering av decentraliserade identiteter med Bitcoins blockkedja. [9]

---

[5] http://certificates.media.mit.edu/

[6] https://github.com/blockchain-certificates

[7] https://identity.foundation

[8] https://w3c-ccg.github.io/

[9] https://w3c-ccg.github.io/didm-btcr/

Identiteter och referenser som hanteras på blockkedjor kan ge mer kontroll och suveränitet för individer att äga sin egen identitet med möjligheten att säkert dela med sig av endast den information som är nödvändig för att verifiera behörighet, bevisa ett visst påstående eller signera ett avtal.

4.5 Smarta kontrakt

Smarta kontrakt är ett koncept som utvecklades av Nick Szabo i mitten av 90-talet innan blockkedjor existerade (Szabo, 1996; Szabo, 1997). Szabo definierar smarta kontrakt som kontrakt som inte verkställs enligt lag, utan av mjukvara eller hårdvara som helt och hållet integrerar de kontraktsvillkor som reglerar dess användande. Ett smart kontrakt är ett kontrakt som verkställer sig självt när kontraktets villkor uppfyllts. Szabo tar en fysisk varuautomat som ett enkelt exempel på ett smart kontrakt, där en vara som väljs automatiskt matas ut när betalning erhålles.

Med hjälp av blockkedjeteknik är det möjligt för människor och maskiner att ingå smarta kontrakt med varandra. Traditionella kontrakt ställer krav på att parterna har förtroende för varandra och uppfyller sina avtalsförpliktelser. Genom att programmera in automatiskt verkställande kontrakt i en decentraliserad blockkedja, som inga enskilda parter kontrollerar och som därmed alla parter potentiellt kan lita på blir det möjligt att eliminera den motpartsrisk som det innebär att ingå ett vanligt kontrakt. Detta gör att trösklarna för att göra affärer och transaktionskostnader kan minskas.

Smarta kontrakt upprätthålls inte av vanliga rättsliga institutioner utan de upprätthålls av blockkedjan. Kontraktet programmeras så att det verkställs automatiskt när de villkor uppfyllts som kontraktet specificerar. Verkställande av ett smart kontrakt resulterar i att en tillgång registrerad på blockkedjan representerad i form av blockkedjans interna valuta överförs till någon av parterna i kontraktet. Till vilken part som tillgångarna överförs och vilka tillgångar som överförs beror på villkoren i det smarta kontraktet. Smarta kontrakt automatiserar och säkerställer flödet av tillgångar mellan avtalsparterna när de specificerade villkoren uppfyllts.

Bitcoins blockkedja har ett begränsat programmeringsspråk för att skriva smarta kontrakt som kan innehålla logiska och aritmetiska operationer som specificerar med vilka kryptonycklar och under vilken tidsperiod tillgångarna i kontrakten kan flyttas.[10] Den största begränsningen består i att loopar (beräkningar som skall svara mot ett visst specifikt villkor som upprepas tills villkoret är uppfyllt) inte är tillåtna för att undvika risken för oändliga loopar vid transaktionsverifieringar.

[10] https://en.bitcoin.it/wiki/Contract

Ethereum är en blockkedja som har byggts specifikt för att kunna utföra mer avancerade smarta kontrakt.[11] De är vad som kallas Turing-kompletta (Turing, 1937). Det innebär att det inte finns några begränsningar i hur avancerade smarta kontrakt som kan programmeras in i blockkedjan. Ethereum-blockkedjan är tänkt att fungera som en decentraliserad universell dator. För att förhindra risken för oändliga loopar kostar varje beräkning som utförs av ett smart kontrakt i Ethereum en viss mängd av Ethereums interna valuta. Om saldot av den interna valutan som tilldelas programmet av användaren tar slut innan programmet körts klart avslutas programmet. Eftersom denna begränsning finns så är inte smarta kontrakt på Ethereum Turing-kompletta i strikt bemärkelse.

Ett mer privat, resurssnålt och flexibelt alternativ till att programmera smarta kontrakt i transaktioner direkt på blockkedjan är att hantera dem av parterna till kontraktet utanför blockkedjan och sedan endast skicka resultatet av det verkställda kontraktet för utbetalning på blockkedjan (Bogart, 2018). Det betyder att istället för att varje nod i nätverket behöver köra alla smarta kontrakt så räcker det med att de inblandade parterna gör det. Denna metod kallas "Scriptless scripts" och bygger på kryptografi med Schnorr-signaturer som är en föreslagen uppgradering till Bitcoin.[12] Därigenom kan blockkedjan användas som ett system för att verkställa smarta kontrakt utan att kontrakten behöver lagras i blockkedjan.

Ett viktigt och olöst problem i många tillämpningar av smarta kontrakt är hur sanningsenlig data från omvärlden utanför blockkedjan ska rapporteras till smarta kontrakt och blockkedjan på ett tillförlitligt sätt. Smarta kontrakt kan endast verkställas automatiskt baserat på data som rapporteras till dem, så det är av central betydelse att dessa data rapporteras sanningsenligt, säkert och korrekt genom vad som brukar kallas ett orakel. Om ett orakel rapporterar felaktiga data kan det resultera i kontraktet verkställs till förmån för fel part i kontraktet. Det finns förslag på olika sätt att mildra detta problem genom att säkerställa att de som agerar orakel inte vet något om de kontrakt som de rapporterar information till och att de rapporterar informationen med jämna mellanrum enligt ett förutbestämt schema så att de kan bygga upp ett rykte över tid om att rapportera korrekta uppgifter (Dryja, 2017). Smarta kontrakt som implementerar denna typ av orakel finns än så länge endast som konceptvalidering (Glasbergen, 2018).

[11] https://github.com/ethereum/wiki/wiki/White-Paper

[12] https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki

4.6 Smart egendom

Smart egendom är ett samlingsnamn för egendom vars ägande kontrolleras via smarta kontrakt på en blockkedja. Detta inkluderar digital egendom som kan representeras direkt genom blockkedjans interna valuta och smarta kontrakt, men kan även inkludera fysisk egendom, exempelvis fastigheter och bilar. Förslag finns presenterade för hur äganderegister av exempelvis fastigheter, bilar och andra fysiska ägodelar skulle kunna hanteras med blockkedjor (Mizrahi, 2015).

Lantmäteriet startade 2016 ett projekt tillsammans med Kairos Future, SBAB, Telia, Landshypotek bank, Chromaway, Skatteverket och Evry för att effektivisera fastighetstransaktioner med blockkedjeteknik och smarta kontrakt. Hur processen är tänkt att fungera förklaras i rapporten "Framtidens husköp i blockkedjan".[13] 2018 gjordes en demonstration av en riktig fastighetstransaktion som skedde med systemet där köpare, säljare, berörda banker och mäklare inför publik gick igenom transaktionsprocessen.[14]

Med blockkedjeteknik kan processen för fastighetstransaktioner och andra transaktioner av egendom effektiviseras genom digitalisering, full transparens för alla inblandade parter och genom att varje steg i processen registreras och signeras kryptografiskt av parterna. Eftersom fysisk egendom inte direkt kan överföras utan mellanhänder via blockkedjan så får istället ägarbeviset för ägandet av den fysiska egendomen hanteras på blockkedjan. Detta ägarbevis kan innehålla information om objektet, dess ägare, ägarhistorik, geografisk plats, eventuella skulder och betalningar. Enbart ett ägarbevis på blockkedjan är dock inte nog för att säkra ägandet av fysisk egendom utan det måste samtidigt finnas ett parallellt ihopkopplat register genom vilken den lagliga rätten till den fysiska egendomen kan regleras i den gällande jurisdiktionen, om inte lagar stiftas så att myndigheter erkänner en blockkedja som det auktoritära registret.

Faktisk kontroll och möjlighet att använda fysisk egendom skulle även i framtiden kunna regleras genom olika fysiska lås som gör egendomen, exempelvis en bil, obrukbar om den inte låses upp med digitala nycklar som kan hanteras av dess ägarbevis genom smarta kontrakt på en blockkedja.

4.7 Värdepapper

Blockkedjeteknik kan erbjuda ett effektivare alternativ till traditionell hantering av värdepapper. Med publika och privata blockkedjor är det möjligt att utfärda värdepapper och hantera transaktioner i dessa. Olika digitala tillgångar, exempelvis aktier, obligationer och fiatvalutor kan representeras genom att öronmärka enskilda

[13] Rapporten "Framtidens husköp i blockkedjan"
https://www.lantmateriet.se/contentassets/8d2b5d7647634c02a329b01e46e61071/blockkedjan_framtidens_huskop-2016.pdf

[14] https://computersweden.idg.se/2.2683/1.703915/lantmateriet-hus-blockchain

enheter av den interna valutan som tolkas av överliggande protokoll enligt olika standarder för färgade mynt (Se Kapitel 3.7.1). Eller så kan logik för utfärdande av nya tillgångar och transaktioner med dessa hanteras genom smarta kontrakt. Det vanligaste exemplet på det senare är i form av ERC-20 standarden på Ethereums blockkedja, som använts av de flesta ICO:s för att utfärda nya digitala tillgångar, som i många fall kan liknas vid att emittera aktier för en börsintroduktion (Se Kapitel 0).

Nasdaq började experimentera relativt tidigt med privata blockkedjor för att hantera värdepapper. 2015 lanserade Nasdaq plattformen Linq som ett test för att handla med onoterade aktier.[15] 2017 initierade Nasdaq ett samarbete med SEB för att digitalisera och effektivisera den svenska fondmarknaden med hjälp av deras blockkedjeplattform.[16]

I december 2015 gav U.S. Securities and Exchange Commission (SEC) företaget Overstock tillåtelse att ge ut aktier i det egna bolaget via en blockkedja (Metz m.fl., 2015). Ett dotterbolag till Overstock har sedan utvecklat en plattform för handel med reglerade blockkedjebaserade värdepapper.[17]

Fördelarna med att använda blockkedjeteknik för hantering av värdepapper är att det kan erbjuda omedelbar clearing och avveckling vilket annars kan ta flera dagar, involvera flera mellanhänder och innebära att banker och finansiella institut behöver reservera stora belopp i säkerhet under tiden transaktionerna behandlas. Automatiseringen som sker med introduktion av blockkedjeteknik vid handel av värdepapper minskar också mängden manuellt arbete och därmed minskar risken för fel orsakade av mänskliga faktorn. Värdepapper på blockkedjor kan även ge ökad transparens och insyn för marknadens aktörer och tillsynsmyndigheter vilket skulle kunna hjälpa till att bekämpa olika former av marknadsmissbruk, som exempelvis insider trading. Det skulle även kunna ge effektivare bolagsstyrning genom att underlätta ett mer aktivt engagemang från aktieägare, exempelvis röstning på distans vid bolagsstämmor.

Banker och finansiella institut kan emittera kryptovalutor knutna till värdet av nationella fiatvalutor för att därigenom få en kryptovaluta med ett stabilt värde jämfört med andra kryptovalutor vars värde flyter fritt mot de olika nationella fiatvalutorna. Dessa brukar kallas "Stable Coins". Det möjliggör ett snabbare och säkrare sätt att göra transaktioner där denna typ av kryptovaluta kan växlas till den nationella fiatvalutan som den är knuten till utan att värdet förändras över tid. JP Morgan lanserade i februari 2019 "JPM Coin", en kryptovaluta knuten till dollar, på deras privata blockkedja Quorum.[18] Ett antal Stable Coins knutna till dollar har lanserats tidigare. Den med högst omsättning, kallad Tether, lanserades 2014 i ett

[15] http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326

[16] https://sebgroup.com/press/news/seb-and-nasdaq-to-use-blockchain-in-mutual-funds

[17] https://www.tzero.com/

[18] https://www.jpmorgan.com/global/news/digital-coin-payments

lager ovanpå Bitcoins blockkedja av kryptovalutabörsen Bitfinex.[19] Ett antal olika Stable Coins med lägre omsättning har lanserats av olika finansiella institut baserade på Ethereums blockkedja.

En Security Token Offering (STO), är ett sätt att emittera värdepapper på publika blockkedjor i samarbete med regulatoriska myndigheter i vissa länder, som exempelvis USA (Bevilacqua m.fl., 2018). Vanligtvis utfärdas de med ERC-20 standarden på Ethereums blockkedja, det vill säga som en ICO. Skillnaden mellan en ICO och en STO är att en STO är reglerad och uppbackad av något konkret, exempelvis ett företags tillgångar, vinster eller intäkter, vilket inte en ICO behöver vara.

4.8 Kuponger, biljetter, medlemskort och nycklar

Med lager ovanpå publika blockkedjor (Se Kapitel 3.7) och via smarta kontrakt är det möjligt att utfärda digitala tillgångar som utöver värdepapper även kan fungera som exempelvis kuponger, biljetter, medlemskort eller nycklar.

Exempelvis skulle en butiksägare kunna utfärda kuponger, som ges ut i samband med köp, som sedan kan lösas tillbaka i butiken enligt utfärdarens uttalade villkor. En biograf skulle kunna utfärda digitala biljetter som gör det möjligt att utan mellanhänder enkelt och säkert köpa biljetter som garanterat inte är förfalskningar. Dataspelstillverkare kan skapa digitala tillgångar som fungerar som valuta eller olika föremål i ett eller flera olika dataspel som garanterat finns i en begränsad upplaga eller är unika (Jimenez, 2018).

Innehav av olika digitala tillgångar på en blockkedja kan även användas som medlemskort eller nycklar för att kontrollera åtkomst till både fysiska och digitala resurser utan behov av centraliserad infrastruktur eller anförtrodda tredjeparter. Digitala mynt på en blockkedja (eng. tokens) skulle kunna användas för att bygga system som kan ge olika nivåer av åtkomst till användare baserat på vilka mynt de äger. Exempelvis en hemsida skulle kunna visas på ett visst sätt för användare som äger ett mynt som ger åtkomst på en grundnivå och på ett helt annat sätt för användare som äger ett eller flera olika typer av mynt för att ge en högre nivå av åtkomst. Blockkedjor kan på detta sätt användas för granulär ”Token controlled access”.

