Vad är Bitcoin?

Björn Segendorf*

Författaren är filosofie doktor i nationalekonomi och verksam vid Riksbankens avdelning för finansiell stabilitet.

Bitcoin är en så kallad virtuell valuta och har konstruerats för anonyma betalningar som görs helt oberoende av stater och banker. Bitcoin har under de senaste åren fått stor uppmärksamhet från olika håll. Betalningar med Bitcoin baseras på en ny och intressant teknisk lösning och fungerar på ett annat sätt än traditionella betalningar. I vissa betalningssituationer kan Bitcoin ha fördelar i form av lägre kostnader, snabbhet, anonymitet med mera framför traditionella sätt att betala men det kan också vara mer riskfyllt att använda eftersom Bitcoin inte direkt omfattas av de lagar som styr annan betalningsförmedling. Det svaga konsumentskyddet är också en av anledningarna till att Bitcoin kan få svårt att bli allmänt accepterad och gångbar som betalningsmedel. Användningen av Bitcoin för betalningar är idag liten och även om Bitcoins framtid är osäker är Bitcoin en intressant innovation som förtjänar att beskrivas. I artikeln förklaras vad en virtuell valuta är och hur Bitcoin fungerar. Dessutom beskrivs användningen av Bitcoin i Sverige, som är mycket begränsad. Slutligen diskuteras framtiden för Bitcoin och andra virtuella valutor.

Ett svar på nya behov?

Den tekniska utvecklingen har på flera områden varit snabb under de senaste åren. Även våra behov att göra betalningar håller på att förändras. Ett exempel är att hushållen handlar allt mer på Internet och att allt fler betalningar går över landsgränser. Betalningslösningarna, speciellt för betalningar mellan privatpersoner, har däremot inte utvecklats lika snabbt. Bitcoin kan ses som ett svar på bristen på sådana betalningslösningar och har under de senaste åren ofta diskuterats i medierna, på arbetsplatser och vänner emellan. Olika faktorer har bidragit till nyfikenheten på hur valutan fungerar, såsom den påstådda anonymiteten för användarna, att banker inte är inblandade i betalningarna, möjligheten att göra betalningar över hela världen. Samtidigt är det svårt att förstå vad Bitcoin egentligen är och hur den fungerar. I den här artikeln försöker jag förklara detta.

Jag börjar med att förklara vad en virtuell valuta är, vilka olika slags virtuell valuta som finns och var Bitcoin passar in i den kategoriseringen. Därefter förklarar jag hur Bitcoin fungerar och vad vi vet om dess användning i Sverige. Slutligen diskuterar jag nytta och risker med Bitcoin samt vilka svårigheter Bitcoin kan komma att stå inför i framtiden.

* Jag vill tacka de personer som bidragit med värdefulla synpunkter. De är för många att nämnas men jag vill speciellt tacka Malin Alpen, Susanna Grufman, Marianne Sterner, Claes Berg och Kristian Jönsson.

Virtuell valuta

Bitcoin är en så kallad virtuell valuta.[1] En virtuell valuta är ett betalningsmedel, det vill säga att enheter av den virtuella valutan representerar ett värde. Den är avsedd att användas för betalningar inom en specifik virtuell gemenskap, som en viss webbplats, eller i ett nätverk av användare med en speciell mjukvara för att hantera den virtuella valutan och göra betalningar. En sådan virtuell gemenskap kan alltså liknas vid en frivillig överenskommelse att använda något specifikt som betalningsmedel. Detta är en viktig skillnad gentemot nationella valutor såsom exempelvis den svenska kronan. Där har vi i lag slagit fast att penningenheten i Sverige ska kallas krona. Den virtuella valutan har alltså en annan mynt-/räkneenhet än nationella valutor. För Bitcoin är räkneenheten just Bitcoin.

Utgivaren av den virtuella valutan kan vara ett icke-finansiellt företag eller till och med en privatperson, men denne står inte under tillsyn av någon statlig myndighet. Utgivningen av virtuell valuta är alltså inte någon statligt reglerad verksamhet.[2] Däremot har varje virtuell valuta någon form av eget regelverk som styr var och hur den kan användas och någon form av teknisk infrastruktur där betalningarna genomförs. Den virtuella valutan, det egna regelverket och den tekniska infrastrukturen utgör tillsammans ett litet betalningssystem, hädanefter kallat virtuellt valutasystem.

Det finns en stor mängd olika virtuella valutasystem som är uppbyggda och fungerar på olika sätt. De kan delas upp i olika kategorier beroende på i vilken utsträckning det är möjligt att köpa och sälja den virtuella valutan. Här delar vi upp dem i slutna, enkelriktade och dubbelriktade virtuella valutasystem. I slutna virtuella valutasystem kan den virtuella valutan varken köpas eller säljas utan endast intjänas och användas på vissa webbplatser (exempelvis World-of-Warcraft Gold). Om den virtuella valutan kan köpas för nationell valuta men inte växlas tillbaka är systemet enkelriktat (exempelvis Amazon coins). När den virtuella valutan kan både köpas och säljas samt användas utanför en viss webbplats är systemet dubbelriktat. Som förklaras nedan är Bitcoin ett exempel på ett dubbelriktat system. Dessa kategorier kan dock överlappa varandra.[3]

En ytterligare distinktion som kan göras är huruvida den virtuella valutan är centraliserad eller decentraliserad. Liksom med sedlar och mynt genomförs betalningar med de virtuella valutaenheterna genom att de byter ägare. Ägarförhållanden måste således registreras någonstans, annars kan det vara frestande för innehavaren av en virtuell valutaenhet att kopiera den och använda den flera gånger. Med ett centraliserat virtuellt valutasystem menas att det finns en centraliserad lösning för att verifiera och utföra transaktionerna, ofta

1 Begreppet virtuell valuta används av ECB (2012) och vi följer deras terminologi. I andra artiklar används ibland andra benämningar, till exempel digital valuta. Det är dock tveksamt om Bitcoin är en valuta i egentlig mening, se Yermack (2014).

2 Utgivning av virtuell valuta måste särskiljas från att erbjuda olika former av betaltjänster i virtuell valuta. Tillhandahållare av finansiella tjänster, också i virtuell valuta, lyder under penningtvättsregelverket. Beträffande betaltjänster regleras de främst genom betaltjänstelagen (2010:751) som anger rättigheter och skyldigheter för både betalningsförmedlaren och användarna av betaltjänsten. Detta gäller dock bara om verksamheten sker i Euro eller annan EES-valuta men i princip skulle lagen kunna utvidgas till att även gälla andra valutor, inklusive virtuell valuta.

