Bitcoin som betalningsmedel

Victor Didriksson

Examensarbete för Tradenom-examen

Utbildningsprogrammet i Informationsbehandling

Raseborg 2014

EXAMENSARBETE

Författare: Victor Didriksson

Utbildningsprogram och ort: Tradenom, Raseborg

Inriktningsalternativ/Fördjupning: Informationsbehandling

Handledare: Tomas Hammar

Titel: Bitcoin som betalningsmedel

Datum: 3.5.2014 Sidantal: 38 Bilagor: 1

Sammanfattning

Examenarbetet skall ge en klar bild om vad virtuella valutor, främst Bitcoin, är för typ av finansinstrument. Jag beskriver hur de virtuella valutorna fungerar, hur de används och varför det lockar nya användare.

Jag fokuserar på Bitcoin eftersom det är den absolut största krypterade virtuella valutan idag, men jag har tagit upp ett par alternativ som har annorlunda tänktesätt entemot Bitcoin.

Samlingen av material har för det mesta skett via Internet, då det saknas böcker inom ämnet. Via Internet har jag strävat efter att samla på mig uppdaterad och trovärdig information. Jag intervjuade också två företag för att ta reda på varför just de har valt att börja acceptera Bitcoin som betalningsmedel och hur kundernas respons har varit.

Ämnet Bitcoin intresserade mig eftersom det är en ny lättillgänglig teknik, som det inte har forskats om så mycket tidigare. I vår media kan man idag läsa artiklar som berör Bitcoin, då och då men de går väldigt sällan desto mera in i systemet och förklarar inte det på en fördjupad nivå.

Resultatet av arbetet ger en klar bild över vad de virtuella valutorna har att erbjuda för nya positiva möjligheter i samhället, men också de stora problemen som de har framför sig.

Språk: Svenska Nyckelord: Bitcoin, E-handel, virtuella valutor

---

BACHELOR'S THESIS

Author: Victor Didriksson

Degree Programme: Business Information Technology, Raseborg

Specialization: Information Processing

Supervisor: Tomas Hammar

Title: Bitcoin as a payment method

Date: 3 May 2014 Number of pages: 38 Appendices: 1

Summary

The thesis strives to give a clear picture of virtual currencies, primarily Bitcoin, as a financial instrument. Is described how virtual currencies work, how they are used and why they attract new users.

The focus is on Bitcoin because it is the biggest encrypted virtual currency today, but also other currencies that differ from Bitcoin are presented. Internet has been the primary source of information, since there are no books on the subject yet. Through the Internet, I have endeavored to collect updated and credible information.

I also interviewed two companies to find out why they have decided to start accept Bitcoin as payment and what the customers' reaction has been.

The topic Bitcoin interests me because it is a new easily accessible technique, and there is not much prior research to be found. The media publishes articles related to Bitcoin occasionally, but how the virtual network operates is rarely explained.

The result of this work provides a good picture of new positive opportunities that virtual currencies can offer, but also possible problems that are involved.

Language: Swedish Key words: Bitcoin, E-commerce, virtual currencies

---

Innehållsförteckning

1 Förord

Ända sedan 600 f Kr har vi människor använt oss av någon form av pengar som ett värderingssystem och betalningsmedel för varor och tjänster. Det tog ända till mitten av 1600-talet innan vi nordbor började använda oss av sedlar, före det användes endast mynt. Hanteringen av pengar har utvecklas oerhört mycket sedan mitten av 1950-talet. Idag används ofta bankkort eller banktransaktioner vid handel. Bankkort och banktransaktioner är en relativt ny teknik, som vi anpassade oss snabbt till.

Bitcoin är en decentraliserad krypterad virtuell valuta, som introducerades den tredje januari 2009. I Finland är Bitcoin fortfarande väldigt främmande för de flesta, det är för det mesta endast teknik- och ekonomiintresserande som verkligen förstår vad valutan har att erbjuda.

De krypterade virtuella valutorna har idag stort stöd från utvecklare och användare runt om i världen. Många anser att det stora intresset för Bitcoin hänger ihop med misstron för våra stora banker och staternas hantering av valutorna. Det nuvarande penningsystemet har fått ta del av en hel del kritik och bankerna anses ha för mycket makt.

1.1 Syfte och mål

Syftet med arbetet är att belysa det nya betalningssystem som utvecklats i och med de krypterade virtuella valutorna. Kunskapen och kännedomen om betalningssystemet är fortsättningsvis obekant för den stora allmänheten. Det nya betalningssystemet har vissa fördelar och nackdelar jämfört med de nuvarande betalningssystemen som våra finans-institut erbjuder. Vidare är syftet att arbetet skall ge en klar bild hur Bitcoins nätverk fungerar och hur systemet har blivit bemött av myndigheter och av media. Det skall också framkomma vilka som har använt eller använder sig av Bitcoin och hur betalningssystemet har fungerat för användarna.

Slutmålet är att arbetet ska ge en informativ bild om de krypterade virtuella valutornas användbarhet för personliga syften samt användbarheten ur ett företags perspektiv.

Det var hösten 2013 som jag för första gången fick höra om den virtuella valutan Bitcoin, valutan fångade mitt intresse eftersom skiljer sig mycket jämfört med våra traditionella valutor. Jag har sedan dess läst artiklar i dagstidningar och studerat lite på Internet om de virtuella valutorna, men jag läste aldrig mera om i systemet på en djupare nivå. Med mitt arbete har jag tänkt få en bra uppfattning om vad de virtuella valutorna har att erbjuda till samhället och för problem de har framför sig. Jag har även haft som målsättning att undersöka möjligheterna till att finna olika informationskällor i ämnet och kritiskt granska dessa.

1.2 Metoder

Informations hämtningen har av naturliga skäl i första hand handlat om att använda sig av källor på Internet. E-böcker, officiella dokument av myndigheter, tidningsartiklar m.m. har även använts som källmaterial för forskningen. Personliga praktiska tester av Bitcoins funktionalitet och intervjuer av företag som accepterar Bitcoin som ett betalningsmedel redovisas även i arbetet.