[19] https://tether.to/

4.9 Decentraliserade plattformar

Idag sker handel på Internet genom mellanhänder i form av centraliserade företag. Även på plattformar som exempelvis Ebay.com, Blocket.se och Tradera.se, där privatpersoner kan köpa och sälja varor direkt till varandra, så tillhandahålls marknadsplatsen och infrastrukturen av ett centralt företag som kan censurera transaktioner, hållas juridiskt ansvarig och som kan stänga ned marknadsplatsen.

Med betalningar via kryptovalutor och smarta kontrakt är det möjligt att bygga applikationer för decentraliserad handel och koordinering mellan köpare och säljare utan mellanhänder. För att använda denna typ av tjänster behöver man endast ladda ned och installera en särskild applikation på sin dator eller mobil.

OpenBazaar är en peer-to-peer mjukvara med öppen källkod som skapar en decentraliserad handelsplats där vem som helst fritt kan annonsera varor och köpa varor med olika kryptovalutor.[20] Eftersom ingen äger, kontrollerar eller agerar mellanhand på plattformen tillkommer inga extra avgifter för köpare och säljare. Första versionen av OpenBazaar lanserades i april 2016 och har utvecklats vidare sedan dess.

Bisq är en peer-to-peer mjukvara med öppen källkod som skapar en decentraliserad valutabörs för växling mellan olika kryptovalutor och fiatvalutor.[21] Bisq lanserades i april 2016 under sitt ursprungliga namn Bitsquare. För att garantera säkerheten vid transaktioner används 2 av 3 multisignaturtransaktioner (Se Kapitel 3.4) och både köpare och säljare behöver lägga en säkerhetsdeposition som betalas tillbaka när transaktionen är slutförd. Skulle en tvist uppstå mellan köpare och säljare så finns det en inbyggd fri marknad för tvistlösare.

Augur är en peer-to-peer mjukvara med öppen källkod som skapar en decentraliserad prediktionsmarknad ovanpå Ethereums blockkedja genom en uppsättning av smarta kontrakt.[22] På en prediktionsmarknad kan individer satsa pengar på sannolikheten av framtida händelser vilket ger en mekanism för att ta tillvara människors vetskap och förutsägelser om framtiden på ett viktat sätt. Användare av Augur kan skapa nya marknader för vilka sorts händelser de vill, exempelvis politiska händelser, ekonomiska resultat och sportresultat. Augur lanserades i juli 2018.

En ytterligare form av tjänst som blockkedjeteknik kan bidra till att decentralisera är sociala nätverk och gemensamma bloggplattformar. Minds är ett decentraliserad socialt nätverk med öppen källkod som lanserades i juni 2015 för att erbjuda ett censurfritt och integritetsskyddat alternativ till Facebook.[23] Minds använder en intern valuta baserad på ERC-20 standarden på Ethereums blockkedja som kan

[20] https://openbazaar.org/

[21] https://bisq.network/

[22] https://www.augur.net/

[23] https://www.minds.com/

användas för olika tjänster på plattformen, exempelvis för att få mer publicitet för innehåll eller för att följa exklusivt innehåll som andra producerar. Steemit är en bloggplattform som lanserades i juli 2016 som är som ett mellanting mellan Medium och Reddit, där användare kan rösta upp och rösta ner andras artiklar för att göra dem mer eller mindre synliga, samt belöna dem med plattformens interna kryptovaluta.[24]

Dessa typer av decentraliserade tjänster, som blockkedjor och kryptovalutor möjliggör kan ge ökad ekonomisk frihet och yttrandefrihet globalt då det inte finns något centralt företag som tillhandahåller plattformen och som kan tvingas att följa regional lagstiftning och hållas juridiskt ansvarig för den verksamhet som dess användare ägnar sig åt.

4.10 Decentraliserad datalagring

Med blockkedjeteknik är det möjligt att skapa peer-to-peer applikationer för att lagra data distribuerat på ett stort antal datorer sammankopplade i ett nätverk och därmed kan enskilda anförtrodda tredjeparter och riskerna med centrala databaser undvikas. Blockkedjeteknik och betalningar via kryptovaluta kan göra det möjligt att skapa en effektiv marknad där vem som helst kan hyra ut oanvänt lagringsutrymme och få kontinuerlig betalning och vem som helst kan betala för att hyra distribuerat lagringsutrymme i nätverket.

Det som ska lagras i nätverket styckas först upp i bitar av lämplig storlek och krypteras innan det laddas upp med applikationens mjukvara. Applikationen innehåller en algoritm som beräknar hur alla bitar ska lagras distribuerat i nätverket på ett effektivt och tillräckligt redundant sätt för att garantera integriteten av data, så att varje användare alltid ska kunna få tillgång till de filer de laddat upp så länge de betalar för tjänsten.

Ett flertal projekt arbetar på att bygga denna typ av applikationer för distribuerad datalagring med öppen källkod. StorJ[25] och Sia[26] började utvecklas 2013, och Filecoin[27] började utvecklas 2014. Sia lanserade sin första publika applikation för decentraliserad lagring 2015 och har vidareutvecklats kontinuerligt sedan dess. StorJ finns än så länge endast tillgängligt som en publik alfaversion för testning och beräknas lanseras hösten 2019. Filecoin siktar också på lansering hösten 2019.

[24] https://steemit.com/

[25] https://storj.io/

[26] https://sia.tech/

[27] https://filecoin.io/

4.11 Elektronisk röstning

Traditionella valsystem med röstning via pappersblanketter och manuell mänsklig rösträkning är sårbara för valfusk, korruption och sabotage. Datoriserade röstningssystem är dock potentiellt ännu mer osäkra eftersom det inte går att garantera att inte någon dator i kedjan fram till att valresultatet presenteras har manipulerats (Rubin, 2002).

Estland var det första landet i världen som möjliggjorde elektronisk röstning över internet i allmänna val, först i ett kommunalval som ett pilotprojekt 2005 och sedan i riksdagsval från 2007, och de fortsätter att använda systemet trots att en hel del kritik riktats mot dess säkerhet (Springall m.fl., 2014).

Blockkedjeteknik har föreslagits som en teknisk lösning för säker elektronisk röstning samtidigt som valhemligheten kan bevaras (Lee m.fl., 2016). System baserade på blockkedjeteknik skulle i framtiden potentiellt kunna användas både vid politiska val och val inom företag och organisationer. Exempelvis aktieägare skulle kunna delta i omröstningar på distans i en bolagsstämma på ett säkrare sätt. Ett tillvägagångssätt är att en digital plånbok först skapas för varje kandidat eller valalternativ och att sedan varje röstberättigad person förses med ett unikt digitalt mynt i blockkedjans interna valuta som skickas till en digital plånbok som endast de har kontroll över. Röstningen sker sedan genom att varje röstberättigad person skickar sitt mynt till plånboken för den kandidat eller det valalternativ som de vill rösta på. Den kandidat eller det valalternativ som får flest digitala mynt vinner omröstningen. Varje person som röstat kan i denna process verifiera att deras röst är inräknad hos rätt kandidat eller rätt valalternativ i slutresultatet utan att de behöver avslöja för någon hur de röstade.

Ett hinder för bred adoptionen av sådana system är att alla röstberättigade måste kunna hantera en digital plånbok på ett säkert sätt. Det är viktigt att mjukvaran som systemet bygger på är öppen källkod så att säkerheten kan verifieras av oberoende parter och att en säker decentraliserad blockkedja används som grund så att inga parter kan manipulera resultatet.

4.12 Decentraliserade autonoma organisationer

De traditionella centrala organisationer, som genom historien varit nödvändiga för att organisera mänsklig samverkan och som den politiska makten använt för att utöva kontroll, kan genom blockkedjetekniken och smarta kontrakt få konkurrens av en organisationsform som kan bli svår att reglera och kontrollera av utomstående parter.

Bitcoin i sig själv kan ses som en decentraliserad autonom organisation med syftet att skapa en ny form av pengar i vilken alla som håller en andel av valutan är dess delägare. Delägarnas arbete för den decentraliserade autonoma organisationen belönas endast indirekt om det resulterar i att priset på bitcoin går upp. Genom publika blockkedjor som hanterar smarta kontrakt är det potentiellt möjligt att skapa andra former av decentraliserade autonoma organisationer i vilka människors och maskiners arbete kan organiseras och belönas genom regler definierade av smarta kontrakt. För att en decentraliserad autonom organisation ska fungera krävs det framför allt en fungerande incitamentsstruktur som gör att det ligger i varje delägares intresse att arbeta för organisationens ändamål.

I april 2016 lanserades vad som var tänkt att bli en ny form av decentraliserad autonom organisation som en uppsättning smarta kontrakt ovanpå Ethereums blockkedja, med namnet The DAO. I slutet av maj 2016 hade hela 14% av Ethereums interna valuta allokerats till The DAO med ett sammanlagt värde av över 150 miljoner dollar. The DAO skulle fungera som en sorts gemensam riskkapitalfond för nya projekt där deltagarna kunde rösta om hur resurser skulle allokeras och där det fanns inbyggda mekanismer för att belöna utvärderingar av föreslagna projekt. I juni 2016 utnyttjades en sårbarhet i programmeringskoden till The DAO vilket gjorde att en okänd användare kunde tömma kontraktet på en tredjedel av alla satsade pengar. Detta ledde strax därefter till att Ethereum genomgick en kontroversiell hard fork i syfte att återställa pengarna som tömts ur The DAO kontraktet, vilket ledde till att Ethereum-blockkedjan delades i två, där originalet fick namnet Ethereum Classic.

Flertalet ICO:s som lanserats med ERC-20-mynt på Ethereum skulle också kunna ses som decentraliserade autonoma organisationer. Det återstår dock att se om några av dem kommer att bli långsiktigt livskraftiga.

5 Adoption och konkurrens bland blockkedjor

Ny teknik i allmänhet och blockkedjeteknik i synnerhet är komplicerat att förstå och hantera. Blockkedjeteknikens användarvänlighet är ofta bristande, kräver tekniskt kunnande, säkerhetstänkande och är inte ännu moget för adoption av den breda allmänheten. Inlärningströskeln är hög för att förstå tekniken och för säker hantering av digitala tillgångar på blockkedjor via kryptonycklar.

Konkurrensen mellan blockkedjor kan ses som en evolutionär process med variation, replikering och selektion, där olika blockkedjors framgång kan mätas i hur många användare de har, och för publika blockkedjor värdet på deras interna valuta. Öppen källkod gör att både koden och blockkedjan hos befintliga system kan kopieras fritt och modifieras för att skapa nya konkurrenter.

Hur adoption av ny teknik generellt går till och vilken roll nätverkseffekter har är viktiga aspekter att behärska för att kunna förutsäga blockkedjeteknikens utveckling och olika blockkedjors konkurrenskraft. I egenskap av kommunikationssystem är nätverkseffekter av stor betydelse för blockkedjor.

5.1 Adoption av ny teknik

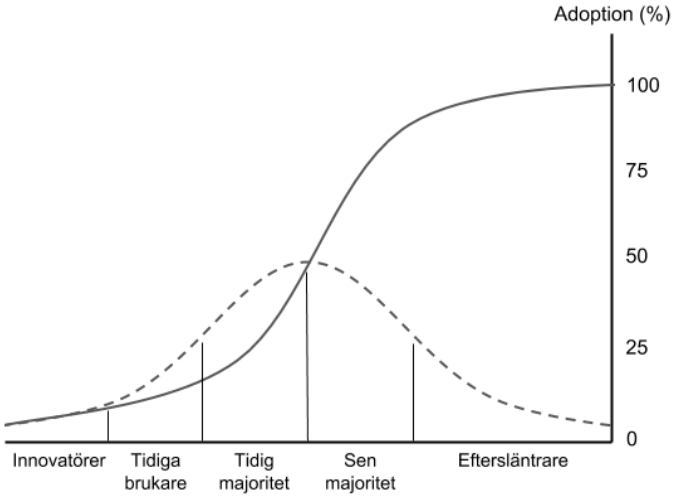
Hur nya idéer och tekniska innovationer sprids har studerats ingående av professor i kommunikationsvetenskap Everett M. Rogers. Han har skrivit boken "Diffusion of Innovations" som publicerats i olika utgåvor mellan 1962 och 2003 och som syntetiserar över 500 studier på området till en allmän teori (Rogers, 2003). Enligt Rogers sprids innovationer genom att de kommuniceras via olika kanaler mellan medlemmar i ett socialt system över tid.

Om en ny innovation införs och hur snabbt adoptionen sker beror på innovationens egenskaper och utmärkande drag. Rogers identifierar i huvudsak fem faktorer som avgörande:

1. Innovationens relativa fördelar i förhållande till tidigare system.
2. Innovationens kompatibilitet med människors sätt att tänka och agera.
3. Innovationens komplexitet och användarvänlighet.
4. Hur lätt innovationen är att få tillgång till och testa.
5. Hur synlig innovationens nytta är för potentiella nya användare.

Beroende på hur snabbt personer och organisationer tar till sig en viss innovation kan de enligt Rogers delas in i fem kategorier och karaktäriseras som innovatörer, tidiga brukare, tidig majoritet, sen majoritet eller eftersläntrare (Figur 10).

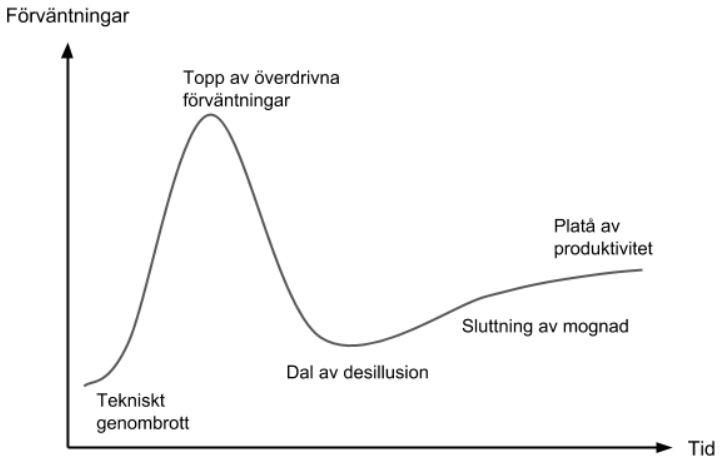
Figur 10



Spridning av innovationer

Vi tenderar ofta att överskatta effekterna av nya tekniska innovationer på kort sikt och underskatta effekterna på lång sikt. Många tekniska innovationer karaktäriseras av orealistiska förväntningar på ett tidigt plan när det i realiteten ofta krävs en lång process av utveckling, infrastruktur och anpassning innan en innovation är mogen för en bredare marknad. Ett sätt att illustrera denna dynamik är genom analytikerfirman Gartners hype-kurva (Figur 11).