3 Se Segendorf (2014) för en mer noggrann beskrivning av de olika kategorierna.

hos utgivaren. I praktiken administrerar denna alla de konton som betalningarna går mellan. I ett decentraliserat virtuellt valutasystem, såsom Bitcoin, verifieras och utförs transaktionerna i stället via nätverket av användare som utför någon form av aktivitet för att göra detta. Rätten att registrera händelser är alltså delegerad till nätverkets deltagare. [4] De decentraliserade virtuella valutasystemen bygger inte sällan på en utväxling av krypterade meddelanden och brukar därför kallas för kryptovalutor. Den anonymitet och säkerhet som detta medför är bärande tankar bakom Bitcoin.

Hur fungerar Bitcoin?

Bitcoin är ett decentraliserat dubbelriktat virtuellt valutasystem och en kryptovaluta.[5] Den har konstruerats för att vara oberoende av stater, banker och andra institutioner. På ett övergripande plan fungerar Bitcoin ungefär som en form av elektroniska kontanter. Det går att köpa Bitcoins på speciella webbplatser både utomlands och i Sverige där Bitcoins växlas mot nationell valuta.[6, 7] Bitcoins växelkurs bestäms av marknaden som en funktion av utbud och efterfrågan.

Betalningar med Bitcoin kan göras mellan alla som har en lämplig mjukvara på sin dator, smarta mobiltelefon eller surfplatta. En sådan mjukvara kallas *wallet* (digital plånbok). Ändå ska man inte tänkta på Bitcoin som en form av digitala kontanter. Anledningen är att Bitcoin inte är digitala värdeenheter som ligger lagrade på exempelvis en dator. En Bitcoin är alltså inte en digital sedel eller mynt och bör inte liknas vid vanliga sedlar och mynt. Snarare ska man tänka på Bitcoin som medel på ett konto. Vid en betalning sänder således inte den betalande parten digitala sedlar och mynt till mottagaren utan betalningen sker som en debitering på avsändarens konto och en kreditering på mottagarens konto. Betalningarna sker genom utväxling av kodade meddelanden och verifieras inom nätverket av användare. Hur detta går till redogör jag för nedan.

4 Också de traditionella massbetalningarna kan delas upp i centraliserade och decentraliserade system. Kontanter är ett decentraliserat system där det räcker att den betalande och mottagande parten är överens om betalningens giltighet för att den ska accepteras. Övriga massbetalningar såsom giro, autogiro, kort och checkar är centraliserade i och med att de clearas centralt och att avvecklingen av betalningarna sker hos ett avvecklingsinstitut, vanligtvis Riksbanken. Se Sveriges riksbank (2013) för en redogörelse för clearing och avveckling av massbetalningar.

5 Bitcoin lanserades 2009 av Satoshi Nakamoto som möjligtvis är en pseudonym. Fram till 6 mars 2014 när Newsweek hävdade att man funnit den riktige Satoshi Nakamoto var alla övertygade om att den riktige grundaren, eller gruppen av grundare, var okänd. Den identifierade mannen har förnekat att han är den riktige Satoshi Nakamoto. Det är i dagsläget osäkert om det är den riktige Satoshi Nakamoto som hittats. Källa: http://mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html och http://www.coindesk.com/one-simply-find-satoshi-nakamoto/

6 Olika växlingsplatser erbjuder lite olika tjänster. En del växlar enbart medan andra kan erbjuda konton. Det finns också webbplatser som matchar köpare och säljare geografiskt. I Sverige och de flesta andra länder är företag som tillhandahåller växlingstjänster reglerade och står under tillsyn.

7 Den klart största internationella växlingsplatsen har länge varit Mt.Gox. I slutet av februari 2014 upptäcktes en större stöld/bedrägeri varpå Mt.Gox kom på ekonomiskt obestånd och försattes i konkurs.

ASYMMETRISK KRYPTERING GER SÄKRA BETALNINGAR

Jag börjar med att förklara begreppet assymmetrisk kryptering och hur avsändaren (person A) och mottagaren (person B) av kodade meddelanden kan identifieras på ett säkert sätt. Assymmetrisk kryptering bygger på att A och B har två stycken kodnycklar vardera. Kodnycklarna är unika och ingen kan ha samma nycklar som någon annan. Den ena nyckeln är publik, det vill säga att den är eller kan göras allmänt känd, medan den andra är privat, det vill säga hemlig. När A vill skicka ett kodat meddelande till B använder hon B:s publika nyckel för att koda meddelandet som sedan endast kan avkodas med B:s privata nyckel. B är alltså den enda personen som kan läsa meddelandet.

Assymmetrisk kryptering kan också användas för signering. Om A använder sin privata nyckel för att kryptera ett meddelande kan detta endast avkrypteras med A:s publika nyckel. Den som avkrypterar meddelandet kan då vara säker på att det är A som har skickat det – ingen annan har ju tillgång till A:s privata nyckel. Man kan likna det vid att A har signerat meddelandet.

Anta att A ska betala 1 Bitcoin (BTC) till B. A och B har var sin digital plånbok på sina datorer och varje sådan plånbok har en privat och en publik kodnyckel. En plånbok associeras med sin publika kodnyckel som fungerar som en adress eller ett kontonummer. Det är via sina plånböcker som A och B kommunicerar.

TRANSAKTIONEN VERIFIERAS AV NÄTVERKET

Transaktionen börjar med att B sänder sin publika kodnyckel (kontonummer) till A. A, eller rättare sagt A:s plånbok, skriver nu en betalningsinstruktion på 1BTC till B och signerar den med A:s privata nyckel. Betalningsinstruktionen sänds ut till nätverket av bitcoinanvändare. Man kan säga att transaktionen mellan A:s och B:s plånböcker föreslås till nätverket som nu ska bekräfta/verifiera transaktionen för att den ska bli giltig. Den metod man använder för att sända meddelandet till nätverket bygger på en teknik liknande fildelning (BitTorrent) som är vanlig för att sprida/dela filmer, musik med mera på Internet.