Jag har i min utredning använt mig av den så kallade kombinerade metoden. Den kvantitativa metoden i används för samlandet av information och analyserande av denna. Den kvantitativa metoden redovisas i kartläggningen och beskrivningen av fenomenet Bitcoin. Den kvalitativa metoden har använts vid intervjuer och egna experiment. Samlandet av information från olika källor på Internet och från övriga publikationer, har varit utmanande då mitt forskningsobjekt varit mycket omskrivet och behandlat i media. Jag har valt att använda en kombinerad metod där jag både kan presentera forsknings-objektets uppkomst, statistiska data och erfarenheter av slutanvändare.

1.3 Avgränsningar

Fokuseringen kommer göras på Bitcoin, även fast det finns ett flertal med andra virtuella krypterade valutor. Men i dagsläget är det Bitcoin som är den stora ledaren och den som har fått mest uppmärksamhet i vår media. Ett par alternativ till Bitcoin behandlas men inte så ingående. Den komplicerade matematiken som ligger till grund för Bitcoins kryptering behandlas inte.

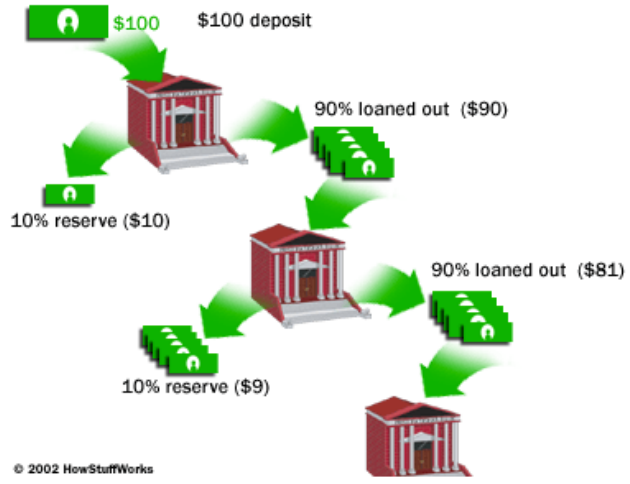
1.4 Praktisk tillämpning

Den praktiska tillämpningen av studien är att i upplysningssyfte ge en informativ sammanfattning över Bitcoin och dess användningsmöjligheter i affärsvärlden åt personer som ej är insatta i ämnet. En upplysning som kan bidra till att ta ställningen för användning av valutan i eventuella framtida egna affärsverksamheter.

2 Nuvarande penningsystem

Banksystemet, fractional reserve banking, används runt om i hela världen. Det är ett system som ständigt ifrågasatts. Hela systemet bygger på att vi som besparare måste ha ett stort förtroende för banken och regeringen. Om ekonomin kraschar eller om bankerna går i konkurs, får vi verkligen ut alla våra pengar som vi har sparade?

Vid insättning av pengar i en bank, så kommer insättningen inte att förvaras i bankens valv utan istället kommer pengarna lånas ut till individer eller företag som behöver dem. Banken sparar bara en mindre summa likvida medel, ifall någon behöver tar ut kontanter. De finns banker som behöver spara 10 %, en del endast 8 % och andra 0 % av kontanterna. Bankanvändarna kan fortfarande använda hela sin deponerade summa, genom att använda bankkort och/eller checker. Det leder till att bankerna skapar pengar ur tomma intet, då du fortfarande kan använda alla dina instoppade pengar och de pengar som banken lånade ut till en annan partner också kan användas. (Hidden Secrets of Money) Figur 1 nedan illustrerar hur banksystemet fractional reserve banking fungerar.



Figur 1. Fractional reserve banking

Om en bank gör dåliga investeringar kan de leda till banken går i konkurs. När bankbespararna hört talas om att banken har gjort misslyckade affärer, så kan de leda till att alla vill ha ut sina besparade pengar. Pengar som inte mera finns i bankvalvet, pengarna har istället blivit utlånande för att skapa vinst åt banken. (Hidden Secrets of Money)

Staten försäkrar bankerna med en stor summa pengar, summan varierar landsvis, så bankbespararna kan få ut sina pengar även om banken har gjort dåliga affärer och slarvat bort dina besparingar. I vanliga fall skulle vi vara väldigt försiktiga med hur våra pengar investeras, men de behöver vi inte vara på grund av försäkringen som staten gör. Detta har lett till att bankerna kan ta allt större risker i sina affärer och låna ut mer pengar. Börskraschen år 2008 berodde på detta fenomen. (Hidden Secrets of Money)

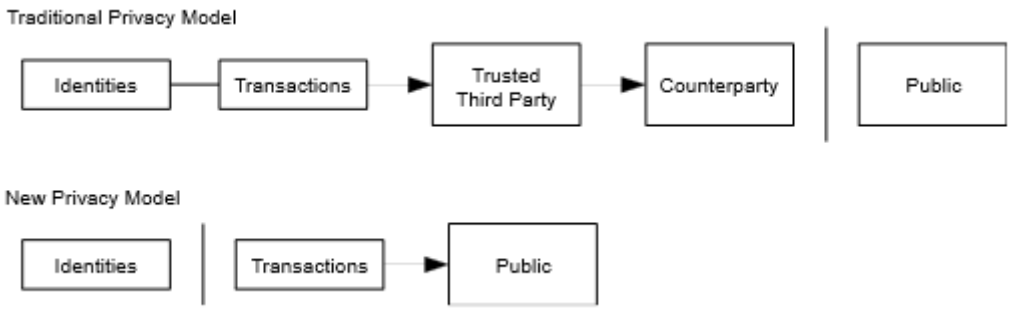
Mängden pengar i vår ekonomi kan öka på två sätt; tryckning av likvidamedel och när affärsbanker beviljar lån. Bitcoin har utvecklas för att sätta stopp på bankernas dominans och istället ge alla individer kontrollen över sina egna pengar. I Bitcoins nätverk kan det endast genereras 21 miljoner BTC. Det kan aldrig röra sig mera än 21 miljoner BTC i nätverket, så ingen med makt kan generera mer valuta för sin egen fördel. (Bitcoin Beginners Guide, 2014)