Figur 11 Gartners hype-kurva som illustrerar dynamiken av förväntningar på innovationer

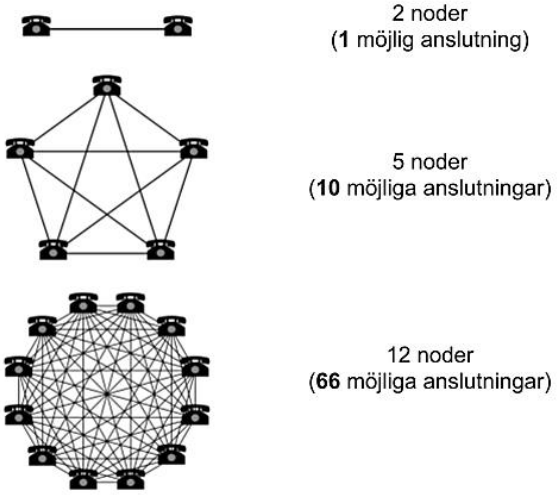


Många tekniska innovationer, exempelvis VR, AI, taligenkänning, 3D-printing och molntjänster har startat med ett tekniskt genombrott som snabbt blivit en hype där vad som kommuniceras om teknikens möjligheter överdrivs och visar sig ta betydligt längre tid att realiseras än utlovat av teknikens tidiga förespråkare. Blockkedjeteknikens utveckling kommer förmodligen att följa detta mönster. Min bedömning är att blockkedjeteknik generellt är i ett tidigt stadium, strax efter, men nära toppen av överdrivna förväntningar, och i Rogers ”Innovatörer”-fas gällande adoption. Bitcoin befinner sig möjligen i början av sluttningen av mognad, men fortfarande i Rogers ”Innovatörer”-fas gällande adoption.

5.2 Nätverkseffekter

Nätverkseffekter spelar stor roll i alla former av kommunikationssystem (Katz & Shapiro, 1994). Nätverkseffekter i detta sammanhang innebär att värdet av en tjänst eller produkt ökar i takt med antalet användare. Ett pengasystem precis som telefoner, faxmaskiner, eller Facebook och andra sociala nätverk är starkt påverkade av nätverkseffekter. Det beror på att den teoretiska nyttan för alla användare i kommunikationsnätverk växer asymptotiskt mot kvadraten av antalet användare i relation till tillväxten av antalet möjliga interaktioner (Figur 12). Detta samband är uppkallat efter Robert Metcalfe som var en av meduppfinnarna till Ethernet och brukar benämnas Metcalfe 's lag (Metcalfe, 2013).

Figur 12 Illustration av Metcalfe’s lag



En blockkedja är ett kommunikationsprotokoll. Ett precist definierat språk för att kommunicera värde över internet. Det kan ses som ännu ett i raden av internetprotokoll i likhet med exempelvis SMTP-protokollet för att skicka e-post på internet och TCP/IP som är det språk datorer använder för att kommunicera mellan varandra för att skapa själva internet.

När Bitcoin-blockkedjan först startades i januari 2009 hade dess interna valuta, bitcoin, inget värde alls. Den interna valutan fick ett värde i samma stund som en första individ satte ett subjektivt värde på den. Sedan har värdet växt i takt med att fler individer gjort egna subjektiva värderingar. En av de första kända transaktionerna som tillskrev bitcoin ett värde initierades drygt ett år efter att nätverket startade på forumet bitcointalk.org. I maj 2010 erbjöd Laszlo Hanyecz från Florida att betala 10 000 bitcoin för två pizzor.[28] Priset på bitcoin har sedan ökat i takt med att antalet användare växt år för år vilket ökat efterfrågan på ett begränsat utbud. I februari 2018 gjorde Laszlo Hanyecz ett nytt köp av två pizzor för bitcoin och priset blev då 0,00649 bitcoin.[29]

Med publika blockkedjor kan fördelarna med ökad adoption samt byggandet av nya applikationer och infrastruktur som använder sig av blockkedjan delas direkt mellan alla dess användare genom att det ökar värdet av den interna valutan, vilket ger incitament till användare och utvecklare att investera tid och resurser för att förbättra blockkedjan och dess samspelande infrastruktur.

5.3 Nätverkseffekters roll vid konkurrens mellan blockkedjor

Olika kryptovalutor och publika blockkedjor som exempelvis Bitcoin, Litecoin, Monero och Ethereum kan ses som konkurrenter till varandra på samma sätt som dollar kan ses som en konkurrent till euro, engelska som en konkurrent till spanska och Facebook som en konkurrent till Twitter. Viktiga aspekter för nätverkseffekterna och konkurrenskraften för kryptovalutor är öppen källkod, infrastruktur i form av mjukvara och hårdvara, tidig spekulation, långsiktiga investerare, samt tillväxten av utbildningsmaterial och personer med specialistkompetens.

Öppen källkod och utveckling genom frivillig kollaboration är en viktig aspekt för nätverkseffekterna och konkurrenskraften för publika blockkedjor och kryptovalutor. Det gör det möjligt för alla som vill delta i utvecklingen och bygga interagerande applikationer utan att fråga någon om lov. Det betyder även att olika kryptovalutor och blockkedjor fritt kan använda olika komponenter från sina konkurrenter då det inte finns några patent eller immateriella rättigheter som kan utgöra artificiella hinder. Säkerheten för protokollen förbättras och härdas med tiden och processen för utveckling av mjukvaran förbättras i takt med att fler blir involverade och mer rigorösa rutiner implementeras för peer-review och tester av nya versioner av mjukvaran innan de släpps.

[28] https://bitcointalk.org/index.php?topic=137.0

[29] http://fortune.com/2018/02/26/laszlo-hanyecz-pizza-bitcoin/

All infrastruktur som byggs upp över tid i form av olika former av mjukvara och hårdvara som interagerar och baseras på en viss blockkedja, samt företag och samarbeten, är avgörande för olika blockkedjors nätverkseffekter och konkurrenskraft. Samt den ackumulerade säkerheten som ges genom att mer beräkningskraft används för Proof-of-work för en blockkedja och att allt mer specialiserad hårdvara för Proof-of-work utvecklas.

En viktig nätverkseffekt för kryptovalutor, som vanligtvis inte finns i andra former av kommunikationsnätverk, är den interna valutans funktion och den prisökning som sker genom köp av spekulanter och långsiktiga investerare. Den inbyggda valutan ger ett finansiellt incitament för användare och utvecklare att att stödja nätverket på ett tidigt plan även då användbarheten fortfarande är låg (Dixon, 2017). Nätverkseffekterna från valutan gör att alla användare får incitament att arbeta mot ett gemensamt mål genom att ökad nytta och tillväxt av användare i nätverket ger värdeökning av valutan. Värdeökningen är även viktig för säkerheten i systemet genom att den betalar för den beräkningskraft som miners bidrar med och den ökade säkerheten kan leda till en ökad legitimitet. Ett ökande pris kan även locka nya personer att undersöka vad det är för fenomen som ligger bakom prisökningen och få dem att läsa på om tekniken och kanske bli intresserade.

Ackumulering av utbildningsmaterial som skapas med tiden av olika användare i form av böcker, kurser, dokumentärer, artiklar, forumposter, podcasts och videomaterial är en annan viktig nätverkseffekt. Fler personer som lär sig om hur systemet fungerar leder till en växande skara av entusiaster, lärare och konsulter, samt programmerare, datavetare, kryptografiexperter och forskare som ägnar sig åt blockkedjeteknik. Det leder även till fler möten, konferenser och workshops där personer kan lära sig mer om tekniken och nätverka.

Alla dessa olika nätverkseffekter samspelar och bidrar till olika blockkedjors konkurrenskraft som byggs upp över tid. Publika decentraliserade blockkedjor kan samtidigt ha en konkurrensnackdel mot mer centraliserade alternativ eftersom det inte finns något enskilt företag som äger systemet och har oproportionerligt mycket att vinna på att marknadsföra det, vilket kan leda till långsammare tillväxt på kort sikt. Om inte kapaciteten för transaktioner i en blockkedja ökar i takt med efterfrågan från dess användare så kan det även ge negativa nätverkseffekter genom att transaktioner blir dyrare att utföra eller tar längre tid innan de inkluderas i blockkedjan.

5.4 Konkurrens mellan valutor

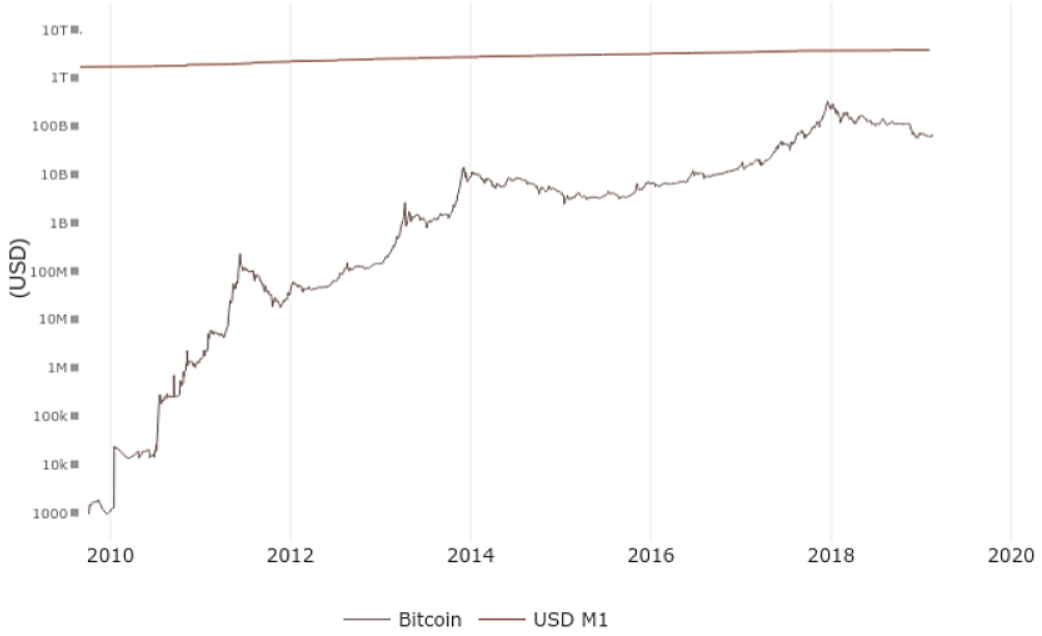
Nationella fiatvalutor har mer eller mindre monopol inom respektive lands gränser. Det innebär att kvaliteten på pengar inte kan förväntas vara så hög som den skulle kunna vara under en fri konkurrens. Detta gäller dock inte kryptovalutor som är en central del av publika blockkedjor och som alla konkurrerar med varandra på ett globalt plan och i växande utsträckning även med fiatvalutor och andra investeringsformer.

Vid konkurrens mellan olika former av pengar kan deras konkurrenskraft förväntas baseras primärt på hur väl de uppfyller funktionen som pengar (Šurda, 2012). Pengars tre viktigaste funktioner är att fungera som lagring av värde, som ett bytesmedel och som ett mått på värde (Jevons, 1875). För att kunna uppfylla dessa tre funktioner så väl som möjligt behöver de ha en begränsad mängd, vara hållbara över tid, vara enkla att förflytta och förvara, vara lätta att identifiera och svåra att förfalska, vara enkla att dela upp i mindre värden och varje enhet av valutan behöver vara utbytbar och vara lika mycket värd som varje annan enhet av valutan (dvs. vara fungibel), samt ha en utbredd användning (Camera, 2017).

Kryptovalutor har även nya monetära egenskaper som inte traditionella valutor har. De kan programmeras genom smarta kontrakt vilket gör att vissa typer av kontrakt kan ingås utan den motpartsrisk som vanliga kontrakt innebär. Kryptovalutor kan skickas över elektroniska kanaler utan mellanhänder och kryptovalutor gör det möjligt att förvara värde som ren information i form en privat kryptonyckel, vilket minskar behovet av anförtrodda tredjeparter vid transaktioner och förvaring av pengar.

Värdet av den totala penningmängden av Bitcoin, som är den klart största kryptovalutan, var i februari 2019 ca 60 miljarder dollar vilket motsvarar ca 1,6% av värdet av penningmängden av amerikanska dollar i måttet M1 (kontanter samt avistainlåning), som i februari 2019 var ca 3750 miljarder dollar (Figur 13).

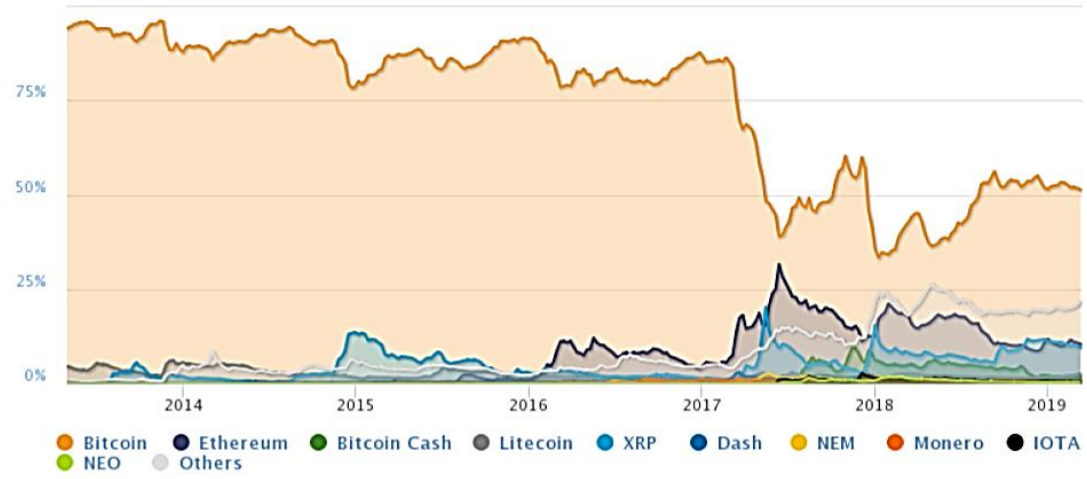
Figur 13 Värdet av den totala penningmängden av Bitcoin jämfört med amerikanska dollar (M1) Källa:



http://charts.woobull.com/bitcoin-money-supply/

Marknadsandelen av Bitcoin i förhållande till andra kryptovalutor har sjunkit senaste åren och var i februari 2019 strax över 50% och har som lägst historiskt varit nere på 34% (Figur 14) Det bör dock påpekas att marknadsvärde (antal mynt * pris/mynt) för en kryptovaluta är ett dåligt jämförelsemått då det är lätt att manipulera för kryptovalutor med låg omsättning och därför kan ge en missvisande bild (Demeester, Blummer, & Lescrauwaet, 2019).