Verifieringen går till så här: Var tionde minut samlar ett visst slags deltagare i bitcoinnätverket upp de transaktioner som förslagits under den senaste tiominutersperioden. Detta sker automatiskt och omgången av uppsamlade transaktioner kallas för ett block och de speciella deltagarna kallas "miners".[8] Deras jobb är att verifiera transaktionen genom att addera det nya blocket (transaktionerna) till den så kallade blockkedjan (block chain) som är den officiella listan eller registret med verifierade bitcointransaktioner. Eftersom blockkedjan innehåller information om avsändande plånböcker, mottagande plånböcker och belopp så kan den användas för att verifiera hur många BTC som tillhör en specifik plånbok. Det är samma sak som att man kan beräkna saldot på ett vanligt bankkonto om man har tillgång till samtliga de transaktioner som gjorts till och från det kontot. En plånbok

8 Vem som helst kan bli en miner, det är ett val som man gör själv. Att de kallas miners beror på att den aktivitet de ägnar sig åt har liknats vid att gräva guld (mining) eftersom de belönas med nya Bitcoins. Liknelsen är dock illa vald eftersom Bitcoin, till skillnad från guld, inte har ett inneboende värde. För guld kommer detta värde från att det kan användas till smycken, i industriella processer osv.

kan därför ses som ett konto där den publika nyckeln fungerar som ett kontonummer för plånboken. En bitcointransaktion är inte fullständigt anonym. Eftersom den läggs till blockkedjan finns den registrerad och tillgänglig på Internet. Det är alltså ganska enkelt att identifiera vilka plånböcker transaktionen gått mellan. Däremot är det mycket svårt att knyta plånböcker till enskilda användare vilket innebär att transaktionen i praktiken är anonym.

Verifieringen av betalningarna sker genom att miners löser ett matematiskt problem där lösningen är svår att beräkna men lätt att verifiera när den väl beräknats. För att bättre förstå verifieringen måste man få en förklaring av begreppet hashfunktion. En hashfunktion är en funktion som omvandlar ett nummer eller en text av godtycklig längd till ett tal av en given längd.[9] Exempelvis kan de individuella siffrorna i ett tal adderas och om summan överstiger ett ensiffrigt tal adderas summans komponenter osv. Talet 678910 blir då 6+7+8+9+1+0 = 31 och 31 blir 3+1 = 4 varvid det flersiffriga talet har omvandlats till ett ensiffrigt tal. Låt x beteckna den ursprungliga blockkedjan, y de transaktioner som ska verifieras och z ett annat tal. Det matematiska problemet som ska lösas kan formuleras $f(x,y,z) \leq v$ där f är en hashfunktion och det gäller att finna ett tal z så att hashfunktionen antar ett lägre värde än v där v i det här fallet kan tolkas som hashfunktionens svårighetsgrad.

Miners tävlar mot varandra i att snabbast hitta en lösning. När en miner har funnit en lösning sänds lösningsförslaget ut i nätverket där andra miners enkelt kan verifiera om lösningen är korrekt eller inte. Ett beslut om att acceptera en lösning tas via majoritetsbeslut där röststyrkan hos en miner beror på hur stor beräkningskapacitet (datorkraft) hon tillför nätverket. När en lösning har stöd hos miners som representerar en majoritet av nätverkets beräkningskapacitet anses lösningen vara accepterad. De föreslagna transaktionerna läggs nu till blockkedjan som blir ett block längre. I och med att transaktionen mellan A och B har blivit accepterad är nu B ägare till de överförda 1BTC som har krediterats hennes plånbok. Samtidigt har A:s plånbok debiterats med 1BTC.

MINERS FÅR NYA BITCOINS FÖR BESVÄRET

Incitamentet för miners att investera datorkraft i verifieringsprocessen är att de som ersättning får skapa nya Bitcoins. Det går till så att den miner som snabbast löste hashfunktionen, det vill säga först räknade ut z, som belöning också lägger till en extra "transaktion" till det block som ska verifieras (y). Denna transaktion krediterar minerns plånbok med N stycken BTC utan att någon annans plånbok debiteras. Med andra ord skapas det N stycken nya Bitcoins med den vinnande minern som ägare. Regelverket (protokollet)[10] som styr Bitcoin justerar varannan vecka svårighetsgraden v på hashfunktionen och det antal Bitcoins (N) som skapas vid varje verifiering. Justeringen ska säkerställa att nätverket kan verifiera transaktioner var tionde minut. Om datorkapaciteten i nätverket ökar kommer svårighets-

9 Den specifika hashfunktion som används i bitcoinprotokollet är SHA-256. För mer om denna funktion, se http://en.wikipedia.org/wiki/Sha-256

10 Ett protokoll är en uppsättning regler som hjälper de berörda datorerna att kommunicera över Internet. Ingen äger ett protokoll utan det är skapat för att vara en användbar standard.

graden också att öka, och vice versa. Antalet Bitcoin som skapas sjunker över tiden genom att N halveras efter 210 000 block vilket motsvarar ungefär 4 år. Initialt var $N = 50$ och nu är $N = 25$. Att N minskar över tiden gör att det finns en övre gräns på 21 miljoner för hur många Bitcoins det kan finnas. Denna gräns kan ses som ett matematiskt gränsvärde som aldrig nås även om antalet BTC kan komma godtyckligt nära. Vid halvårsskiftet 2014 fanns det nära 13 miljoner BTC.

Detta sätt att skapa nya Bitcoins gör att det, till skillnad mot de nationella valutorna som ges ut av centralbanker, inte finns någon central utgivare av Bitcoin – nyskapandet av Bitcoin styrs ju av dess protokoll. Bitcoin är därför inte heller en monetär fordran på någon. Svenska sedlar och mynt är formellt en fordran på Riksbanken och tillgodohavanden hos en bank är en fordran på banken som backar upp denna med sin balansräkning. En Bitcoins värde baseras alltså inte på någon form av fordran eller underliggande tillgång utan dess marknadsvärde beror enbart på en förväntan att den kan användas i transaktioner i framtiden.

BETALNINGEN SKER INTE I REALTID

En betalning med Bitcoin är ingen realtidsbetalning. Det kan ta upp till tio minuter innan en betalning verifieras och tumregeln är att man dessutom bör vänta sex verifikationsomgångar för att vara säker på att betalningen verkligen lagts till blockkedjan.[11] Att få en bitcoinbetalning verifierad kan alltså ta upp emot en timme. Beroende på situationen kan detta upplevas som en lång eller kort tid. Det är också värt att notera att det på grund av fildelningstekniken och verifikationsprocessen inte finns någon central lagringsplats för blockkedjan. Varje deltagare i nätverket har information om hela eller delar av blockkedjan.

Ruta 1. Elektroniska pengar är inte virtuell valuta

Begreppet elektroniska pengar ska inte förväxlas med virtuell valuta. Elektroniska pengar är ett elektroniskt förvarat penningvärde som representerar en fordran på utgivaren, har ett värde högst motsvarande det belopp de köpts för och som accepteras av andra än utgivaren.[12] Med det sistnämnda avses att e-pengarna ska accepteras av en tillräckligt bred krets av företag. Bitcoins är alltså inte elektroniska pengar, bland annat för att de inte representerar någon fordran på utgivaren.