3 Handel på Internet

Handel på Internet har tidigare alltid skett via en tredje part, ett finansiellt institut, för att få gjort de elektroniska transaktionerna utförda. Systemet fungerar väl för de flesta transaktionsmodellerna, men det finns en tydlig svaghet inom modellen då man måste förlita sig på en tredje partner. (Bitcoin: A Peer-to-peer electronic cash system) Finansinstituten kan inte erbjuda icke-upphävbara transaktioner, eftersom det kan bli tvister mellan betalaren och mottagaren. Finansinstituten har möjligheten att upphäva pengarna ifall tvister uppstår mellan betalaren och mottagaren. Tanken att någon som skall ha makten att upphäva en transaktion som inte egentligen har något med affären att göra, kan för vissa tänkas vara moraliskt fel. Försäljarna tvingas kräva information av deras köpare, som de egentligen inte behöver för att kännas tryggare med sin affär. (Bitcoin: A Peer-to-peer electronic cash system)

Via Paypal, Internets mest kända finansiella institut, sköts de flesta Internet transaktioner idag. Paypal är en aktör som fungerar i stort sett som en bank, de har möjligheten att frysa dina pengar och att upphäva transaktioner mellan olika partners. (Kryptovalutorna växer sig starkare)

Bedrägerier har skett med Paypals system, då användare har att kontaktat Paypal och förklarat för dem att de aldrig har godkänt en utbetalning från sitt konto för att få den upphävd, även fast de egentligen är fullt medvetna om betalningen och utfört den själv. (Kryptovalutorna växer sig starkare) Figur 2 nedan klargör för både den traditionella e-handel metoden och Bitcoins e-handels metod.



Figur 2. Modell för Internethandel

Med Bitcoin behövs inte ett finansinstitut vid handel på Internet. Bitcoin använder sig av ett krypteringssystem, som gör det möjligt att två parter kan sända transaktioner till varandra utan att blanda in en tredje aktör. Tanken är att det virtuella krypteringssystemet skall vara så säkert så att ingen användare skall behöva förlita sig på någon annans ärlighet. När en transaktion sker med valutan Bitcoin så finns det inget sätt att reversibla betalningen, vilket på sådant sätt skyddar försäljaren från bedrägerier. I Bitcoins nätverk har det också utvecklas en depositionsmekanismer som gör det möjligt att hålla pengarna låsta innan båda parterna är nöjda med affären. Processen att överföra pengar tar för de flesta finansinstitut också betydligt längre än vad det gör för Bitcoin. (Bitcoin: A Peer-to-peer electronic cash system)

4 Bitcoin den virtuella krypterade valutan

Bitcoin är den första framgångsrika decentraliserade kryptovalutan, det innebär att valutan inte kontrolleras av någon myndighet. Alla transaktioner görs via ett P2P-nätverk, ett icke-hierarkiskt nät d.v.s. ett nätverk av individuella värdar som godkänner hur protokollet implementeras och används. Användare i nätverket är kopplade till en pseudonym, istället för deras riktiga identitet. (Bitcoin: A Peer-to-peer electronic cash system)

Bitcoin kan tänkas vara en kollektiv post i en datafil som sparar och räknar ihop alla uträknade summor. Alla Bitcoin transaktioner är öppna för allmänheten. Genom att ganska datafilen kan man få ut information om hur mycket Bitcoin varje plånbok i nätverket innehåller. Med våra nuvarande valutor kan man inte få fram en sådan information. (Bitcoin: A Peer-to-peer electronic cash system)

4.1 Satoshi Nakamoto

Satoshi Nakamoto, mannen eller möjligvis gruppen som skapade Bitcoin, försvann någon gång år 2010 och sedan dess har ingen hört någonting av honom. Det har varit väldigt mycket spekulationer kring vem skaparen av Bitcoin egentligen är, men det har aldrig blivit bevisat. En del påstår att det är en japansk man i 64 års ålder, men den utpekade mannen har aldrig erkänt själv att det är han som är skaparen. Vissa tror istället att Satoshi Nakamoto är en pseudonym för en grupp begåvade datautvecklare, då Bitcoins anses vara för väl konstruerat för att enbart vara utvecklat av en person. (Who Is Satoshi Nakamoto, Mysterious Bitcoin Founder)

Hela kryptovalutan Bitcoin lever på dess community. Användningen och utvecklingen tog åter fart år 2013, då Bitcoins värde mångdubblades vilket ledde till att medierna tog upp den virtuella valutan. (Who Is Satoshi Nakamoto, Mysterious Bitcoin Founder)

4.2 Virtuella valutor

Det existerar flera olika format av pengar. Pengar är digitala eller fysiska och oreglerade eller reglerade. Den vanligaste formen av oreglerade pengar som används idag är virtuella valutor. Tabell 1 nedan redovisar för alla typer av pengar som används. (European Central Bank, Virtual Currency Schemes)

Tabell 1. Typer av pengar i vårt samhälle

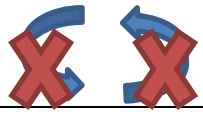
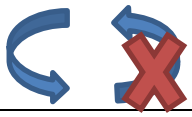
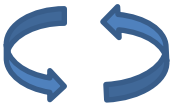
<table>
<tr><td rowspan="3">Rättslig ställning</td><td>Oreglerade</td><td>- Vissa typer av lokala valutor</td><td>- Virtuella valutor</td></tr>
<tr><td rowspan="2">Reglerade</td><td rowspan="2">- Banknoter, sedlar och mynt</td><td>- E-pengar</td></tr>
<tr><td>- Kommersiella bank pengar</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Fysiska</td><td>Digitala</td></tr>
<tr><td colspan="2">Format av pengar</td></tr>
</table>

Cirka 39 % av jordens befolkning hade tillgång till Internet 2013, och har de ökat i antal varje senaste år. Internet har ändrat människornas levnadsvanor, sätt att kommunicera, hitta information och även sättet på hur vi spenderar våra pengar. (European Central Bank, Virtual Currency Schemes)

Under de senaste åren har det uppstått många virtuella så kallade communitys på internet. Den vanligaste typen av en virtuell nätmötesplats är de sociala nätverken så som Facebook och Twitter. Wikipedia är ett exempel på ett Community där syftet är att dela och sprida information, det har också uppstått virtuella värdar som Second life och virtuella nätverk där syftet är underhållning och spel ex. Online Casino. (European Central Bank, Virtual Currency Schemes)