Figur 14 Marknadsandel av Bitcoin i förhållande till andra kryptovalutor



Källa: https://coinmarketcap.com/charts/

På kort sikt påverkas konkurrensen mellan kryptovalutor till stor del av spekulation och marknadsföring, men på lång sikt så borde stabilitet, säkerhet och hur väl de uppfyller funktionen som pengar vara avgörande. Kryptovalutor anses idag generellt vara långt ifrån att kunna uppfylla pengars tre standardfunktioner, inte minst på grund av hög volatilitet. Men om kryptovalutor fortsätter att växa och utvecklas i den takt som de har gjort hittills kan de potentiellt om ett antal bli ett konkurrenskraftigt alternativ till allt fler nationella valutor och därmed potentiellt påverka centralbankers förmåga att styra penningpolitiken och kontrollera räntan i länder med svaga valutor. Nationella valutor har en stor konkurrensfördel till följd av överlägset utbredd användning och alla nätverkseffekter det ger, men dessa riskerar att långsamt eroderas genom negativa räntor, monetär inflation, ökande regulatorisk friktion och ökande instabilitet till följd av en allmän skuldtillväxt.

6 Konkurrens, tillsyns och regulatoriska perspektiv på blockkedjeteknik

6.1 Konkurrenslagstiftningens historia och syfte

Konkurrenslagstiftning syftar till att säkerställa en välfungerande konkurrens mellan företag för att gynna konsumenter genom lägre priser, högre kvalitet och ett bredare urval av varor och tjänster. Regleringarna på området innefattar konkurrensbegränsande samarbeten mellan företag, missbruk av dominerande ställning och sammanslagningar av företag som gör att en dominerande ställning skapas eller förstärks.

Modern konkurrenslagstiftning har sin början med "Sherman Antitrust Act" 1890 som var den första federala konkurrenslagstiftningen i USA, samt en liknande lag "The Act for the Prevention and Suppression of Combinations formed in restraint of Trade 1889", som stiftades i Kanada ett år tidigare. "Sherman Antitrust Act" förbjöd kontrakt, sammanslagningar av företag och konspirationer som hindrar handel, samt förbjöd monopol och försök att upprätta monopol.

En "Trust" var ett förvaltningsbolag där aktieägare i olika bolag överförde sina aktier till en gemensam styrelse av förvaltare som centralt tillsatte direktörer och tjänstemän i alla de gemensamt förvaltade bolagen, samt förvaltade vinsten för alla ingående bolag och delade ut den till aktieägarna. Lagarnas syfte var att upplösa denna typ av gemensam förvaltning av olika bolag vilket ansågs sätta konkurrensen ur spel.

1914 utökades konkurrenslagstiftningen i USA med "Clayton Antitrust Act" som specificerar ett antal otillåtna beteenden, bland annat prisdiskriminering, villkorad försäljning under krav att köparen inte handlar från konkurrenter, eller att kunden samtidigt måste köpa en annan vara, samt krav på notifiering inför sammanslagningar av företag över en viss storlek infördes. "Clayton Antitrust Act" gav också specifikt tillåtelse för fackföreningar, vilka hade tolkats som olagliga under "Sherman Antitrust Act". Samtidigt skapades "Federal Trade Commission" med uppdrag att överse att konkurrenslagarna följdes och att skydda konsumenter.

1923 blev Tyskland det första landet i Europa som införde en konkurrenslagstiftning vilket innebar att karteller behövde registreras hos myndigheterna, men 1933 ersattes den av en lag som gjorde karteller obligatoriska och under finansministeriets kontroll (Quack & Djelic, 2003).

1925 får Sverige sin första konkurrenslagstiftning som gav myndigheterna rätt att undersöka företag med dominerande ställning. 1946 införs lagen om övervakning av konkurrensbegränsning inom näringslivet där företagare på begäran av övervakningsmyndigheten blev skyldiga att rapportera ingångna kartellavtal eller

andra liknande konkurrensbegränsande överenskommelser. 1953 kom konkurrensbegränsningslagen som innehöll straffsanktionerade förbud mot bruttoprissättning och anbudskarteller. Dessutom bildades Näringsfrihetsombudsmannen med uppgift att förhandla bort skadliga konkurrensbegränsningar, samt Näringsfrihetsrådet som sedan omvandlades till Marknadsdomstolen. 1956 uppdaterades 1946 års lagstiftning med krav på uppgiftsskyldighet för pris och konkurrensförhållanden. Statens Pris- och Kartellnämnd (SPK) bildades som fick till uppgift att utreda hur konkurrensen fungerade i olika branscher. 1982 kom en ny konkurrenslag som gav myndigheter ökade befogenheter att motverka företags konkurrensbegränsande åtgärder, exempelvis prissamverkan, marknadsdelning och prisdiskriminering, samt regler för att kunna ingripa mot särskilt skadliga företagsförvärv infördes. 1988 ändrade Statens Pris- och Kartellnämnd namn till Statens Pris- och Konkurrensverk.

1992 inrättades Konkurrensverket som ersatte Statens Pris- och Konkurrensverk samt Näringsfrihetsombudsmannen. 1993 kom en ny skärpt konkurrenslag som inte skiljer sig mycket från nu gällande konkurrenslagstiftning. 2004 och 2008 skedde uppdateringar av lagen för att harmoniera med EU:s konkurrenslagstiftning, i vilken förbjudna samarbeten mellan företag regleras i artikel 101, missbruk av dominerande ställning i artikel 102 och företagskoncentrationer i Rådets förordning (EG) nr 139/2004.

I nu gällande svensk konkurrenslag (2008:579) regleras konkurrensbegränsande samarbeten mellan företag och företags missbruk av en dominerande ställning i kapitel 2. Den huvudsakliga ordalydelsen gällande dessa är följande:

> ***2 Kap. 1 § Konkurrenslag (2008:579)***
> *Sådana avtal mellan företag som har till syfte eller resultat att hindra, begränsa eller snedvrida konkurrensen på marknaden på ett märkbart sätt är förbjudna, om inte annat följer av denna lag.*
>
> *Detta gäller särskilt sådana avtal som innebär att*
>
> *1. inköps- eller försäljningspriser eller andra affärsvillkor direkt eller indirekt fastställs,*
>
> *2. produktion, marknader, teknisk utveckling eller investeringar begränsas eller kontrolleras,*
>
> *3. marknader eller inköpskällor delas upp,*
>
> *4. olika villkor tillämpas för likvärdiga transaktioner, varigenom vissa handelspartner får en konkurrensnackdel, eller*
>
> *5. det ställs som villkor för att ingå ett avtal att den andra parten åtar sig ytterligare förpliktelser som varken till sin natur eller enligt handelsbruk har något samband med föremålet för avtalet.*

2 Kap. 7 § Konkurrenslag (2008:579)
Missbruk från ett eller flera företags sida av en dominerande ställning på marknaden är förbjudet.

Sådant missbruk kan särskilt bestå i att

1. direkt eller indirekt påtvinga någon oskäliga inköps- eller försäljningspriser eller andra oskäliga affärsvillkor,

2. begränsa produktion, marknader eller teknisk utveckling till nackdel för konsumenterna,

3. tillämpa olika villkor för likvärdiga transaktioner, varigenom vissa handelspartner får en konkurrensnackdel, eller

4. ställa som villkor för att ingå ett avtal att den andra parten åtar sig ytterligare förpliktelser som varken till sin natur eller enligt handelsbruk har något samband med föremålet för avtalet.

6.2 Blockkedjeteknik ur ett regulatoriskt perspektiv

Teknisk utveckling och nya sätt att utföra tjänster kan utmana rådande regleringsstrukturer. Ett exempel på detta är Skype som 2003 lanserade IP-telefoni till en global marknad av konsumenter. Skype hävdade att de endast utvecklat en mjukvara som de släppt till användare och att de därmed inte var ett telekommunikationsföretag enligt rådande regleringar och därför inte borde regleras som ett sådant (Jackson, 2014). Skype menade att när deras användare körde mjukvaran så skapades ett peer-to-peer nätverk mellan dem som är oberoende av företaget som skapat mjukvaran. Ett liknande exempel är företaget Uber som hävdar att de är ett mjukvaruföretag och inte ett taxiföretag och därför inte bör falla under den reglering som gäller taxiverksamhet.

Ett liknande resonemang kan föras för Bitcoin och andra publika blockkedjor, men här finns inte något enskilt företag som utvecklat mjukvaran, utan endast frivilliga deltagare från olika delar av världen. Blockkedjeteknik som bygger på publika kommunikationsprotokoll med öppen källkod är svår att reglera på grund av sin decentraliserade natur utan någon enskild ägare eller central infrastruktur i någon enskild jurisdiktion. Det som däremot kan regleras är företag som på olika sätt interagerar med blockkedjor.

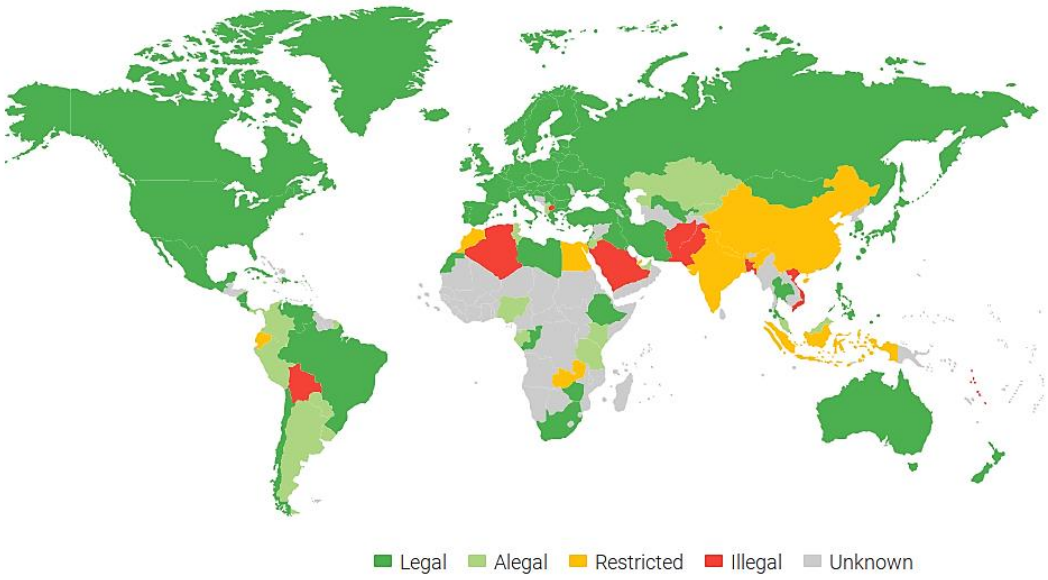
Blockkedjeteknik kan även ses från ett annat perspektiv. Ett kommunikationsprotokoll består av en samling av specifika regler för hur meddelanden tas emot och skickas. Det fungerar som ett språk för kommunikation mellan datorer i ett nätverk. Ur detta perspektiv kan olika användningsområden av blockkedjeteknik såsom Bitcoin ses som strikt reglerade genom reglerna i protokollet. Det enda sättet att delta i nätverket är att strikt följa protokollets regler för att kunna kommunicera i det exakta språket som gäller i nätverket. Decentraliserade blockkedjor är reglerade genom programkod istället för genom traditionella mänskliga politiska och juridiska institutioner.

Kryptovalutors och blockkedjetekniks decentraliserade natur och grund i fri mjukvara är svår att placera under rådande regleringar av exempelvis valutor, finansiella instrument och finansiella institutioner eftersom de inte har någon enskild skapare, ägare, utgivare eller geografisk hemvist. Då blockkedjeteknik är en generell ny teknik som kan användas för olika tillämpningar kan det vara bättre för myndigheter att tydliggöra hur redan rådande lagstiftning ska tolkas gällande specifika tillämpningar av blockkedjeteknik. Detta skulle även implicera att rådande lagstiftning gäller för tillämpningar som redan regleras av lagar trots att de tillhandahålls på nya sätt genom ny teknik som inte följer gamla strukturer och antaganden.

6.3 Historik över regleringar av blockkedjor i världen

De regleringar som tillämpats av olika länder har framförallt handlat om Bitcoin och dess roll som en alternativ valuta. Bitcoin och kryptovalutor är lagliga i de flesta länder med ett fåtal undantag (Figur 15). De länder där Bitcoin och kryptovalutor är förbjudna officiellt är Algeriet, Bangladesh, Bolivia, Marocko, Nepal, Nordmakedonien, Pakistan, och Vietnam.

Figur 15 Laglig status för Bitcoin i olika länder i mars 2019



Källa: https://coin.dance/poli#legalitymap

2012 publicerade europeiska centralbanken en rapport där de klassificerade virtuella valutorna i tre olika kategorier baserat på om de inte har någon kontakt, enriktad handel eller dubbelriktad handel med det övriga ekonomiska systemet (ECB, 2012). I rapporten konstaterade de att direktiv (2009/110/EC) gällande elektroniska valutor och direktiv (2007/64/EC) om betaltjänster inte kan tillämpas på Bitcoin och andra kryptovalutor eftersom de saknar ansvarig utgivare och inte ges ut som en fordran på en utgivare.