I allmänhet kan en virtuell valuta uppfylla ett par av kriterierna ovan, men inte alla. Exempelvis uppfyller de flesta virtuella valutor inte kravet på tillräckligt bred krets av mottagare. Det är inte heller alltid möjligt att lösa in den virtuella valutan mot nationell valuta. Virtuella valutor anges också i andra räkneenheter än de nationella. Detta är en viktig skillnad gentemot elektroniska pengar. Återlösen

11 Rekommendationen kommer från Bitcoin.se. Den underliggande anledningen till att man bör vänta ett par verifieringsomgångar är en konsekvens av den decentraliserade verifieringsprocessen. Enkelt uttryckt kan det uppkomma olika versioner av blockkedjan. I dessa fall anses den längsta blockkedjan vara den riktiga. Den transaktion som nyss har verifierats finns registrerad i det sista blocket i blockkedjan. Om det skulle uppstå dubbla versioner finns det alltså en risk den andra versionen av blockkedjan väljs som den riktiga av nätverket och därmed att den det sista blocket ser annorlunda ut. Finns inte transaktionen längre med i blockkedjan är den inte heller verifierad. Det är därför klokt att vänta ett par verifieringsomgångar för att eliminera risken att blockkedjan ändras.

12 Se Sveriges riksbank (2013) för en beskrivning av lagen.

behöver inte ske med ett ett-till-ett förhållande eftersom värdeenheterna är olika. Vid eventuell återlösen eller växling till nationell valuta kan värdet vanligtvis inte förutses eftersom växelkursen varierar. Kontrollen av den virtuella valutans regelverk ligger hos utgivaren. Det finns ingen tillsyn över valutan och utgivaren är vanligtvis ett icke-finansiellt företag. Betalningar via virtuella valutasystem omfattas alltså inte av lagen (2011:755) om elektroniska pengar eller lagen (2010:751) om betaltjänster. Utgivaren finns dessutom vanligtvis inte i Sverige.

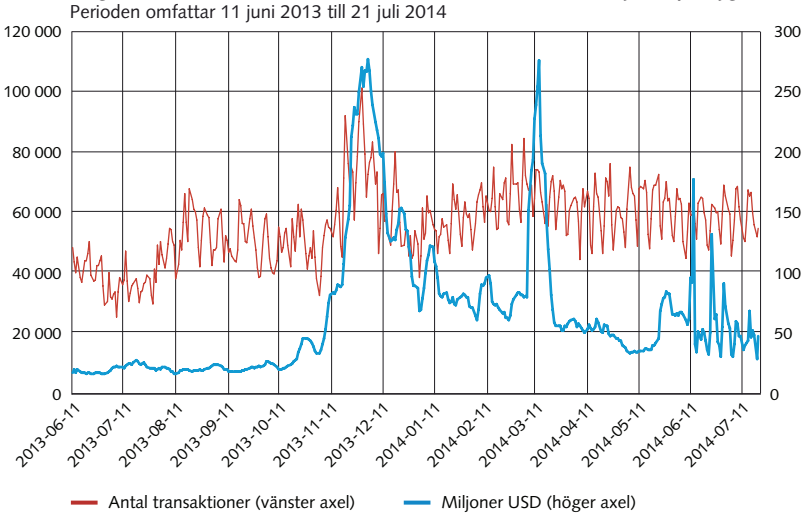
I vilken omfattning används Bitcoin?

Det finns statistik om alla transaktioner som gjorts med Bitcoin från 2009 och framåt. Denna statistik kommer från blockkedjan och är i princip tillgänglig för alla. Vissa analyser finns tillgängliga på Internet och ger en bild av den globala användningen av Bitcoin. Det är däremot inte möjligt att se hur stor användningen är i ett visst land eftersom innehavarna av de digitala plånböcker som transaktionerna gått mellan inte kan identifieras.

LITEN ANVÄNDNING AV BITCOIN GLOBALT

Under det senaste året har det i genomsnitt gjorts nästan 60 000 bitcointransaktioner per dygn. Som lägst var antalet drygt 28 000 per dygn och som högst drygt 100 000. Det motsvarar ungefär 0,1 promille av antalet kortbetalningar. Det totala värdet, mätt i miljoner USD, har också varierat kraftigt – delvis som en följd av stora variationer i växelkursen. I genomsnitt var det sammanlagda värdet inte mer än cirka 64 miljoner USD per dygn. Diagram 1 visar antalet transaktioner per dygn och det totala förmedlade värdet.

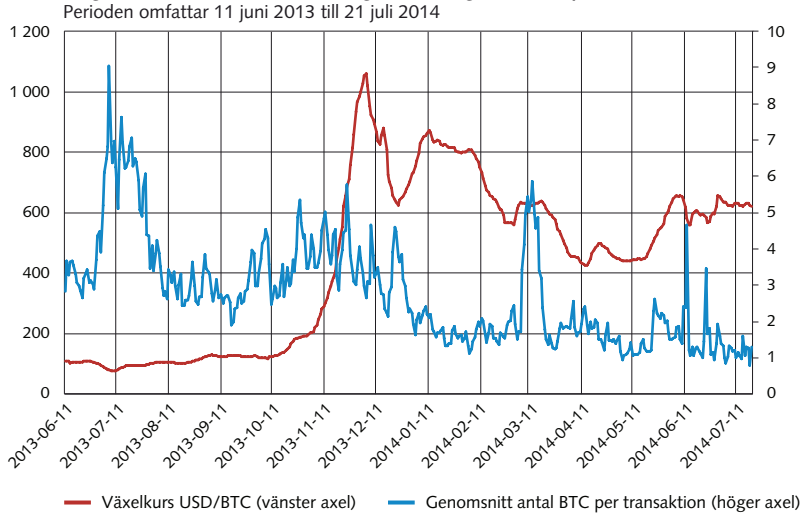
Diagram 1. Antal bitcointransaktioner och förmedlat värde (USD miljoner) per dygn
Perioden omfattar 11 juni 2013 till 21 juli 2014



Källa: Blockchain.info. Bearbetning av Riksbanken

Det genomsnittliga transaktionsvärdet, mätt i BTC, har sjunkit något över tiden, troligtvis som en följd av att växelkursen stärktes markant under hösten 2013. Diagram 2 visar växelkursen och antalet Bitcoin per transaktion. Uppgången i det förmedlade värdet under hösten 2013 förklaras ofta med ökad efterfrågan på Bitcoin från Kina.