Vissa av de här nämnda nätverken har utvecklat egna system för pengahantering, digitala valutor. Systemen kan innebära nya positiva aspekter för användare och nya betalningssätt, men på grund av den minimala regleringen av dem så finns det också en hel del risker med ett sådana system. (European Central Bank, Virtual Currency Schemes)

Tabell 2. Olika typer av virtuella pengar

Typ 1	Typ 2	Typ 3
Riktig ekonomisk valuta	Riktig ekonomisk valuta	Riktig ekonomisk valuta
		
Virtuella pengar	Virtuella pengar	Virtuella pengar
		
Används endast för köp virtuella av varor och tjänster	Kan användas för köp av riktiga eller virtuella varor och tjänster	Kan användas för köp av riktiga eller virtuella varor och tjänster

Typ1 – Det är en virtuell valuta som endast kan tjänas i den virtuella världen och endast användas inom den. Den här typen används ofta i virtuella spel för köp av varor och tjänster, t.ex. i spelet World Of Warcraft.

Typ2 - Kan köpas med en riktig valuta men inte sedan växlas tillbaka till en riktig valuta. Företaget Nintendo använder sig av en typ 2 version.

Typ3 – Det är den version av valuta som Bitcoin och de flesta virtuella krypterade valutorna är baserade på. Tanken att de skall vara fritt fram att sälja och köpa de virtuella valutorna.

Tabell 2 ovan redovisar för olika typer av virtuella pengar. (European Central Bank, Virtual Currency Schemes)

4.3 Bitcoins utveckling

Domänen bitcoin.org registrerades 18 augusti 2008. Den individen/gruppen första som uttalade sig om Bitcoin gick under namnet, Satoshi Nakamoto. Uttalandet skickades till en e-postlista om kryptografi.(The History of Bitcoin) Meddelandet började så här:

”I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”

Tredje januari 2009 skapades det första blocket i Bitcoins nätverk, i blocket fanns det ett meddelande som är ett starkt bevis för att de inte hade skapats tidigare block. Beviset kom ifrån en artikel i den Amerikanska tidningen The Times, som publicerades samma dag. ”The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”. Det bevisar att Satoshi Nakamoto inte kan ha en mängd förgenererade BTC undansparade i hemlighet. (The History of Bitcoin)

Första versionen av Bitcoin släpptes ut den nionde januari år 2009, de första månaderna av dess existens användes och diskuterades det väldigt lite kring den nya innovationen. Det var först i december 2009 som Bitcoin började ta mer fart, då släpptes 0,2 versionen och svårighetsgraden av att lösa ett block ökades. Första handelsplatsen som erbjöd tjänster för att köpa och sälja Bitcoins med dollar öppnades den 6 februari år 2010. (The History of Bitcoin)

Sidan använde sig av betalningssystemet Paypal vid uttagning och insättning av pengar. Bitcoins första transaktionen som skedde i den ”riktiga världen” ägde rum 22 maj år 2010, transaktionen tog plats på ett internetforum. Det var en programmerare från Florida som erbjöd 10 000 BTC för en pizza, vid den tidpunkten värderades 10 000 BTC till ungefär 25dollar. (The History of Bitcoin)

Den 7 juli samma år lanserades Bitcoin 0.3. Det började skrivas och diskuteras mer kring den virtuella kryptovalutan på olika internetforum och webbsidor, speciellt på websidan slasdot.org. Idag har Bitcoin hundratusentals användare runt om i världen, den nuvarande versionen av Bitcoin är 0.9.0. (The History of Bitcoin)

Det finns planer på att göra Bitcoin till en mera användarvänlig valuta, snart ska man kunna uppge en användares alias istället för en kryptisk adress vid en transaktion och det kommer bli möjligt att göra återbetalningar och att få signerade kvitton. (Virtuella valutor värdefulla för kriminella)

4.4 Bitcoins plånbok

För att kunna köpa och sälja BTC behöver man en Bitcoin plånbok. Varje Bitcoin plånbok har en unik publik adress. Med den unika adressen kan man ta emot betalningar med BTC.

Första gången du startar upp din plånbok kommer det att skapas en slumpmässig publik- och privatnyckel. Totalt finns det totalt 1.46*10^48 olika typer av möjliga Bitcoin adresser, så chansen är i det närmaste obefintlig att du skulle få en likadan adress som någon redan använder (How Bitcoin works under the hood).

För att sedan kunna använda sig av plånboken behövs ett den privata nyckeln och eventuellt ett lösenord som användaren själv kan ange. Den privata nyckeln kommer din applikation att spara en version av, men det rekommenderas att du sparar den på ett fysiskt papper. Eftersom om den privata nyckeln är förlorad så är det omöjligt att komma åt dina Bitcoins.(Så fungerar kryptovaluta i din virtuella plånbok)

4.4.1 Lokalplånbok

Vid användning av en lokal plånbok som sparas på din egen dator eller på din smart-telefon, har du som användare ett fullständigt eget ansvar att inte tappa bort filen eller ha bristande säkerhet i ditt system. Det är viktigt att säkerhetsspara plånboksfilen på en hårddisk som är sparad i ett säkert förvar, om filen borttappas eller förstörs och det är den enda kopian, så är alla BTC kopplade till plånboken borta för alltid. (Plånböcker, David Hedqvist)

4.4.2 E-plånbok

En E-plånbok skapas och lagras på en server. Idag finns det många företag som erbjuder Bitcoin användare att skapa e-plånböcker på deras webbsidor. Användaren måste förlita sig på att företaget inte tömmer plånboken på alla BTC. Det är också upp till företaget att sköta om sin säkerhet så pass bra att ingen hackare kommer åt alla BTC på deras servrar. (Plånböcker, David Hedqvist)

4.4.3 Hybridplånbok

Hybridversionen är en Bitcoin plånbok som kombinerar den lokala plånboken med en E-plånbok. Plånboken kan användas på alla datorer eller smart-telefoner med internetuppkoppling, utan att företaget som erbjuder tjänsten har tillgång till plånbokens uppgifter. Före den privata nyckeln skickas till företagets server, sker en kryptering med hjälp av javascript. (Plånböcker, David Hedqvist)