2013 klassificerades Bitcoin i Tyskland som en typ av privata pengar och därför ska kapitalvinstskatt betalas för bitcoin som säljs inom ett år. Finland gav ut vägledning kring regleringen av Bitcoin samma år med krav på kapitalvinstskatt samt att inkomst från mining räknades som inkomst av näringsverksamhet. Svenska skatteverket gav vägledning kring Bitcoin 2014 och tolkade det som en sorts kapitalinvestering med krav på kapitalvinstskatt.[30] Finansinspektionen hade dock ansett att Bitcoin var ett betalningsmedel sedan 2012 och krävt att företag som handlar med Bitcoin registrerar sig och följer lagar kring penningtvätt.[31] Runt 2013 och 2014 var det sammanlagt ett trettiotal länder som gav vägledning kring Bitcoin och vilka skatter som gällde. Få länder meddelade någon avsikt att vilja förbjuda kryptovalutor.

I mars 2013 gavs den första regulatoriska vägledningen ut i USA av Financial Crimes Enforcement Network (FinCen) där Bitcoin och andra kryptovalutor klassificerades som virtuella valutor.[32] Enligt FinCen kunde inte privatpersoner som växlar mellan nationell valuta och virtuell valuta anses syssla med utländsk valutaväxling och därför var inte "Bank Secrecy Act" tillämplig. Däremot ansågs det att personer som bedrivit mining av kryptovalutor och sålt förtjänsten för fiatvaluta skulle regleras som "Money Transmitters". FinCen ansåg även att amerikanska företag som ägnade sig åt betalningsförmedling eller valutaväxling med kryptovalutor skulle behöva samla in information om deras kunder, rapportera misstänkt aktivitet och följa regleringar kring penningtvätt i likhet med traditionella finansiella institutioner.

I december 2013 meddelade Kinas centralbank att banker och finansiella institut i landet var förbjudna att hantera kryptovalutor, men landets privatpersoner var fortfarande fria att köpa och sälja kryptovalutor.[33]

I juni 2015 lanserade New York State Department ett licensieringsprogram som krav för företag som ville erbjuda tjänster involverande kryptovalutor inom delstaten eller riktat till delstatens invånare.

I oktober 2015 fattade EU-domstolen beslut om att moms inte ska betalas vid växling mellan virtuell valuta och fiatvaluta som svar på en rättslig tvist där svenska skatteverket bett om ett förhandsbesked av EU-domstolen. Beskedet blev att Bitcoin var undantagen från moms och är att betrakta som ett betalningsmedel då det primärt används på motsvarande sätt som lagliga betalningsmedel.

---

[30] https://www.bitcoin.se/articles/skatteverket-om-kapitalvinstbeskattning-av-bitcoin

[31] https://www.svd.se/fi-ser-penningtvattrisk-med-bitcoin

[32] https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[33] https://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html

Leverantörer som erbjuder växlingstjänster mellan virtuella valutor och fiatvalutor, samt tillhandahållare av plånböcker för virtuella valutor inkluderas i EU:s femte penningtvättsdirektiv (5AMLD) (EU) 2018/843 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism.[34] Direktivet ska vara infört som lag i EU:s medlemsländer senast i januari 2020. Där uttrycks även en önskan om att behöriga myndigheter, genom ansvariga enheter, ska kunna övervaka användningen av virtuella valutor samt kunna erhålla information som gör det möjligt för dem att knyta virtuella valutaadresser till en virtuell valutas ägare. Senast i januari 2022 ska kommissionen utarbeta en rapport om genomförandet av direktivet och lägga fram den för Europaparlamentet och rådet. Rapporten ska sedan vid behov åtföljas av lämpliga lagstiftningsförslag. Där det är lämpligt ska det avseende virtuella valutor ges befogenhet till finansunderrättelseenheter att upprätta och underhålla en central databas för registrering av användarnas identitet, plånboksadresser, samt ges möjlighet till självdeklaration.

Dataskyddsförordningen (GDPR) (EU) 2016/679 som började gälla i maj 2018 syftar till att ge fysiska personer kontroll över hur deras personuppgifter lagras och behandlas. Denna lag kan få konsekvenser för hur företag, organisationer och myndigheter kan använda sig av blockkedjeteknik. Lagen reglerar hur företag och andra organisationer som verkar inom Europeiska unionen och övriga EES får behandla och lagra personuppgifter. Den innehåller bland annat krav på samtycke för att företag och organisationer ska ha rätt att lagra personuppgifter och dessa ska endast lagras under den tid som är nödvändig samt kunna tas bort ur register och databaser på begäran. Att lagra personuppgifter i en blockkedja där data inte kan ändras i efterhand verkar stå i konflikt med denna lag (Finck, 2017). Denna typ av lagar gällande dataskydd skulle kunna utgöra ett hinder för företag och organisationer att använda blockkedjeteknik för tillämpningar som innefattar lagring av personuppgifter (Brandman & Thampapillai, 2016).

USA:s kongressbiblioteks "Global Legal Research Directorate" publicerade en omfattande rapport i juni 2018 som dokumenterar regleringen av kryptovalutor i 130 länder som utfärdat lagar eller direktiv på området (Law Library of Congress, 2018). Bland de vanligaste åtgärderna är offentliga meddelanden för att informera om riskerna med att investera i kryptovalutor och för att informera om skillnaden mellan kryptovalutor och valutor som utfärdas och garanteras av staten. Ett 30-tal länder har direktiv om hur kryptovalutor ska hanteras skattemässigt respektive hanteras för att förhindra penningtvätt och finansiering av terrorism.

Vissa länder har arbetat för att profilera sig som särskilt välkomnande jurisdiktioner för blockkedjeföretag, exempelvis Gibraltar, Hong Kong, Kanada, Luxemburg, Malta, Schweiz, Singapore samt delstaten Wyoming i USA. Maltas regering lanserade en särskild myndighet för digital innovation i februari 2018 i syfte att ge klarhet till företag som utvecklar blockkedjeteknik och hanterar kryptovalutor.

---

[34] (EU) 2018/843 av den 30 maj 2018 om ändring av direktiv (EU) 2015/849 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32018L0843

Wyoming har antagit hela 13 nya lagar för att erbjuda en välkomnande jurisdiktion och regulatorisk klarhet för företag med verksamhet inom olika aspekter av blockkedjeteknik och för att främja privat ägande och handel med tillgångar på blockkedjor (Long, 2019).

6.4 Risker för konkurrenshämmande verksamhet med blockkedjeteknik

Generellt borde transaktioner som sker genom blockkedjor innebära lägre risk för konkurrenshämmande aktiviteter till följd av ökad transparens enligt Schrepel (2018). Blockkedjeteknik kan även ha möjlighet att förbättra konkurrensen på marknader som idag är dominerade av stora digitala plattformar, som exempelvis Google, Facebook och Amazon (Catalini & Tucker, 2018; Lianos, 2018).

Digitala plattformar har skaffat sig starka marknadspositioner genom att agera mellanhand i informationsutbyte mellan användare och i transaktioner mellan köpare och säljare (Milnes, 2016). Det gör att företagen som driver de digitala plattformarna kan få ett stort informationsövertag över de andra aktörerna på marknaden och kan utnyttja informationsasymmetrier för att stärka sin egen position.

System baserade på blockkedjeteknik, där alla parter har likvärdig tillgång till information om transaktioner i marknaden och inget enskilt företag äger informationen, skulle kunna jämna ut villkoren och förbättra konkurrensen. Vid användning av blockkedjeteknik behöver inte fördelarna av nätverkseffekter leda till koncentrerat marknadsinflytande för enskilda företag. Blockkedjeteknik skulle genom möjligheten att bygga decentraliserade plattformar för handel och informationsutbyte kunna användas för att överbrygga de koordinationsproblem som annars leder till att nätverkseffekter blir en källa till marknadsinflytande och kan ge en dominerande ställning för enskilda företag (Catalini & Gans, 2016).

Publika blockkedjor kan ses som en ny decentraliserad institution som löser koordineringsproblem och som har möjlighet att sänka transaktionskostnader mellan marknadens aktörer (Davidson, Filippi, & Potts, 2018). Publika blockkedjor kan som en ny sorts ekonomisk institution komplettera och konkurrera med andra institutioner, vilket inkluderar företag, marknader och myndigheter, genom att ge säker äganderätt, underlätta transaktioner och tillhandahålla en plattform för att ingå och genomdriva kontrakt (Berg, Davidson, & Potts, 2018).

Med publika blockkedjor kan fördelarna med ökad adoption samt tillväxt av nya applikationer och infrastruktur som använder sig av blockkedjan delas mellan alla dess användare. Publika blockkedjor med interna valutor ger även incitament till tidiga användare och utvecklare att investera tid och resurser för att förbättra blockkedjan och dess samspelande infrastruktur för att attrahera fler användare.

Blockkedjeteknik kan även göra det betydligt enklare för användare att röra sig mellan olika plattformar och använda flera samtidigt. Med publika blockkedjor som använder interna valutor är det enkelt att växla tillgångar på en blockkedja till tillgångar på en annan blockkedja utan inlåsningseffekter. Plånböcker och annan infrastruktur för hantering av tillgångar på blockkedjor har även ofta stöd för tillgångar på flera olika blockkedjor.

Publika blockkedjor är genom minimala marknadshinder utsatta för konstant konkurrens både av andra publika blockkedjor och av en ständig potentiell konkurrens genom möjligheten att förgrenas genom en hard fork, om en andel av dess användare inte känner att blockkedjan levererar maximal nytta och utvecklas i rätt riktning (Se Kapitel 3.5.2).

6.4.1 Blockkedjesamarbeten mellan företag

Det är vanligt att olika företag samarbetar i utvecklingen av blockkedjeteknik. Enligt en rapport från Deloitte fanns det i augusti 2017 över 40 olika konsortium av företag som bildats i syfte att utveckla och implementera blockkedjeteknik (Gratzke, Schatsky, & Piscini, 2017). Beroende på hur en blockkedja implementeras som används gemensamt av konkurrerande företag inom ett konsortium, så kan det uppstå oro för att konkurrenshämmande verksamhet kan underlättas (Kully & Dewey, 2017). Deltagare inom blockkedje-konsortier bör framförallt se till att inte dela information som kan uppfattas kunna begränsa oberoende beslutsfattande när det gäller vilka priser de tar ut för sina produkter (Kully & Dewey, 2017). Samarbeten inom ett konsortium bör inte innehålla regler som oskäligt begränsar konkurrensen mellan dess deltagare (Breu, 2017).

Samarbeten mellan företag inom blockkedjeteknik kan dels handla om gemensam forskning och utveckling och dels handla om att etablera gemensamma standarder för att säkerställa interoperabilitet. Samarbeten mellan företag för forskning och utveckling är endast problematiskt ur konkurrenssynpunkt om företagen är konkurrenter till varandra och de tillsammans har en betydande marknadsandel. Enligt EU:s konkurrenslagstiftning artikel 101(3) finns gruppundantag för forsknings- och utvecklingsavtal om de inblandade företagen inte tillsammans har mer än 25% marknadsandel på någon relevant produkt- eller teknikmarknad.[35] För att undantaget ska gälla krävs det att avtalet föreskriver att alla parter ska ha fullständig tillgång till de slutliga resultaten från den gemensamma forskningen och utvecklingen, inklusive immateriella rättigheter och sakkunskap som uppstår.

För standardiseringssamarbeten har EU-kommissionen satt upp en så kallad "safe harbor" under förutsättning att vissa villkor uppfylls. Deltagandet i standardiseringsarbetet behöver vara öppet för alla, följa en transparent process och det får

[35] (EU) nr 1217/2010 av den 14 december 2010 om tillämpningen av artikel 101.3 i fördraget om Europeiska unionens funktionssätt på vissa grupper av forsknings- och utvecklingsavtal https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX:32010R1217

inte finnas några krav på att de ingående parterna behöver följa den framtagna standarden, samt tillgång ska ges till standarden på rättvisa och skäliga villkor (Glader, Serre, & Pritchard, 2010).

Ett partnerskap mellan olika konkurrerande företag i ett konsortium, som exkluderar andra konkurrenter eller nekar andra företag tillgång till konsortiets faciliteter, kan utgöra ett olagligt konkurrenshämmande handelshinder (Finney, 2017). För att en målsägande ska kunna vinna ett sådant typ av mål behöver de bevisa att samarbetet mellan konkurrenter i ett konsortium resulterar i en konkurrenshämmande effekt utan att den svarande parten kan påvisa en konkurrensförbättrande effekt av samarbetet. Om den svarande lyckas med det kan målsägande i sin tur försöka påvisa att ett mindre konkurrenshämmande alternativ till den nuvarande samarbetsformen mellan företagen existerar. Om målsägande lyckas med det vinner de målet (Finney, 2017).

6.4.2 Karteller koordinerade genom blockkedjor

Det finns en oro för att blockkedjor skulle kunna underlätta upprätthållandet av karteller genom förutsättningarna för hur tekniken fungerar (Schrepel, 2019). Nya metoder för att utbyta information kan underlätta koordinering mellan konkurrenter, men frågan är om blockkedjor utgör en särskild anledning till oro i detta avseende. En publikation från OECD konstaterar att om den data som lagras i blockkedjan endast avser historiska transaktioner av digitala tillgångar, så bör den informationen inte i sig öka risken för otillåtna samarbeten mellan företag (OECD, 2018). Det är framförallt delning av information om framtida priser och strategier som kan möjliggöra kartellverksamhet.

Om specifika detaljer för varje enskild transaktion delas genom blockkedjan inklusive information om priser och volymer och blockkedjan är den enda kanal som handel sker genom på en specifik marknad så kan det finnas risk för att den informationen kan användas i syfte att upprätthålla konkurrensbegränsande samarbeten mellan företag. Prövningar om konkurrenshämmande aktivitet föreligger måste basera på vilken effekt informationen som delas får på marknaden snarare än faktumet att viss information delas genom blockkedjan (Nazzini, 2018). Eftersom blockkedjan registrerar information om historiska händelser eller händelser som sker i realtid, så behöver eventuella konkurrensbegränsande effekter analyseras utifrån marknadens struktur och hur den informationen som delas kan underlätta för företag att nå en jämvikt där priserna är högre och utbudet lägre än vad det skulle vara utan informationsutbytet genom blockkedjan. Enligt rapporten "Algorithms and Collusion: Competition Policy in the Digital Age" (OECD, 2017) finns det ökad risk för både uttrycklig och tyst samverkan mellan företag i transparenta marknader där konkurrenter kan övervaka varandras pris- och marknadsstrategier och risken att en tyst samverkan mellan företag uppstår är högst i transparenta marknader med få aktörer och homogena produkter.