Diagram 2. Växelkurs USD/BTC och genomsnittligt antal BTC per transaktion
Perioden omfattar 11 juni 2013 till 21 juli 2014



Källa: Blockchain.info. Bearbetning av Riksbanken

Endast 4 % av alla Bitcoins omsätts inom en vecka av sina innehavare. När tidsspannet ökas till tre månader omsätts ytterligare 24 procent. Först efter sex månader har mer än hälften omsatts. Ungefär 38 procent hålls mer än ett år.[13] Innehavarna av Bitcoins tycks alltså inte omsätta dem särskilt ofta. Till saken hör också att många miners, speciellt större aktörer eller sådana miners som samarbetar i pooler, ofta omgående omsätter sina intjänade Bitcoins till nationell valuta för att täcka sina omkostnader. Det faktum att endast en liten del av alla Bitcoins tycks användas för transaktioner antyder att större delen av dem innehas för mer långsiktiga syften, till exempel för växelkursspekulation eller sparande.

ÄNNU MINDRE ANVÄNDNING AV BITCOIN I SVERIGE

En grov uppskattning ger vid handen att det i mitten av augusti 2014 fanns ett trettiotal företag/webbplatser som accepterar Bitcoin i Sverige.[14] Det är främst fråga om små företag och Bitcoin tycks inte ha någon bred acceptans som kommersiellt betalningsmedel. Det är därför troligt att en stor del av bitcointransaktionerna där avsändaren eller mottagaren befinner sig i Sverige sker mellan privatpersoner eller till webbplatser utomlands.

Transaktioner med Bitcoin är anonyma och det går inte att ta fram statistik över betalningar där en av parterna finns i Sverige. Däremot finns det vissa data över antalet och

13 Källa: Swanson (2014).
14 Källa: bitcoin.se

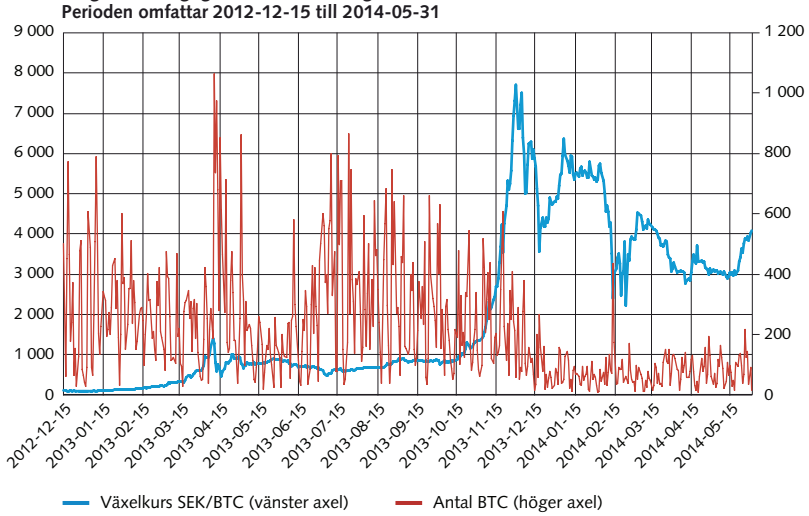
värdet på växlingstransaktioner mellan BTC och SEK.[15] Tabellen nedan visar aggregerad information över den växlingstrafiken för perioden 15 december 2012 till 31 maj 2014. Dagligen växlades i genomsnitt 266 000 kronor. Den stora volatiliteten i växlingstransaktionerna illustreras i diagram 3. Det sammanlagda värdet av växlingstransaktionerna mellan BTC och SEK förefaller uppgå till ett par procent av motsvarande värde för växling mellan BTC och EUR och mindre än 1 % av växlingsvärdet mellan BTC och USD. SEK är alltså en liten valuta i bitcoinsammanhang. Att växling mellan BTC och SEK är en liten marknad framgår också om man jämför den med de 25 miljarder SEK som i genomsnitt dagligen växlas avista till och från USD.[16]

Tabell 1. Dagliga värden för växling mellan Bitcoin och SEK
Perioden omfattar 2012-12-15 till 2014-05-31

	VOLYM (BC)	VÄXELKURS (SEK)	OMSÄTTNING (SEK)
Medelvärde	212	1 995	265 501
Min	7	89	2 536
Max	1 065	7 720	2 574 066
Standardavvikelse	184	1 916	312 520

Källa: http://bitcoincharts.com, Safello och BTCX. Bearbetning Riksbanken

Diagram 3. Dagliga värden för växling mellan BTC och SEK
Perioden omfattar 2012-12-15 till 2014-05-31



Källa: http://bitcoincharts.com, Safello och BTCX. Bearbetning: Riksbanken

15 Växlingar som svenska privatpersoner och företag gör mot exempelvis USD fångas inte in i denna statistik. Det är okänt hur omfattande växling svenska aktörer gör mot andra valutor. Exempelvis anger Dagens Industri (2014) att KNC Miner tjänar 3 miljoner kronor per dag i att bryta Bitcoin men att de alltid växlar detta till USD.

16 Avser genomsnitt för juni 2014. Källa: http://www.riksbank.se/Documents/Statistik/Turnover/2014/stat_oms-FX_1406_sve.xls

Det är osäkert hur väl växlingstransaktionerna återspeglar betalningstrafiken med Bitcoin. Om Bitcoin återanvänds för betalning utan att växlas in till kronor däremellan så underskattas användningen av Bitcoin i betalningssyfte, men om Bitcoin köps och hålls i spekulativt syfte överskattas den. Om svenska innehavares användning liknar den globala användningen bör lejonparten av innehavet vara sparande eller spekulation och växlingstransaktionerna bör då överskatta mängden rena bitcoinbetalningar. Oavsett vilket som är fallet är det små värden i relation till det svenska betalningssystemet. Totalt uppgår hushållens betalningar till ungefär halva BNP under ett år. I genomsnitt blir det mer än 4,5 miljarder kronor per dag. Bara med kort och kontanter gör hushållen mer än 8 miljoner betalningar till ett värde av mer än 3 miljarder kronor per dag. Även om användningen av Bitcoin i Sverige skulle vara betydligt större än det växlade värdet är det jämförelsevis mycket låga värden.

FUNGERAR BITCOIN SOM EN VALUTA?

En valuta har tre funktioner. För det första fungerar den som betalningsmedel, i form av sedlar och mynt. För det andra tjänar den som en räkneenhet som vi använder för att uttrycka priser, sparande, huslån och så vidare i termer av exempelvis kronor och ören. För det tredje fungerar den som en värdebevarare vid sparande, det vill säga att jag kan avstå från konsumtion idag, lägga pengarna under madrassen och konsumera för dem i morgon.