4.4.4 Pappersplånbok

Det absolut säkraste sättet att förvara sina BTC är att skriva ut en pappersplånbok. Det är omöjligt att komma åt pengarna utan att ha pappersplånboken, vilket gör den säker från hackare och andra intrång. Med pappersplånboken får man tillgång till alla BTC som är besparade, så det är viktigt att den förvaras så säkert som möjligt. (Plånböcker, David Hedqvist)

5 Bitcoins nätverk och dess transaktioner

För att utföra en transaktion med en Bitcoin plånbok behövs ett meddelande och den kopplade privata nyckeln, de två skapar sedan en digital signatur som används för verifikation av transaktionen. Den digitala signaturen och meddelandet kan sedan verifiera att sändaren använde sig av sin privata nyckel, utan att behöva ha tillgång till den. Eftersom den digitala signaturen är beroende av meddelandet, kommer varje digitala signatur vara olik för varje enskild transaktion. Ifall någon försöker göra en förändring på meddelandet så kommer transaktionen inte att accepteras, eftersom meddelandet, den offentliga och privata nyckeln, är kopplade till den digitala signaturen. Matematiken som används för det här systemet är ecdsa och ”mathematical trap door”. (How Bitcoin works under the hood)

5.1 Exempel på en transaktion

Figur 3 och figur 4 är ett exempel på hur en transaktion går till i Bitcoins nätverk. I exemplet skickar användaren Lisa, med publika nyckeln ”jpKfasdf56fgf5412as” 0,55BTC till Alex som har den publika adressen ”54Hffggd43345fgdf”.

Inputs Inputs: Totalt 46,05 BTC

Index (tidigare output)	Belopp	Från adress	Typ	ScriptSignatur
Ergsdfv1263as..1	5	32F4adafGCsxsdassd5D	Adress	14645dfgdfg 564sdfhghf….
51afa4sdfssd..2	16	roDs53sfFdasdaXZ12aF	Adress	Dfg481b1fgDs 153dfgbvbS...
Generation	25	Generation	Pubkey	-
351dsfc1sdfs..0	0,05	5tedgGG5sdvXC5411PV	Adress	Ysdfg2561asd sdfh534rFS…

Figur 3. Figur över en transaktion

Output

Index	Index	Belopp	Till adress	Typ	ScriptSignatur
0	92ASdg63as…	0,55	54Hffggd43345fgdf (Alexs adress)	Adress	146asd5dfzxdfg 54sdfhghf….
1	23gtc76vxcvD..	45,50	jpKfasdf56fgf5412as (Lisas adress)	Adress	DfafSDafgDs B5fdfggbvbS...

Figur 4. Figur över en transaktion

För att Lisas transaktion skall accepteras av nätverket krävs det först att finns en tillräcklig mängd med oförbrukade BTC i hennes plånbok. Eftersom alla transaktioner i Bitcoins nätverket är beroende av de tidigare utförda transaktionerna kommer systemet söka igenom alla transaktioner som är kopplade till hennes signatur, för att få reda på hur många Bitcoins hennes plånbok innehåller.

Eftersom alla transaktioner kopplas ihop med varandra i nätverket, kommer den här transaktionen på 0,55BTC till Alex använda sig av alla fyra tidigare index Lisas plånbok innehåller. Lisas plånbok innehåller mer än 0,55BTC kommer det resterande BTC som hon äger kommer skickas tillbaka hennes egen adress. Ifall ett index är exakt samma summa som transaktioner är begär, behöver alla index inte kopplas.

5.2 Blockkedjan och dubbelspendering

Säkerhetssystemet mot dubbelspendering är en av de största innovationerna med Bitcoin, tidigare har det inte funnits ett säkert system för att lösa problemet. Problemet har varit att användare har använt informationen ifrån en sänd transaktion, för att sedan använda informationen och skicka ut den i nätverket igen. Nätverket måste veta vilken transaktion som utfördes först för att förhindra dubbelspenderade. En tidstämpel är inte tillräckligt eftersom det är väldigt lätt att ljuga när transaktionen utfördes. (How Bitcoin works under the hood)

I Bitcoins nätverk är det ”The blockchain” som används för att rangordna transaktionerna. Varje nytt block i nätverkets block kedja kopplas med tidigare blocket, det är möjligt att kolla igenom vartenda block ända tillbaks till den första transaktionen. I blocken samlas de transaktioner som användaren har skickat ut i nätverket. För att ett block skall kopplas med block kedjan så kommer tusentals datorer runt om i världen försöka lösa det matematiska problemet, en process som i genomsnitt tar 10 minuter att genomföra. Ifall blocken löses snabbare så kommer Bitcoins nätverk höja på svårighets-graden på de matematiska problemen som måste utföras.

Den dator som löste problemet kommer bli belönad med egna BTC till en egen Bitcoin plånbok, det är så nya Bitcoins uppstår i det virtuella nätverket. (How Bitcoin works under the hood)

Det är väldigt ovanligt att två datorer lyckas lösa ett block samtidigt, eftersom den matematiska lösningen är så slumpmässig, men ifall det skulle ske så kommer block kedjan fortsätta på det blocket som nätverket kommer fortsätta bygga nya block på. (How Bitcoin works under the hood) Figur 5 nedan illustrerar Bitcoins blockkedja.