Företag som bildar en kartell för att koordinera priser och volymer skulle teoretiskt kunna använda en blockkedja för att registrera information om alla transaktioner som de gör för att övervaka varandra. Men om detta inte sker genom en blockkedja, som utgör den enda kanalen för handel som utförs av medlemmarna i kartellen är det i min mening svårt att se hur informationen som registreras i blockkedjan skulle kunna garanteras vara sanningsenlig, eller varför en blockkedja skulle vara att föredra för denna typ av informationsutbyte framför andra kommunikationskanaler. Detta förutsätter att en blockkedja blivit så dominerande att ingen annan handelskanal används mellan kartellens medlemmar och alla dess handelspartners på en specifik marknad. Om information om alla transaktioner som genomförs inom en kartell finns registrerade i en gemensam blockkedja borde det även underlätta för konkurrensmyndigheter att utreda och bevisa att ett olagligt samarbete har skett (Lianos, 2018).

Det finns några artiklar som lagt fram hypoteser om att karteller via en blockkedja skulle kunna underlättas och göras mer stabila genom smarta kontrakt som övervakar att alla företag inom kartellen håller sig till överenskomna priser och volymer, samt som även har möjlighet att bestraffa avvikelser (Cong & He, 2018; Deng, 2018; Schrepel, 2019). Jag anser att det inte finns tekniska eller praktiska förutsättningar för detta idag och att det är osannolikt att förutsättningarna för detta kommer att infinna sig inom överskådlig framtid.

Dessa hypoteser förutsätter att alla företag inom kartellen utför alla transaktioner genom en eller flera blockkedjor som utgör de enda handelskanalerna som de använder med alla sina handelspartners, samt att tillräckligt mycket sanningsenlig information gällande priser och volymer för enskilda produkter registreras i blockkedjan vid varje transaktion och att all denna information kan övervakas av smarta kontrakt. Alternativt att alla transaktioner som företagen kan göra även utanför blockkedjor kan övervakas av orakel (Se Kapitel 4.5), som har möjlighet att rapportera information sanningsenligt till de smarta kontrakten.

Det finns i dagsläget inga orakel som skulle kunna göra något sådant och det är oklart om det kommer att bli möjligt i framtiden. Orakel som kan garanteras ge sanningsenlig information är idag ett olöst problem. Ett smart kontrakt kan inte på egen hand hämta information som befinner sig utanför blockkedjans interna tillstånd. En fysisk eller juridisk person måste använda mjukvara som antingen manuellt eller automatiskt levererar data till det smarta kontraktet att agera utifrån genom att utföra en transaktion på blockkedjan som innehåller den informationen. Förutom att det vore komplicerat tekniskt att utforma ett sådant smart kontrakt och att det inte ännu finns programmeringsspråk för att skriva säkra smarta kontrakt, så skulle dessutom kartellens medlemmar behöva hitta en neutral tredjepart som åtar sig uppgiften att agera orakel åt kartellen. Möjligheten för bestraffning via smarta kontrakt är även högst begränsad. Ett smart kontrakt kan endast fördela pengar till olika parter som först frivilligt låsts upp i ett smart kontrakt. Kartellens medlemmar skulle alltså först behöva enas om att låsa upp en tillräckligt stor summa pengar vardera i ett smart kontrakt, vilket även måste ske i form av en

blockkedjas interna valuta, vilket medför ökad risk. Den maximala bestraffningen skulle sedan bestå i att en kartellmedlem inte får tillbaka de pengar som de frivilligt låst upp om de bryter mot kartellens avtal.

Om det någon gång i framtiden skulle finnas förutsättningar för karteller som övervakas och upprätthålls via blockkedjor och smarta kontrakt borde det faktum att en eller flera blockkedjor används för transaktioner och tillhörande information mellan företagen i kartellen kunna underlätta för konkurrensmyndigheter att upptäcka kartellverksamhet och säkerställa bevisning.

Enligt en analys av revisions- och konsultföretaget EY finns det ingen särskild anledning för företag att vara alltför försiktiga med att använda blockkedjeteknik på grund av någon väsentlig risk att bryta mot konkurrenslagstiftningen (Desai, 2018). Men företag bör ha konkurrenslagstiftningen i åtanke när det gäller vilken typ av information de väljer att registrera i en blockkedja, särskilt om den används av flera olika konkurrerande företag.

6.4.3 Missbruk av dominant ställning

Publika blockkedjor är öppna för alla att använda på lika villkor så det kan inte förekomma någon diskriminering eller särbehandling av olika användare gällande priser eller andra villkor. Det vore teoretiskt möjligt att utöva missbruk av dominant ställning med en publik blockkedja som är under kontroll av enskilda parter, exempelvis genom att uppgradera blockkedjan till nackdel för konsumenter, eller genom att ta ut högre transaktionsavgifter. Men det förutsätter att en sådan publik blockkedja skulle kunna uppnå en dominant ställning i konkurrens med decentraliserade publika blockkedjor, vilket jag anser är osannolikt eftersom en publik blockkedja behöver vara decentraliserad för att kunna ge unika fördelar över en traditionell databas.

Privata blockkedjor är under kontroll av enskilda parter som bestämmer vem som kan få tillgång till blockkedjan och under vilka villkor. Dessa villkor kan även förändras till nackdel för den privata blockkedjans användare utan att dessa behöver ta något aktivt beslut. Enligt (Schrepel, 2018) är det sannolikt att oskäliga priser och affärsvillkor, teknisk utveckling till nackdel för konsumenter samt diskriminering kan ske med privata blockkedjor, men att det är osannolikt med publika blockkedjor. Anledningen till det är att privata blockkedjor är under kontroll av enskilda företag som därmed har möjlighet att missbruka denna kontroll. Men det förutsätter att en privat blockkedja har möjlighet att uppnå en dominant ställning för att det skulle utgöra ett problem i konkurrenshänseende.

En teoretisk möjlighet är att ett konsortium som använder en privat blockkedja uppnår en dominant ställning och att den infrastruktur de bygger upp leder till sådana dramatiska effektivitetsvinster att det blir praktiskt omöjligt för företag som inte har tillgång till konsortiets blockkedja att konkurrera. Om ett konsortium av

företag får en sådan dominant position i den relevanta marknaden och kontrollerar resurser som anses vara nödvändiga att ha tillgång till för att kunna konkurrera, så kan det leda till att konsortiet kan behöva hindras från att neka utomstående konkurrenter inträde till konsortiet eller dess faciliteter under rimliga och icke-diskriminerande villkor (Nazzini, 2018). För att en konkurrensmyndighet eller annan målsägande ska göra detta gällande så krävs det att de dels bevisar att tillgång till blockkedjan är oumbärlig för effektiv konkurrens, dels att vägran att ge konkurrenter tillträde skadar konsumenter (Schrepel, 2018). Ett lättare sätt att öppna upp tillgång till en dominant, men inte nödvändigtvis oumbärlig blockkedja genom konkurrenslagarna kan enligt Nazzini (2018) vara att pröva fallet enligt artikel 102(c), vilken förbjuder en dominant marknadsaktör att tillämpa olika affärsvillkor vid likvärdiga transaktioner med olika handelspartner. I det fallet kan det räcka med att påvisa att en diskriminering föreligger. Om tillgång till en privat blockkedja som används av medlemmar i ett konsortium inte är nödvändig för utomstående företag att konkurrera bör riskerna för konsortiet att fällas under konkurrenslagarna minska. Likaså bör de minska om utomstående konkurrenter har möjlighet att få tillgång till motsvarande mjukvara och kan bygga upp motsvarande system som används inom konsortiet. Konsortier kan även proaktivt arbeta med att dokumentera konkurrensförbättrande effekter och förbättringar för konsumenter av deras samarbete för att minska riskerna att anklagas för konkurrenshämmande verksamhet.

OECD har påpekat i en publikation att en annan typ av risk är att etablerade företag skulle kunna utnyttja sin dominanta ställning för att bromsa adoption av blockkedjeteknik genom att överdriva riskerna med tekniken eller genom att ägna sig åt lobbyverksamhet för att upprätta regulatoriska hinder som ökar kostnaderna och trösklarna för dess potentiella konkurrenter (OECD, 2018).

6.4.4 Tillsyn och lagtillämpning

Det finns på publika blockkedjor inga hinder för tillsynsmyndigheter att ta del av all transaktionshistorik och göra analyser för att upptäcka och spåra olaglig verksamhet. Det finns flera företag som specialiserat sig på att hjälpa myndigheter och företag med denna typ av uppgifter (Se Kapitel 0). Om ökad ekonomisk verksamhet i framtiden sker genom publika blockkedjor skulle tillsynsmyndigheter och ekonomer kunna få en betydligt mer detaljerad inblick i hur marknader fungerar (Kobie, 2018).

Tillsynsmyndigheter skulle även kunna ges möjlighet till tillträde på privata blockkedjor genom att delta som en nod i nätverket för att övervaka transaktioner i syfte att säkerställa att ingen konkurrenshämmande verksamhet förekommer. Sådan övervakning skulle kunna ge starka incitament till deltagarna i blockkedjan att inte försöka sig på några otillåtna verksamheter eller otillåtna samarbeten. En sådan tillsyn skulle kunna implementeras antingen via ett lagstöd eller på frivillig väg som ett sätt att öka legitimiteten för blockkedjan.

Tillsynsmyndigheter skulle även kunna ges insyn vid utvecklingsarbetet av privata blockkedjor inom konsortier för att säkerställa att information inte delas som kan anses vara konkurrenshämmande. Genom att utforma privata blockkedjor i samråd med myndigheter så att inte känslig information görs tillgänglig utanför parterna till transaktionen så borde riskerna för konkurrenshämmande verksamhet till stor del kunna uteslutas (Louven & Saive, 2018).

Om tillsynsmyndigheter deltar i konsortier som utvecklar blockkedjor från ett tidigt stadium kan de samtidigt lära sig om hur tekniken fungerar och hur den kan påverka den relevanta marknaden och konkurrensen innan eventuella problem hinner uppstå.

Deltagande i en privat blockkedja skulle kunna leda till solidariskt delat juridiskt och ekonomiskt ansvar för blockkedjans deltagare för handlande som leder till ekonomisk skada enligt Zetzsche, Buckley, & Arner (2018). Det kan innebära en ökad ekonomisk risk för företag i ett konsortium där varje företag som driver en egen nod vilken validerar transaktioner i den gemensamma blockkedjan kan bli ekonomiskt ansvariga för ekonomiska skador orsakade av något av de andra företagen. Enligt Zetzsche, Buckley, & Arner (2018) kan detta utgöra juridiska hinder för företag att driva en gemensam blockkedja tillsammans med många andra företag och över landsgränser. Det kan leda till att privata blockkedjor av juridiska skäl hanteras av en enskild part eller ett litet antal parter.

Då blockkedjesamarbeten kan innefatta företag som befinner sig i olika delar av världen krävs det tydlighet om vilken lag som ska tillämpas vid tvister. Ett sätt att hantera det skulle kunna vara att ett kontrakt upprättas mellan alla parter i ett blockkedjesamarbete som specificerar enligt vilken lagstiftning tvister ska bedömas och hur skadeansvar ska fördelas om tekniska problem uppstår med blockkedjan.

6.4.5 Konkurrenslagstiftningens tillämpbarhet på blockkedjor

En förutsättning för att kunna tillämpa konkurrenslagstiftning på blockkedjor är att det finns identifierbara ansvariga juridiska personer. Publika decentraliserade blockkedjor består av ett nätverk av noder som är utspridda över världen och systemet drivs oberoende från stater och centralbanker och befinner sig inte i någon särskild jurisdiktion (Breu, 2017). Publika blockkedjor som är decentraliserade har ingen enskild part som är ansvarig för skapandet eller driften av blockkedjan. Utvecklingen av mjukvaran sker genom ett frivilligt samarbete mellan individer från olika delar av världen i en öppen transparent process, där enskilda deltagare inte nödvändigtvis behöver identifiera sig. Utvecklarna har ingen tvångsmakt utan alla deltagare (noder) väljer frivilligt vilken mjukvara de vill köra. Valideringen av transaktioner i blockkedjan sker genom en decentraliserad process utan fasta eller nödvändigtvis identifierbara enskilda parter som deltagare. De enskilda aktörer som validerar transaktioner har heller ingen särskild makt att påverka systemet som upprätthålls genom protokollets regler av alla användare som kör en egen nod

i nätverket. Likaså regleras inte transaktionsavgifter och andra villkor genom några kontraktuella förbindelser som kan prövas i en domstol utan av mjukvaruprotokollet som skapar blockkedjan (Huberman, Leshno, & Moallemi, 2017).

Lagar mot konkurrenshämmande verksamhet är designade för att lösa problem där marknadsinflytande centraliserats och har inte utformats för att hantera system som skapats för att säkerställa decentralisering. Företag som erbjuder tjänster kopplade till kryptovalutor och publika blockkedjor, exempelvis börser, betalningsförmedlare och plånbokstjänster kan däremot regleras under konkurrenslagarna om det skulle behövas. Men jag anser att det är osannolikt att det blir aktuellt eftersom blockkedjeteknik möjliggör skapandet av decentraliserade plattformar som kan göra dessa mellanhänder överflödiga.