Ur en principiell synvinkel kan Bitcoin sägas fylla en valutas tre roller men i praktiken gör den det inte. Rollen som betalningsmedel förutsätter att det i samhället finns en bred acceptans för valutan, annars är det svårt att genomföra betalningar med den. I Sverige finns ingen sådan bred acceptans och möjligheterna att använda Bitcoin som betalningsmedel är därför i praktiken mycket begränsade. Likaså är det ovanligt att priser uttrycks i termer av Bitcoin även om det naturligtvis förekommer. Bitcoin kan därför inte heller sägas fungera som en allmänt vedertagen räkneenhet. Slutligen gör den höga volatiliteten i Bitcoins växelkurs den olämplig som värdebevarare eftersom dess köpkraft kan minska mycket snabbt och en stor del av värdet går då förlorat.

Ytterligare en skillnad mellan Bitcoin och traditionella nationella valutor, såsom den svenska kronan, är att de senare har en speciell legal status i det land där de ges ut. I Sverige slås det i riksbankslagen fast att penningenheten i Sverige heter krona, att den indelas i hundra ören, att endast Riksbanken kan ge ut sedlar och mynt och att dessa är lagliga betalningsmedel, det vill säga att det finns en skyldighet mottagaren av en betalning att acceptera kontanter.[17]

Nytta och risker med Bitcoin för användaren

För den individuella användaren finns både för- och nackdelar med Bitcoin, beroende på betalningssituationen. Fördelarna rör främst anonymitet/integritet, smidighet, snabbhet och kostnader. Nackdelarna rör främst att det inte finns någon form av skydd för användaren. I

17 Lagen om Sveriges Riksbank (1988:1385).

vissa situationer kan fördelarna överväga och i andra i stället nackdelarna. Vanligtvis torde fördelarna överväga i situationer där det inte finns enkla och kostnadseffektiva traditionella betaltjänster.

BITCOIN SKYDDAR ANVÄNDARENS IDENTITET

Det uttalade syftet med Bitcoin är att möjliggöra anonyma betalningar över Internet och att göra dem oberoende av stater, banker och andra institutioner. För användarna är alltså nyttan av Bitcoin att nätverket inom vilket betalningar förmedlas är globalt och att vissa betalningar som av integritetsskäl inte gjorts tidigare nu kan genomföras, både lokalt och globalt. Om en betalning på en webbplats reduceras till en knapptryckning i stället för att bygga på att man skriver in en mängd betalningsinformation i form av kortnummer med mera sänks den betalande partens (tids)kostnad för en betalning. Bedrägeririsken kan dessutom upplevas som lägre om inte kortnummer eller kontonummer behöver lämnas ut till mottagaren. Den personliga integriteten kan då också upplevas som högre. En virtuell valuta kan också tillåta användarna att göra betalningar till nya grupper av mottagare som det annars är svårt att nå, speciellt vid betalningar där avsändare och mottagare befinner sig i olika länder. För vissa sådana gränsöverskridande betalningar kan dessutom Bitcoin vara ett betydligt billigare och/eller smidigare alternativ till mer traditionella betaltjänster.

BITCOIN REGLERAS INTE AV NÅGON NATIONELL LAGSTIFTNING

Det finns ingen central utgivare av Bitcoins eftersom värdeenheterna skapas automatiskt inom nätverket. Bitcoin faller alltså inte under någon nationell lagstiftning och det finns inte heller någon att rikta eventuella anspråk mot. Betalningarna är också anonyma och det är i regel inte möjligt att visa att en betalning gjorts till en viss mottagare. Undantaget är om de inblandade parterna känner till varandras identiteter och det är möjligt att styrka vem som äger en viss digital plånbok. Det finns alltså endast en liten möjlighet för den enskilde användaren att hävda sin rätt om en betalning skulle gå snett.

Det som ur ett konsumentskyddsperspektiv skiljer en betalning i Bitcoin från en betalning i svenska kronor är just att bitcoinbetalningen förmedlas via ett globalt och decentraliserat nätverk utanför den finansiella sektorn. De regelverk som styr vanlig betalningsförmedling, såsom betaltjänstlagen, är inte tillämpliga och därmed har inte heller konsumenten samma skydd som vid exempelvis giro- eller kortbetalningar. Det kan med andra ord vara mer riskfyllt för den betalande parten att göra betalningar med Bitcoin än med traditionella betaltjänster.

BITCOINS VÄXELKURS VARIERAR KRAFTIGT

Bitcoin representerar inte någon fordran på någon annan utan dess värde består helt och hållet i förväntan att den kan användas i framtida transaktioner. Värdet är alltså mycket känsligt för förändringar i dessa förväntningar. Diagrammen 2 och 3 visar tydligt den stora volatiliteten hos Bitcoins växelkurs. Beroende på vid vilken tidpunkt någon köper eller tar

emot Bitcoin kan stora växelkursvinster eller förluster göras. Huruvida detta är dåligt eller inte beror på i vilket syfte som man håller sina Bitcoins. Är det i rent transaktionssyfte brukar växelkursrisk anses vara någonting negativt eftersom det gör betalningen mer riskfylld, det vill säga avsändaren och mottagaren av betalningen får svårare att sätta priser i BTC. Detta upplevs som en ökad transaktionskostnad.

För innehavaren av Bitcoin finns också en risk att förlora värdet, antingen genom bedrägeri eller olyckshändelse. Detta beror på att den digitala plånboken och kodnycklarna lagras på någon form av medium, exempelvis en hårddisk. Om hårddisken av någon anledning skulle förstöras går också informationen förlorad och därmed tillgången till de Bitcoin som finns registrerade i plånboken. Via dataintrång kan någon extern part också komma över värdet genom att initiera en betalning till en plånbok som denne kontrollerar. Det har skett bedrägerier och det främsta exemplet är det som skedde mot växlingsföretaget Mt Gox där flera hundra tusen Bitcoins gick förlorade.[18] Bitcoins är på det sättet mer lika kontanter än banktillgodohavanden. Tappar du bort eller oavsiktligt förstör kontanter är det monetära värdet förlorat. De kan också stjälas. Banktillgodohavanden är mer skyddade. Om banken agerar försumligt är den ersättningsskyldig, agerar du själv försumligt finns det en lagstadgad gräns för din ersättningsskyldighet och skulle banken gå i konkurs finns det en statlig insättningsgaranti som skyddar ditt tillgodohavande upp till ett värde motsvarande EUR 100 000.

Nytta och risker för samhället

Den nytta samhället har av en virtuell valuta som Bitcoin är främst av tre slag. För det första kan betalningar i Bitcoin vara mer kostnadseffektiva än traditionella betalningar i vissa situationer. Bitcoin kan alltså i en del fall innebära besparingar och därmed ett effektivare betalningssystem.