Figur 5. Bitcoins blockkedja

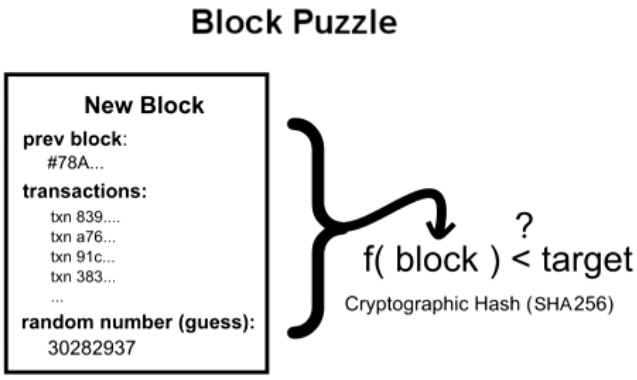
De blåa blocken tillhör den längsta block kedjan som är kopplade med gröna blocket (Bitcoins första block) därför är de den kedjan som används. De gråa blocken har inte blivit accepterade av Bitcoins nätverk pga. två datorer lösa samma block samtidigt eller någon i nätverket har misslyckats med att försöka dubbelspendera sina BTC. De nya blocken kopplas endast ihop med det föregående blocket, det är inte möjligt att två block kopplas ihop i blockkedjan. (How Bitcoin works under the hood)

Ifall en användare vill dubbel spendera sina BTC, kan personen först börja bygga på sitt block när ”hash” värdet är uträttat, det betyder att hon kommer att tävla med hela nätverkets datorer. För att ha 50 % chans att generera ett block före hela nätverket, krävs 50 % av alla data resurser som arbetar i nätverket. (How Bitcoin works under the hood)

För att sedan lyckas med att få block kedjan att acceptera dubbelspenderingen krävs det att personen bygger flera block i följd snabbare än hela nätverket. (How Bitcoin works under the hood)

5.3 Skapandet av ett block

De matematiska problem som datorerna i nätverket måste lösa för att skapa ett nytt block innehåller det tidigare blocket, transaktioner mellan Bitcoin användare och ett slumpmässigt nummer. (How Bitcoin works under the hood) Figur 6 nedan illustrerar hur ett block skapas i Bitcoins nätverk.



Figur 6. Pusslet som utförs för att generera nya block

Hela den här informationen kommer sedan köras igenom ett kryptografiskt hash funktion, SHA256, ända till dess output är ett visst värde. (How Bitcoin works under the hood)

Blockets hash output är kopplat till dess innehåll, en enda liten förändring betyder att hash resultatet blir totalt annorlunda. Hash output:et från det genererade blocket används som referens till nya block. Det går inte att byta ut det gamla blocket emot ett nytt, eftersom det ihopkopplade blocket inte känner igen det föregående blocket. Det innebär också att det inte går att börja skapa ett block innan det föregående blocket redan är färdigskapat. (How Bitcoin works under the hood)

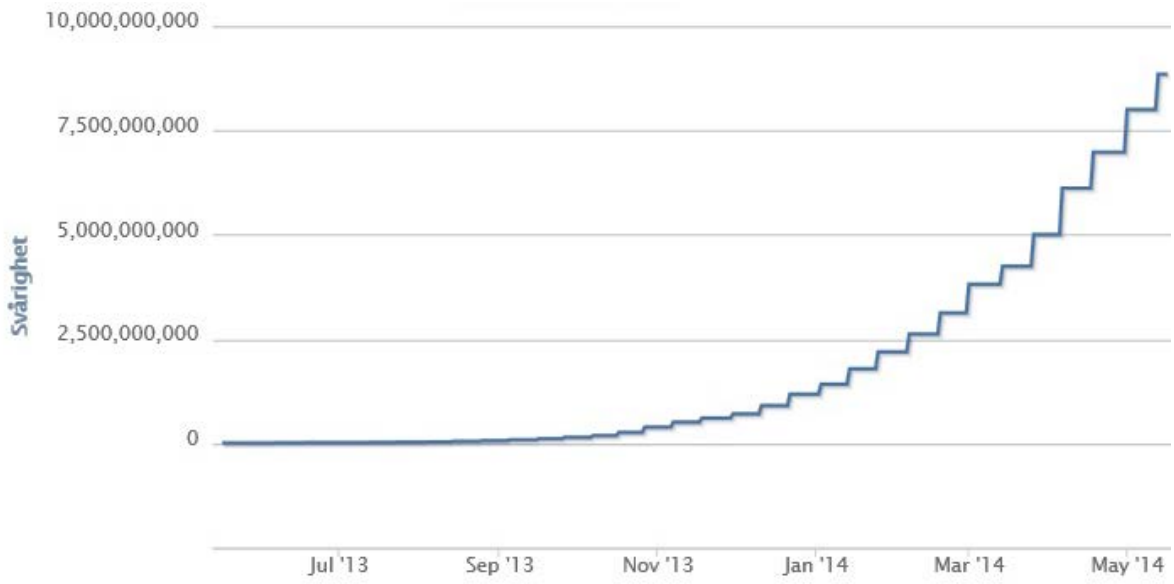
Nedan skiljer endast en punkt på slutet de två meningarna, notera ändå hur stor skillnad det blev på det två olika kryptografiska hash resultaten. Det ända sättet för att lösa den problemet är att göra slumpmässiga gissningar.

SHA256("The quick brown fox jumps over the lazy dog")
0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

SHA256("The quick brown fox jumps over the lazy dog.") (en extra punkt på slutet)
0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

5.4 Svårighetsgraden på att utvinna av data

Det matematiska problemet som måste lösas idag för att utvinna data i Bitcoins nätverk, skulle ta upp till tiotals år för en normalsnabb dator att lösa. Svårighetsgraden är oerhört hög, för det är ett stort antal datorer som arbetar för att generera blocken och för att det har utvecklas supersnabba Asic-kort, vars syfte är att generera Bitcoin block. Många entusiaster för virtuella valutor tycker Bitcoin har tappat sitt decentraliserade kännetecken, eftersom idag är det nästan praktiskt omöjligt att lösa egna block i nätverket. Det är idag i stort sett bara tre stycken företag som sköter om utvinningen av data i Bitcoins nätverket. Diagrammet (figur 7) nedan visar hur svårighetsgraden ständigt ökar för att utvinna data i Bitcoins nätverk.



Figur 7. Svårighetsgraden på utvinning av data

Det finns stora serverhallar som använder sig av Asic-kort för blocklösning, kort som är speciellt utvecklade för att lösa Bitcoin algoritmer. Asic-korten kostar flera tusen euro och en sådan investering tar lång tid att tjäna ihop, så det är i det närmaste otänkbart för en privat person att göra en sådan investering. (How Bitcoin works under the hood)

För att en person i dagsläget skall ha en chans att få ta del av belöningen som utdelas via nätverket när ett block har blivit löst, har man börjat ansluta sig till grupper ”mining pools” som arbetar tillsammans för att generera block.