Att tillämpa konkurrenslagstiftningen på företag eller enskilda parter som driver och kontrollerar en viss blockkedja (som därmed inte är decentraliserad), borde inte vara mer problematiskt än att tillämpa konkurrenslagstiftningen på företag eller enskilda parter som driver andra former av digitala plattformar. Dock skulle det i vissa fall kunna uppstå svårigheter i att bevisa att ett företag eller en enskild part de facto har kontroll över en viss blockkedja. Likaså, att tillämpa konkurrenslagstiftningen på konsortier av företag som samarbetar om utveckling och drift av privata blockkedjor på ett otillbörligt sätt, borde inte vara mer problematiskt än gällande andra former av samarbeten och kanaler för informationsdelning mellan företag. Tvärtom borde användningen av en blockkedja i konkurrenshämmande samarbeten kunna göra det lättare att säkra bevismaterial.

7 Slutsatser

- Blockkedjeteknik är i ett tidigt stadium generellt och merparten av utvecklingen och tillämpningen av tekniken har skett inom publika blockkedjor och kryptovalutor.

- Publika blockkedjor kan förbättra konkurrensen genom att överbrygga de koordinationsproblem som annars leder till att nätverkseffekter blir en källa till marknadsinflytande och kan ge en dominerande ställning för enskilda företag som agerar mellanhand i informationsutbyten och ekonomiska transaktioner.

- Privata blockkedjor som företag, banker och finansiella institut visat stort intresse för är på ett tidigt stadium av utveckling och konceptvalidering. Eftersom dessa inte är decentraliserade utan under kontroll av enskilda parter så kan de inte erbjuda de unika nya användningsområden som publika decentraliserade blockkedjor möjliggör.

- Huvuddelen av farhågorna kring konkurrensbegränsande verksamhet kopplat till blockkedjeteknik rör formerna för samarbeten mellan konkurrerande företag inom konsortier. Risker med konkurrenshämmande samarbeten mellan företag i utveckling och implementering av privata blockkedjor skulle kunna avhjälpas av att konkurrensmyndigheter ges insyn i privata blockkedjor som utvecklas inom konsortier av företag, antingen på frivillig väg eller via lagstiftning.

- Det har föreslagits att koordinering och informationsutbyte med hjälp av blockkedjor och smarta kontrakt skulle kunna användas av företag för att upprätthålla karteller. Detta ger blockkedjor och smarta kontrakt varken tekniska eller praktiska förutsättningar för idag och jag anser det vara osannolikt att förutsättningarna för detta kommer att infinna sig inom överskådlig framtid.

- Missbruk av en dominant ställning vore teoretiskt möjligt med en privat blockkedja, eftersom den är under kontroll av enskilda parter som kan missbruka den kontrollen. Men det förutsätter iså fall att en privat blockkedja kan uppnå en dominant ställning för att det konkurrensmässigt sätt skulle kunna bli ett problem.

- Det är inte möjligt att utöva missbruk av en dominant ställning med decentraliserade publika blockkedjor eftersom de är öppna för alla att använda på lika villkor och inte under någon enskild parts kontroll. Det finns då ingen part som har kontroll eller makt över andra som kan missbrukas.

- Det vore teoretiskt möjligt att utöva missbruk av en dominant ställning med en publik blockkedja som inte är decentraliserad, utan under kontroll av enskilda parter. Men det förutsätter att en sådan blockkedja skulle kunna uppnå en dominant ställning i konkurrens med decentraliserade publika blockkedjor, vilket jag anser är osannolikt eftersom en publik blockkedja behöver vara decentraliserad för att kunna ge unika fördelar över en traditionell databas.

8 Referenser

Back, A. (2002). Hashcash - *A Denial of Service Counter-Measure*. Hämtad från https://nakamotoinstitute.org/static/docs/hashcash.pdf

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Wuille, P. (2014). *Enabling Blockchain Innovations with Pegged Sidechains*. Hämtad från https://blockstream.com/sidechains.pdf

Bendiksen, C., Gibbson, S., & Lim, E. (2018). *The Bitcoin Mining Network - Trends, Composition, Marginal Creation Cost, Electricity Consumption & Sources*. Hämtad från https://coinshares.co.uk/wp-content/uploads/2018/11/Mining-Whitepaper-Final.pdf

Benedetti, H., & Kostovetsky, L. (2018). *Digital Tulips? Returns to Investors in Initial Coin Offerings*. https://doi.org/10.2139/ssrn.3182169

Berg, C., Davidson, S., & Potts, J. (2018). *Institutional Discovery and Competition in the Evolution of Blockchain Technology*. https://doi.org/10.2139/ssrn.3220072

Bevand, M. (2018). *Electricity consumption of Bitcoin: a market-based and technical analysis*. Hämtad från http://blog.zorinaq.com/bitcoin-electricity-consumption/

Bevilacqua, L., Levites, P., & Rahmati, L. (2018). *Security Token Offerings White Paper*. Bevilacqua PLLC. Hämtad från https://www.bevilacquapllc.com/security-token-offerings-white-paper/

BitFury Group. (2015). *Proof of Stake vs Proof of Work*. Hämtad från https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

Bogart, S. (2018). *Crypto Innovation Spotlight 2: Scriptless Scripts*. Hämtad från https://medium.com/blockchain-capital-blog/crypto-innovation-spotlight-2-scriptless-scripts-306c4eb6b3a8

Brandman, G., & Thampapillai, S. (2016). *Blockchain – Considering the Regulatory Horizon*. Hämtad från https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/blockchain-%E2%80%93-considering-regulatory-horizon

Breu, S. (2017). *Blockchains and Cybercurrencies Challenging Anti Trust and Competition Law*. https://doi.org/10.2139/ssrn.3081914

Brown, R. G. (2016). *Introducing R3 CordaTM: A Distributed Ledger Designed for Financial Services*. Hämtad från https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

Camera, G. (2017). *A Perspective on Electronic Alternatives to Traditional Currencies*. Hämtad från https://papers.ssrn.com/abstract=2902721

Catalini, C., & Gans, J. S. (2016). *Some Simple Economics of the Blockchain*. National Bureau of Economic Research. https://doi.org/10.3386/w22952

Catalini, C., & Tucker, C. E. (2018). *Antitrust and Costless Verification: An Optimistic and a Pessimistic View of the Implications of Blockchain Technology*. https://doi.org/10.2139/ssrn.3199453

Chaum, D. L. (1983). *Blind Signatures for Untraceable Payments. Advances in Cryptology* (s. 199–203). Springer US.

Chaum, D. L. (1985). *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*. Communications of the ACM, 28(10), 1030–1044.

Chaum, D. L. (1981). *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Communications of the ACM, 24(2), 84–90.

Clark, J., & Essex, A. (2012). *Commitcoin: Carbon dating commitments with bitcoin*. In International Conference on Financial Cryptography and Data Security (pp. 390-398). Springer, Berlin, Heidelberg.

Cong, L. W., & He, Z. (2018). *Blockchain Disruption and Smart Contracts*. National Bureau of Economic Research. https://doi.org/10.3386/w24399

Daian, P., Pass, R., & Shi, E. (2016). *Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake*. CornellTech. Hämtad från https://eprint.iacr.org/2016/919.pdf

Dai, W. (1998). *b-money*. Hämtad från https://nakamotoinstitute.org/b-money/

Davidson, S., de Filippi, P., & Potts, J. (2018). *Blockchains and the economic institutions of capitalism*. Journal of Institutional Economics, 14(4), 639–658.

Decker, C., & Wattenhofer, R. (2013). *Information propagation in the Bitcoin network*. IEEE P2P 2013 Proceedings (s. 1–10).

Demeester, T., Blummer, T., & Lescrauwaet, M. (2019). *A Primer on Bitcoin Investor Sentiment and Changes in Saving Behavior*. Hämtad från https://medium.com/@adamant_capital/a-primer-on-bitcoin-investor-sentiment-and-changes-in-saving-behavior-a5fb70109d32

Deng, A. (2018). *Smart Contracts and Blockchains: Steroid for Collusion?* https://doi.org/10.2139/ssrn.3187010

De Oliveira, L. C., De Oliveira Simoyama, F., Grigg, I., & Bueno, R. L. P. (2017). *Triple entry ledgers with blockchain for auditing*. International Journal of Auditing Technology, 3(3), 163.

Desai, K. S. (2018, april). *Blockchain and competition law - EY Law alert*. Hämtad från https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-competition-law/$FILE/ey-blockchain-and-competition-law.pdf

Diffie, W., & Hellman, M. (1976). *New directions in cryptography*. IEEE transactions on Information Theory, 22(6), 644-654.

Dilley, J., Poelstra, A., Wilkins, J., Piekarska, M., Gorlick, B., & Friedenbach, M. (2016). *Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks*. arXiv [cs.CR]. Hämtad från http://arxiv.org/abs/1612.05491

Dixon, C. (2017). *Crypto Tokens: A Breakthrough in Open Network Design*. Hämtad från https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef

Dryja, T. (2017). *Discreet Log Contracts. MIT Digital Currency Initiative*. Hämtad från https://adiabat.github.io/dlc.pdf

Dwork, C., & Naor, M. (1992). *Pricing via processing or combatting junk mail*. In Annual International Cryptology Conference (pp. 139-147). Springer, Berlin, Heidelberg.

ECB. (2012). *Virtual currency schemes*. ECB. Hämtad från https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Finck, M. (2017). *Blockchains and Data Protection in the European Union*. https://doi.org/10.2139/ssrn.3080322

Finney, B. (2017). *Blockchain and Antitrust: New Tech Meets Old Regs*. Transactions: Tenn. J. Bus. L. Hämtad från https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/transac19&section=36

Finney, H. (2004). *RPOW - Reusable Proofs of Work*. Hämtad från https://nakamotoinstitute.org/rpow/

Garay, J. A., & Kiayias, A. (2014). *The Bitcoin Backbone Protocol: Analysis and Applications*. Cryptology ePrint Archive, Report 2014/765. Hämtad från https://eprint.iacr.org/2014/765.pdf

Glader, M., de la Serre, E. B., & Pritchard, S. (2010). *Standardisation and the Commission's new horizontal guidelines*. Hämtad från

http://competitionlawblog.kluwercompetitionlaw.com/2010/11/04/standardisation-and-the-commissions-new-horizontal-guidelines/

Glasbergen, G.-J. (2018). *Discreet Log Contracts: invisible smart contracts on the Bitcoin blockchain*. Hämtad från https://medium.com/@gertjaap/discreet-log-contracts-invisible-smart-contracts-on-the-bitcoin-blockchain-cc8afbdbf0db

Goya, I. (2017). *Comparison of Blockchain Technologies - Comunytek*. Hämtad från http://comunytek.com/en/comparison-of-blockchain-technologies/

Gratzke, P., Schatsky, D., & Piscini, E. (2017). *Banding together for blockchain*. Hämtad från https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/emergence-of-blockchain-consortia.html

Grigg, I. (2005). *Triple Entry Accounting*. Hämtad från http://iang.org/papers/triple_entry.html

Haber, S., & Stornetta, W. S. (1990). *How to time-stamp a digital document*. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.

Huberman, G., Leshno, J., & Moallemi, C. C. (2017). *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System*. Hämtad från https://papers.ssrn.com/abstract=3032375

Hughes, E. (1993). *A Cypherpunk's Manifesto*. Hämtad från https://nakamotoinstitute.org/cypherpunk-manifesto/

Jackson, M. (2014). *Bitcoin and Regulation: Lessons from the Early Days of Skype*. Hämtad från https://www.coindesk.com/bitcoin-regulation-lessons-early-days-skype

Jayachandran, P. (2017). *The difference between public and private blockchain - Blockchain Pulse: IBM Blockchain Blog*. Hämtad från https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Jevons, W. S. (1875). *Money and the Mechanism of Exchange*. London: Appleton.

Jimenez, G. (2018). *Ubisoft and allies push blockchain gaming to the next level*. Hämtad från https://decryptmedia.com/4268/owned-ubisoft-allies-blockchain-industry-gaming-next-level

Karp, R., Schindelhauer, C., Shenker, S., & Vocking, B. (2000). *Randomized rumor spreading*. In Proceedings 41st Annual Symposium on Foundations of Computer Science (s. 565–574).

Katz, M. L., & Shapiro, C. (1994). *Systems competition and network effects*. Journal of economic perspectives, 8(2), 93-115.

Kleinrock, L. (2010). *An early history of the internet [History of Communications]*. IEEE Communications Magazine, 48(8), 26–36.

Kobie, N. (2018). *This is how politicians should regulate the blockchain*. Hämtad från https://www.wired.co.uk/article/regulate-blockchain

Koomey, J. G. (2018). *Talking Sense About Bitcoin Electricity Use*. Hämtad från http://www.koomey.com/post/179556571967

Kully, D. C., & Dewey, J. (2017). *Blockchain collaborators should be attuned to potential antitrust issues*. Hämtad från https://store.legal.thomsonreuters.com/law-products/news-views/corporate-counsel/blockchain-collaborators-attuned-to-potential-antitrust

Kully, D., & Dewey, J. (2017). *Bitcoin tech may be the future, but it raises serious antitrust questions*. Hämtad från https://thehill.com/blogs/pundits-blog/technology/335140-is-bitcoin-tech-the-future-or-will-they-violate-antitrust-laws

Lamport, L., Shostak, R., & Pease, M. (1982). *The Byzantine Generals Problem*. ACM Transactions on Programming Languages and Systems, 4(3), 382–401.

Landauer, R. (1961). *Irreversibility and Heat Generation in the Computing Process*. IBM Journal of Research and Development, 5(3), 183–191.

Law Library of Congress. (2018). *Regulation of Cryptocurrency Around the World*. Hämtad från https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf

Lee, K., James, J. I., Ejeta, T. G., & Kim, H. J. (2016). *Electronic Voting Service Using Block-Chain*. Journal of Digital Forensics, Security and Law, 11(2), 8.