För det andra kan en virtuell valuta som Bitcoin på sikt bidra till ett mer robust betalningssystem genom att inte alla betalningar går genom den traditionella finansiella infrastrukturen som utgör knutpunkter där betalningsflödet koncentreras.[19] Om en sådan knutpunkt skulle bli satt ur funktion av någon anledning upphör också den relaterade

18 Mt Gox var världens största växlingsföretag för virtuell valuta. De var lokaliserade i Japan och erbjöd sina tjänster globalt. Mt Gox har själva har varit mycket förtegna kring händelsen men följande tros ha hänt: en/flera hackare tycks ha manipulerat blockkedjan så att det verkade som om inte utbetalningen av Bitcoin gick igenom till köparen. Mt Gox gjorde då automatiskt en ny utbetalning och har på så sätt under en längre tid långsamt dränerats på Bitcoin. Mt Gox började få svårigheter att göra utbetalningar i slutet av 2013 och stoppade utbetalningar i början av februari 2014. Totalt tycks ca 850 000 Bitcoins ha försvunnit. Marknadsvärdet torde då uppgå till ett par tre miljarder kronor. I Kanada har Flexcoin, en bitcoinbank/växlingssite, blivit bestulet på bitcons motsvarande USD 600 000. Källa: http://www.businessweek.com/articles/2014-02-26/where-did-the-bitcoins-go-the-mt-dot-gox-shutdown-explained#r=read

19 Se Sveriges riksbank (2013). Kapitel 1 förklarar hur det svenska betalningssystemet fungerar och kapitel 6 diskuterar framtida risker.

betalningstrafiken. Bara det faktum att det finns alternativa vägar för vissa slags betalningar är positivt ur ett kontinuitetsperspektiv.[20]

För det tredje finns det en potentiell nytta i form av innovation av nya betaltjänster och finansiella tjänster som kan byggas kring Bitcoin. En annan viktig aspekt är att Bitcoins protokoll ligger allmänt tillgängligt på Internet och att det kan ändras om en majoritet av nätverkets beräkningskapacitet stödjer en sådan förändring.

De risker som Bitcoin kan medföra för betalningssystemet är främst av två slag. För det första finns det en risk att ett eventuellt misstroende mot Bitcoin skulle kunna sprida sig och leda till ett mer omfattande misstroende också mot andra aktörer på massbetalningsmarknaden. Detta skulle kunna innebära att konsumenter och företag väljer bort även säkra betaltjänster och aktörer till förmån för kanske kostsammare och långsammare betaltjänster. Marknaden skulle då fungera sämre.

För det andra, om centrala aktörer på massbetalningsmarknaden såsom banker och finansiell infrastruktur skulle ha stora innehav av Bitcoin skulle detta kunna exponera dem för stora finansiella risker. Det är de som tillhandahåller betaltjänster till hushåll och företag och om ett par sådana aktörer vid samma tillfälle hamnar på obestånd skulle det kunna försämra marknadens funktion, åtminstone temporärt. På samma sätt kan det teoretiskt uppkomma risker för den finansiella stabiliteten om viktiga finansiella institutioner är direkt exponerade mot den virtuella valutan eller om det uppstår kreditförluster genom att institutionens kunder är starkt exponerade.

LITEN ANVÄNDNING INNEBÄR LITEN NYTTA OCH SMÅ RISKER

Det är i dagsläget mycket små belopp som omsätts i Bitcoin på den svenska marknaden och det finns inget som tyder på att centrala aktörer innehar Bitcoins. Det gör att såväl den potentiella välfärdsvinsten som systemriskerna är mycket små och slutsatsen är därför att Bitcoin hittills inte har haft någon mätbar inverkan på den svenska massbetalningsmarknaden eller den finansiella stabiliteten.

En annan typ av problem på samhällsnivå är dock att vissa virtuella valutasystem, såsom Bitcoin, som tillåter anonyma betalningar kan användas för penningtvätt och i andra kriminella syften.[21] Ingen vet hur stor den kriminella användningen av Bitcoin är, men anekdotiska exempel (se fotnot 21) antyder att det kan vara fråga om betydande belopp.

20 Riksbanken och den aktuella infrastrukturen arbetar därför aktivt med att förebygga risker i den centrala finansiella infrastrukturen, se Sveriges riksbank (2012). Riksbanken bedömer att den svenska finansiella infrastrukturen är säker och håller hög internationell standard, se Sveriges riksbank (2014).

21 Webbplatsen "Silk Road" där droger och kriminella tjänster bjöds ut mot Bitcoin är det mest kända exemplet. Den stängdes av FBI i oktober 2013. En ny webbplats, Silk Road 2.0 öppnades dock snart under annan ledning än den ursprungliga webbplatsen. Den nya webbplatsen stängdes dock i mitten av februari 2014 eftersom Bitcoins för ca USD 2,5 miljoner saknades – troligen genom förskingring. Penningtvätt är ett annat bekymmer. Webbplatsen Liberty Reserve som användes för omfattande penningtvätt stängdes i maj 2013. Bedragare hade tillskansat sig vanlig valuta och växlat denna till Bitcoin som sedan sänts iväg och inte kunnat spåras.

Hur ser framtiden ut för Bitcoin och andra virtuella valutor?

Bitcoin tycks endast i liten utsträckning användas för betalningar. I stället hålls valutan främst i spekulationssyfte eller som ett sparande. Om Bitcoin ska ta marknadsandelar från de traditionella betaltjänsterna behöver den alltså användas för betalningar i mycket större utsträckning än idag. Vad kan då hindra en sådan utveckling? Vilken roll kan andra virtuella valutor spela i framtiden?

KONSUMENTSKYDD OCH TILLSYN SAKNAS

Det som troligtvis främst gör det svårt för Bitcoin att växa som betalningsmedel är frånvaron av konsumentskydd och tillsyn från myndigheternas sida. Anledningen till detta är enkel. Om Bitcoin i stor omfattning ska användas för betalningar betyder det också att en stor del av konsumenterna ska vara beredda att hålla Bitcoins. Om Bitcoins upplevs som riskfyllda är det mindre troligt att allmänheten är beredd att göra detta. Jag har tidigare i artikeln påtalat den här bristen på konsumentskydd vid betalningar med Bitcoin. Innehav av Bitcoin är också mer riskabelt än ett banktillgodohavande. Det är därför troligt att Bitcoin på något sätt måste föras in under samma eller motsvarande regelverk som gäller för andra betaltjänster eller kontotillgodohavanden för att kunna få en bred acceptans – för annat än mycket små betalningar.

Att på så vis göra användningen av Bitcoin mer lik traditionella betalningar är dock samtidigt att avvika från den grundläggande tanken med Bitcoin, nämligen att den ska vara oberoende av stater och den finansiella sektorn. Det kan också bli svårt för staten att skapa nödvändiga regelverk. Hur reglerar man exempelvis något som är decentraliserat och inte har en utgivare?