Vissa mining pools har blivit så pass stora att de har lyckas lösa upp flera block efter varan, BTC Guild är den största gruppen och den har lyckas lösa sex stycken block i rad. (How Bitcoin works under the hood) För att vara helt säker på att en transaktion har blivit accepterad av nätverket, ska man vänta på att flera block har blivit genererade. (How Bitcoin works under the hood)

Tanken från början var att du själv hemma skulle kunna ha möjlighet att starta din egen dator och börja lösa algoritmer i Bitcoins nätverk, men idag är detta helt omöjligt då svårighetsgraden på att lösa ett block är ofantligt hög. En virtuell valuta som konstruerades så att blocken skulle lösas betydligt lättare, skulle det betyda det att valutan skulle det kräva mycket mindre energi för att hålla upp nätverket. Svårighetsgraden på att lösa algoritmerna i Bitcoins nätverk är en av de största orsakerna varför just nya alternativa krypterade valutor har dykt upp och fått så pass stort intresse, då det är möjligt att lösa block själv hemma med sin stationära dator. Problemet som har uppstått är att stora företag ser möjligheten att tjäna pengar på att bygga upp stora datahallar som dagarna i ända endast löser Bitcoins algoritmer.

Dessa datahallar som byggs idag för Bitcoins nätverk är i storleksordningen av Facebooks serverhallar, ur en miljömässig synvinkel är det lite av en katastrof. (Bitcoin miners building 10 megawatt data center in Sweden) Hårdvaran som används för att utvinna data i Bitcoins nätverk är idag väldigt kraftfull. Den totala hastigheten av alla datorer som arbetar i nätverket är 39,5 Petahash.

MegaBigPower är ett företag utvinner 7000-8000 Bitcoins i månaden med hjälp av Asic-kort. Hårdvaran som företaget använder består av 1,4 miljoner datachips och 5000 Raspberry Pis, allt kostade sammanlagt cirka 2-3 miljoner dollar. Enbart kostanden för företagets elektricitet är endast 40 000 dollar i månaden, lokalen är taktiskt placerad i Washington USA nära colombiafloden, som de lyckas utvinna billig vattenkraft ifrån. Företaget har en total kapacitet på 2,2 Petahash och med det lyckas de utvinna 5-10 % av alla Bitcoins som skapas idag. (Meet the manic miner who wants to mint 10 % of all new bitcoins)

Från början var tanken att Bitcoin inte skulle styras av något företag som själv generar sina alla Bitcoins i nätverket och kan i stort sett själv bestämma hur mycket en transaktions kostar att utföra. Den som genererade blocket där transaktionen befann sig i, får ta del av transaktionskostnaden. (Bitcoin miners building 10 megawatt data center in Sweden)

Idag är kostnaderna väldigt små (0,0002-0,0005BTC) och ibland ingen kostnad alls. I framtiden kommer det förmodligen bli lite högre transaktionskostnader, men troligen mindre än dagens avgifter för användande av kreditkort.

5.5 Antalet Bitcoin

I dag finns det ungefär 12,5 miljon BTC i Bitcoins virtuella nätverk. Totalt kommer totalt genereras 21 miljoner BTC. Bitcoins system är konstruerat så att de blir svårare och svårare att generera BTC. Desto mer datorer som utvinner data i nätverket desto högre kommer svårighetsgraden att bli.

De första åren gav ett block 50 BTC, idag ger ett block 25BTC, år 2017 så kommer ett block att ge 12,5BTC och därefter kommer det ännu halveras vart fjärde år. Det är först år 2140 som alla 21 miljoner BTC kommer att vara genererade.

Den minsta transaktionen som kan utföras i Bitcoins nätverket är 0,000 0 000 1 BTC, att det endast kommer att existera totalt 21 miljoner stycken BTC kommer förmodligen inte förhindra valutans möjligheter. (How Bitcoin works under the hood)

6 Investeringar och handel med Bitcoins

De första åren av valutan Bicoin användes tekniken främst för illegala köp av produkter på nätet, eftersom nätverket var så pass nytt och okänt. Det växte upp en hel marknad, kallad Silkroad, för köp av droger i USA.

Idag utförs transaktioner med ett sammanlagt värde på nästan 100 miljoner dollar varje dygn, eller cirka 70 000 Bitcoin transaktioner (Kryptovalutorna växer sig starkare). En del ser Bitcoin och de andra virtuella valutorna endast som en typ av aktiebörs. Hela tiden spekuleras det kring värdet på de olika virtuella valutorna.

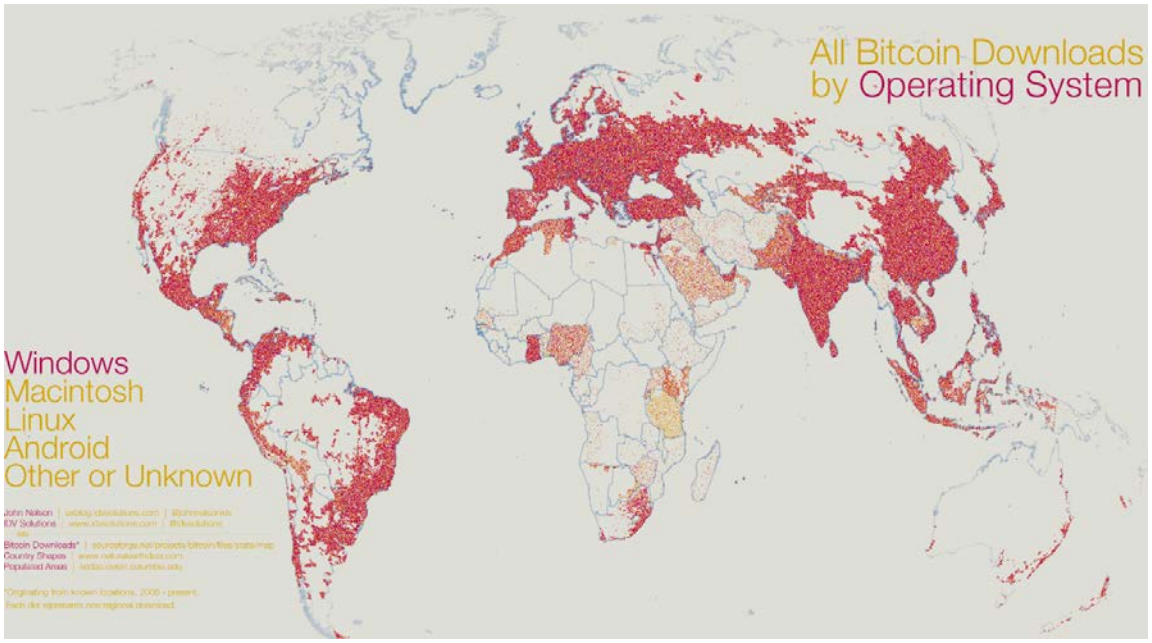
Till skillnad från aktiebörsen så kan man köpa och sälja när som helst, det existerar ingen utsatt bestämd tid när affärerna måste utföras. Det har lockat en hel del personer att försöka tjäna stora pengar, då alla kan köpa och sälja i realtid.