Lemieux, V. L. (2016). *Trusting records: is Blockchain technology the answer?* Records Management Journal. https://doi.org/10.1108/RMJ-12-2015-0042

Lerner, S. D. (2015). *RSK White Paper*. RSK. Hämtad från https://www.rsk.co/

Levy, S., Matsakis, L., Dreyfuss, E., Greenberg, A., Newman, L. H., & Barrett, B. (1993). *Crypto Rebels*. Wired. Hämtad från https://www.wired.com/1993/02/crypto-rebels/

Lianos, I. (2018). *Blockchain Competition*. Hämtad från https://papers.ssrn.com/abstract=3257307

Li, J., & Mann, W. (2018). *Initial Coin Offerings and Platform Building*. Hämtad från https://doi.org/10.2139/ssrn.3088726

Long, C. (2019). *What Do Wyoming's 13 New Blockchain Laws Mean? Forbes Magazine*. Hämtad från https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/

Louven, S., & Saive, D. (2018). *Antitrust by Design – The Prohibition of Anti-Competitive Coordination and the Consensus Mechanism of the Blockchain*. Hämtad från https://doi.org/10.2139/ssrn.3259142

Lua, E. K., Crowcroft, J., Pias, M., Sharma, R., Lim, S., & Others. (2005). *A survey and comparison of peer-to-peer overlay network schemes*. IEEE Communications Surveys and tutorials, 7(1-4), 72–93.

May, T. C. (1988). *The Crypto Anarchist Manifesto*. Hämtad från https://nakamotoinstitute.org/crypto-anarchist-manifesto/

McGraw, G. (2004). *Software security*. IEEE Security Privacy, 2(2), 80–83.

McLeay, M., Radia, A., & Thomas, R. (2014). *Money Creation in the Modern Economy*. Hämtad från https://papers.ssrn.com/abstract=2416234

Merkle, R. C. (1988). *A Digital Signature Based on a Conventional Encryption Function*. In Advances in Cryptology (s. 369–378). Springer Berlin Heidelberg.

Metcalfe, B. (2013). *Metcalfe's Law after 40 Years of Ethernet*. Computer, 46(12), 26–31.

Metz, C., Karabell, Z., Lapowsky, I., Martineau, P., Finley, K., Matsakis, L., & Dreyfuss, E. (2015). *SEC Approves Plan to Issue Stock Via Bitcoin's Blockchain*. Wired. Hämtad från https://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchain/

Miller, A., & LaViola, J. J. (2014). *Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin*. Hämtad från https://nakamotoinstitute.org/research/anonymous-byzantine-consensus/

Miller, V. S. (1985). *Use of elliptic curves in cryptography*. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Springer, Berlin, Heidelberg.

Milnes, M. (2016). *Blockchain: Issues in Competition & Consumer Law*. Hämtad från https://www.linkedin.com/pulse/blockchain-issues-competition-consumer-law-michael-milnes/

Mizrahi, A. (2015). *A blockchain-based property ownership recording system*. Hämtad från https://chromaway.com/papers/A-blockchain-based-property-registry.pdf

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

Nazzini, R. (2018). *The Blockchain (R)evolution and the Role of Antitrust*. Hämtad från https://doi.org/10.2139/ssrn.3256728

Nick, J. (2016). *Bitcoin Privacy: Theory and Practice*. Hämtad från https://www.reddit.com/r/Bitcoin/comments/4b9ylx/bitcoin_privacy_theory_and_practice_jonas_nick/

O'Connor, R. (2017). *Simplicity: A New Language for Blockchains*. Hämtad från https://blockstream.com/simplicity.pdf

OECD. (2017). *Algorithms and collusion: Competition policy in the digital age*. OECD. Hämtad från http://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm

OECD. (2018). *Blockchain and competition policy*. OECD. Hämtad från http://www.oecd.org/competition/blockchain-and-competition-policy.htm

Poelstra, A. (2015). *On Stake and Consensus*. Hämtad från https://nakamotoinstitute.org/research/on-stake-and-consensus/

Poon, J., & Dryja, T. (2016). *The bitcoin lightning network: Scalable off-chain instant payments*. Hämtad från https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf

Quack, S., & Djelic, M.-L. (2003). *The story of antitrust and competition law in Germany and Europe*. Hämtad från https://core.ac.uk/download/pdf/153145481.pdf

Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A Method for Obtaining Digital Signatures and Public-key Cryptosystems*. Communications of the ACM, 21(2), 120–126.

Rogers, E. M. (2003). *Diffusion of Innovations*, 5th Edition. Free Press.

Rosenfeld, M. (2012). Overview of colored coins. Hämtad från https://bitcoil.co.il/BitcoinX.pdf

Rubin, A. D. (2002). *Security Considerations for Remote Electronic Voting*. Communications of the ACM, 45(12), 39–44.

Sadeghi Gazani, M. (2018). *En rättslig utredning av Initial Coin Offerings (ICO:s) status i svensk rätt*. Uppsala universitet. Hämtad från http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1186648&dswid=7087

Schrepel, T. (2018*). Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*. https://doi.org/10.2139/ssrn.3193576

Schrepel, T. (2019). *Collusion By Blockchain And Smart Contracts*. https://doi.org/10.2139/ssrn.3315182

Smid, M. E., & Branstad, D. K. (1988). *Data Encryption Standard: past and future*. Proceedings of the IEEE, 76(5), 550–559.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). *Security Analysis of the Estonian Internet Voting System*. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (s. 703–715). New York, NY, USA: ACM.

Stallman, R. (1985). *The GNU Manifesto*. Hämtad från https://www.gnu.org/gnu/manifesto.en.html

Šurda, P. (2012). *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?* Vienna University of Economics and Business . Hämtad från https://nakamotoinstitute.org/research/economics-of-bitcoin/

Szabo, N. (1996). *Smart contracts: building blocks for digital markets*. EXTROPY: The Journal of Transhumanist Thought,(16). Hämtad från http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Szabo, N. (1997). *Formalizing and Securing Relationships on Public Networks*. Hämtad från https://nakamotoinstitute.org/formalizing-securing-relationships/

Szabo, N. (1997). *The idea of smart contracts*, 1997. Hämtad från http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html

Szabo, N. (2001). *Trusted Third Parties are Security Holes*. Hämtad från https://nakamotoinstitute.org/trusted-third-parties/

Szabo, N. (2002). *Shelling Out: The Origins of Money*. Hämtad från https://nakamotoinstitute.org/shelling-out/

Szabo, N. (2005a). *Antiques, time, gold, and bit gold*. Hämtad från http://unenumerated.blogspot.com/2005/10/antiques-time-gold-and-bit-gold.html

Szabo, N. (2005b). *Bit Gold*. Hämtad från https://nakamotoinstitute.org/bit-gold/

Szabo, N. (2017). *Money, Blockchains, and Social Scalability*. Hämtad från https://nakamotoinstitute.org/money-blockchains-and-social-scalability/

Todd, P. (2016). *OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin*. Hämtad från https://petertodd.org/2016/opentimestamps-announcement

Torvalds, L. (1991). *What would you like to see most in minix?* Hämtad från https://groups.google.com/forum/#!original/comp.os.minix/dlNtH7RRrGA/SwRavCzVE7gJ

Turing, A. M. (1937). *On computable numbers, with an application to the Entscheidungsproblem*. Proceedings of the London mathematical society, 2(1), 230-265.

Vaughan, W., Bukowski, J., & Wilkinson, S. (2016). *Chainpoint White Paper*. Github. Hämtad från https://github.com/chainpoint/whitepaper

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). *The distributed liability of distributed ledgers: Legal risks of blockchain*. University of Illinois law review, 1361.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2018). *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*. https://doi.org/10.2139/ssrn.3072298

Zimmermann, P. R. (1991). *Why I Wrote PGP*. Hämtad från https://nakamotoinstitute.org/why-i-wrote-pgp/

Bilaga 1. Ordlista

Asymmetrisk kryptering	En krypteringsmetod där en publik nyckel används för att kryptera och en matematiskt länkad privat nyckel används för att dekryptera, eller tvärtom då de är varandras inverser. En digital signatur kan skapas genom att signera ett meddelande med en privat nyckel, vilket gör att avsändarens identitet kan verifieras med tillhörande publika nyckel.
Bitcoin	Världens första decentraliserade digitala valuta som lade grunden till blockkedjeteknik. Bitcoin, med stor bokstav, används för att beskriva kryptovalutan, blockkedjan, eller nätverket i sin helhet, medans bitcoin, med liten bokstav, används för att beskriva enheter av blockkedjans interna valuta.
Blockkedja (eng. Blockchain)	En blockkedja är i vid mening ett transaktionsregister bestående av block med data som länkas samman kryptografiskt i kronologisk ordning och som upprätthålls och uppdateras av användare inom ett nätverk i enlighet med en konsensusmekanism som syftar till att säkerställa att alla användare är överens om en gemensam transaktionshistorik.
Cypherpunk	En aktiviströrelse som startade i början av 90-talet som förespråkar utvecklandet och användandet av integritetsfrämjande tekniker för att möjliggöra frihet och öppenhet i en digital värld.
Decentraliserad Autonom Organisation	En organisation som använder en blockkedja och smarta kontrakt för att upprätta en fungerande incitamentsstruktur för sin förvaltning utan behov av ett centralt styrande organ.
Dubbelspendering	Att samma digitala mynt spenderas till flera mottagare. Bitcoin var först med en lösning på hur dubbelspendering kan undvikas i ett decentraliserat elektroniskt betalningsnätverk.
Ethereum	En publik blockkedja som skapats för att möjliggöra avancerade smarta kontrakt
Fork	En förgrening av ett projekt med öppen källkod så att en kopia görs som utvecklas i en ny riktning från det ursprungliga projektet. Eller en förgrening av en blockkedja så att en alternativ parallell blockkedja skapas. När en bakåtkompatibel förändring av en blockkedjas protokoll görs kallas det för en soft fork. En förändring som inte är bakåtkompatibel kallas hard fork. Om en hard fork inte antas eller avslås enhälligt så kan det resultera i att en blockkedja förgrenas i två separata nätverk.
Färgade mynt (eng. Colored Coins)	Mynt av en blockkedjas interna valuta som öronmärkts för att representera andra tillgångar genom ett överliggande protokoll.
Hash	Ett digitalt fingeravtryck av en digital fil som skapas genom en hashfunktion. I blockkedjor används en hash av ett föregående block för att kryptografiskt koppla ihop det med

	nästkommande block, vilket i förlängningen bildar en kryptografiskt länkad kedja av block. En hashfunktion används även i flera andra komponenter av blockkedjor, exempelvis mekanismen för Proof-of-work .
Initial Coin Offering (ICO)	Ett sätt för företag och projekt att dra in kapital genom att skapa en ny kryptovaluta och sälja den till investerare. Vanligtvis som representerande en ägarandel eller en funktionell enhet som kan användas för att få tillgång till resurser i ett system som ska utvecklas.
Konsensus	Att alla är överens, exempelvis om hur ett blockkedjeprotokoll ska uppgraderas, eller att alla noder i ett nätverk lagrar en identisk kopia av samma blockkedja och därmed är överens om transaktionshistoriken, vilket säkerställs genom protokollets konsensusalgoritm.
Kryptovaluta	Intern valuta i en blockkedja.
Lightning Network	Ett nätverk av betalningskanaler skapade genom smarta kontrakt där transaktioner kan utföras på ett kryptografiskt säkert sätt utanför blockkedjan och när en betalningskanal stängs så registreras det aggregerade resultatet av transaktionerna på blockkedjan. Det är ett lager ovanpå Bitcoins blockkedja för att skala upp transaktionskapaciteten och erbjuda nya funktioner.
Mining	Processen för att lägga nya block med transaktioner till blockkedjan i Bitcoin och andra kryptovalutor genom att utföra beräkningar för att producera Proof-of-work . För varje block med transaktioner så skapas en ny andel av blockkedjans interna valuta som ges som belöning för arbetet inklusive transaktionsavgifter.
Nod	En dator uppkopplad i ett nätverk som kan sända, ta emot och vidarebefordra information till andra datorer som använder samma protokoll. I ett blockkedjenätverk så lagrar varje nod en kontinuerligt uppdaterad kopia av blockkedjan och validerar nya transaktioner.
Orakel	En mekanism för att rapportera information från omvärlden utanför blockkedjan till ett smart kontrakt
Peer-to-peer nätverk	Ett nätverk av sammankopplade datorer som kommunicerar med varandra på lika villkor istället för med en central server.
Proof-of-stake	En algoritm för att uppnå konsensus i ett blockkedjenätverk baserat på att de noder som kontrollerar en andel av den interna valutan får delta i processen och ha en chans att lägga nya block med transaktioner till blockkedjan.
Proof-of-work	En algoritm för att uppnå konsensus i en publik blockkedja baserat på att noder i nätverket behöver göra resurskrävande beräkningar för att ha en chans att hitta en lösning som ger rätten att lägga ett nytt block med transaktioner till blockkedjan.
Privat blockkedja	En blockkedja som kräver tillstånd för att få åtkomst till och som består av identifierade

	deltagare där alla användare inte behöver ha samma befogenheter att läsa, skriva och validera transaktioner i nätverket.
Privat nyckel	I en blockkedja används privata kryptonycklar för att kontrollera tillgångar och utföra transaktioner.
Protokoll	En uppsättning formella regler som beskriver hur data skickas och tas emot i ett nätverk.
Publik blockkedja	En blockkedja som är öppen för alla att använda och delta i på lika villkor utan krav annat än att protokollets regler följs.
Publik nyckel	I en blockkedja används en publik kryptonyckel för att ta emot transaktioner.
Token	Ett annat ord för ett mynt av en blockkedjas interna valuta vilket kan representera andra tillgångar än pengar. En security token kan liknas vid ett värdepapper och en utility token kan liknas vid en kupong som kan användas för åtkomst till en viss resurs.
Sidokedja (eng. Sidechain)	Sidokedjor är blockkedjor som är kopplade till och kompatibla med huvudblockkedjan så att tillgångar kan flyttas mellan dem. Genom sidokedjor kan nya funktioner introduceras utan att kompromissa med säkerheten för huvudkedjan.
Smarta kontrakt	Ett kontrakt i form av programkod som verkställer sig självt på en blockkedja när kontraktets villkor uppfyllts vilket resulterar i att tillgångar representerade på en blockkedja flyttas.
Öppen källkod (eng. Open Source)	Öppen källkod betyder att instruktionerna för att konstruera ett datorprogram är publikt och fritt att använda, läsa, kopiera, modifiera och vidaredistribuera.

KONKURRENSVERKET
Swedish Competition Authority

Adress 103 85 Stockholm
Telefon 08-700 16 00
Fax 08-24 55 43
konkurrensverket@kkv.se

www.konkurrensverket.se