FUNGERAR INTE FÖR ALLA TYPER AV BETALNINGAR

Ett annat hinder är att Bitcoin inte lämpar sig för alla slags betalningar. Betalningarna med Bitcoin sker ju inte i realtid. Betalningar verifieras var tionde minut men det rekommenderas dessutom att man väntar tills ytterligare fem verifieringar har skett om man vill vara säker på att transaktionen verkligen adderats till blockkedjan. Det kan alltså ta upp till en timme innan man kan vara säker på att betalningen verkligen gått igenom. Det gör Bitcoin olämplig vid många vanliga betalningar, till exempel i kassan på snabbköpet. Kortbetalningar, som inte heller sker i realtid eftersom mottagaren får pengar på sitt konto en eller flera dagar senare, löser detta problem genom att reservera medel på den betalande partens konto och garantera betalningen till mottagaren. Bitcoin som inte har någon central utgivare eller verifieringsprocess kan inte göra detta. Däremot kan enskilda betaltjänstleverantörer garantera bitcoinbetalningar gentemot sina kunder. Men att hitta en garanti som understödjer den decentraliserade användningen av Bitcoin fri från centrala aktörer är svårt.

TROVÄRDIGHETSPROBLEM AV TEKNISK NATUR UTGÖR OCKSÅ HINDER

Bitcoins funktion bygger på att miners verifierar transaktioner. Incitamenten för dem att göra detta består främst i att miners blir tilldelade nya Bitcoins. Detta incitament kan dock urholkas, vilket kan bidra till att trovärdigheten för den virtuella valutan eroderar.

Ett skäl är att nyskapandet av Bitcoins avtar över tiden.[22] Detta riskerar minska incitamentet för miners att fortsätta sin verksamhet. En annan är den övre gränsen på hur många Bitcoins som kan finnas (21 miljoner). Det grundläggande problemet är att virtuell valuta enkelt kan nyskapas. Om 21 miljoner Bitcoins plötsligt kan bli 42 miljoner kommer också varje enskild Bitcoin att bli mindre värd. Att hålla den övre gränsen på 21miljoner Bitcoins är därför viktigt för att bibehålla trovärdigheten kring Bitcoins framtida värde. Den trovärdigheten påverkas av hur stabilt det protokoll som styr Bitcoin upplevs vara. I samband med problem eller en kris kan protokollet snabbt behöva ändras. Men om det bedöms vara alltför lätt att ändra protokollet finns också en risk att den övre gränsen för antalet Bitcoin blir mindre trovärdig.

Ytterligare ett skäl till att incitamenten för miners kan urholkas är att växelkursen kan sjunka vilket skulle minska belöningens värde. Till det kommer att det kan bli för dyrt med datorkraft och elektricitet. I takt med att hashfunktionen blir mer komplex krävs alltmer datorkraft och specialbyggda datorer.

Ett annat potentiellt problem är att längden på blockkedjan ökar ständigt. Idag uppgår den till över 14 gigabytes. Bitcoins nätverk förutsätter att det finns ett stort antal noder som har hela blockkedjan lagrad på sina maskiner – detta gör nätverket robust. Incitamenten att hantera en sådan "full" nod har minskat och dessa noder verkar bli allt färre.[23] Det tycks med andra ord som om Bitcoin blir allt mer centraliserat och därmed mindre robust.

Om incitamenten för miners försvinner kommer den decentraliserade verifikationen av transaktioner att upphöra och Bitcoin kommer inte att gå att använda.

ANDRA VIRTUELLA VALUTOR KAN ERSÄTTA BITCOIN

Det finns således flera potentiella hinder för att Bitcoin skall kunna växa som betalningsmedel. Men det är också viktigt att komma ihåg att Bitcoin var den första virtuella valutan. Även om Bitcoins protokoll är förändringsbart och allmänt tillgängligt, vilket stimulerar ytterligare innovation kring Bitcoin, är det inte säkert att Bitcoin är slutpunkten för de virtuella valutornas evolution – det kan komma bättre lösningar som konkurrerar ut Bitcoin. Det finns idag det över 450 andra kryptovalutor och de blir ständigt fler.[24] Vissa av dem har utgått från Bitcoins konstruktion men vidareutvecklat eller förändrat den. Andra tycks ha kommit till som en del av en affärsmodell för att dra nytta av uppmärksamheten kring Bitcoin.

22 Som beskrivits ovan i avsnittet om hur bitcoinstransaktioner fungerar halveras belöningen (N) till miners ungefär var fjärde år.

23 Se Cawrey, D. (2014a) och (2014b).

24 Enligt http://coinmarketcap.com/ fanns det cirka 460 olika kryptovalutor i mitten av augusti 2014. I början av 2014 finns det mindre än hälften så många. De fem största i termer av utgivet värde är Bitcoin, Ripples, Litecoin, Peercoin och Mastercoin. Lite mer om andra virtuella valutor finns i Segendorf (2014).

Bitcoins framgång och framtid är alltså inte given. Det enda vi vet är att framtiden inte kommer att se ut som idag och hur vi kommer att betala om 25 eller 50 år är en öppen fråga.

Referenser

Cawrey, Daniel (2014a), "What Are Bitcoin Nodes and Why Do We Need Them?", www.coindesk.com, 9 maj, 2014.

Cawrey, Daniel (2014b), "The Five Biggest Threats Facing Bitcoin", www.coindesk.com, 26 maj, 2014.

Dagens Industri (2014), Drar in en halv miljard på bitcoin, artikel, mars 24, 214.

ECB (2012), *Virtual Currency Schemes*, oktober 2012.

Velde, François R. (2013), "Bitcoin – a primer", *Chicago Fed Letter*, nr. 317, December 2013.

Segendorf, Björn (2014), "Har virtuella valutor påverkat marknaden för betalningar?", *Ekonomisk kommentarer*, nr 2, Sveriges riksbank, 2014.

Sveriges riksbank (2012), *Riksbankens övervakning av den finansiella infrastrukturen.*

Sveriges riksbank (2013), "Den svenska massbetalningsmarknaden", *Riksbanksstudier*, Sveriges riksbank.

Sveriges riksbank (2014), *Finansiell infrastruktur.*

Swanson, Tim (2014), "What Block Chain Analysis Tells Us About Bitcoin", www.coindesk.com, 17 maj, 2014.

The Economist (2013), "Bitcoin under pressure", November 30.

Yermack, David (2014), "Is bitcoin a real currency – An economic appraisal", Working paper, New York University Stern School of Business och National Bureau of Economic Research.