Vissa använder sig av Bitcoin eller andra virtuella valutor för att de vill minska på staternas och bankernas makt kring ekonomin, andra använder sig av nätverken för att utföra effektiva och billiga överföringar av pengar oavsett avståndet mellan transaktionen. Det skickas kring 332 miljarder euro i klassiska pengar globalt per år, normalt mot höga avgifter som bankerna tjänar stora pengar på. Dessa stora kostnader kan undvikas med nätverken som de krypterande virtuella valutorna erbjuder. (Kryptovalutorna växer sig starkare)

Bitcoin har visat sig att vara en väldigt osäker investering, värdet på valutan ändrar från dag till dag. Olika regleringar och varningar av myndigheter och stater har lett till att värdet ha minskat radikalt. EU:s bankmyndighet har gått ut och varnat för riskerna med investeringar i virtuella valutor. (EU:s bankmyndighet varnar för Bitcoin)

Med hjälp av projekt som finansierats helt utav Bitcoins egna användare, har valutan kunnat expandera snabbt. Nya applikationer, program, byteshandel, säkerhetsåtgärder m.m. kanske leder till att fler fångar upp intresset för Bitcoin. Det påverkar i sin tur värdeökningen och därmed också möjligheten att slå sig in på nya marknader. Desto mer användarna är beredda på att spendera eller arbeta för Bitcoins, desto mer kommer valutan utvecklas och användas.

Med de virtuella krypterade valutorna är det möjligt att göra transaktioner billigt och snabbt oavsett avståndet mellan parterna i affären. Med dagens banksystem kan man få vänta ett par bankdagar innan transaktionen är utförd, med Bitcoins nätverk kan man räkna med 10 till 20 minuters väntetid.



Figur 8. Karta över nerladdade Bitcoin program

Plånböcker för att utföra Bitcoin transaktioner används över hela världen, figur 8 ovan ger en överblick på var Bitcoin plånböcker för operativsystemet Windows har blivit nerladdade.

De tidiga Bitcoin användarna har tjänat en hel del pengar på sina investeringar, men de saknas fortfarande stora handelsmarknader för dem att spendera sina Bitcoins på, utan att behöva växla dem till klassisk valuta.

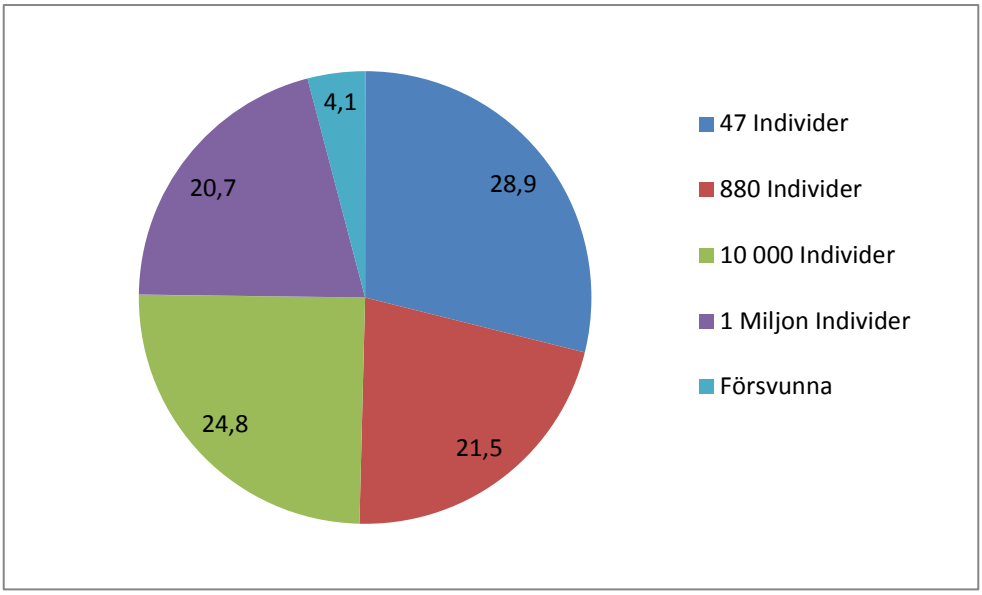
Bitcoins har börjat bli en accepterad valuta som främst används vid internethandel. På Internet är det möjligt att köpa allt från underkläder till flygresor med Bitcoin. Overstock är ett internationellt företag som har börjat acceptera Bitcoin vid betalning. Företaget fick ta del av massor med gratis mediareklam, då det var en stor nyhet att ett sådant stort företag accepterar Bitcoin som betalningsmedel. En del Bitcoin förespråkare menar att det är en självklarhet att börja acceptera BTC, då det leder till nya kunder och gratis marknadsföring.

För internationella företag är Bitcoin ett billigt och enkelt alternativ till vårt banksystem. Jag testade skicka Bitcoin från Finland till min bror som är bosatt i Texas, USA och det tog cirka 10 minuter innan Bitcoinsen var tillgängliga för honom.

Doneringsprojekt är väldigt vanligt i de virtuella valutornas nätverk, stora orsaken är att kostnaden för transaktionerna är minimala och snabba oavsett var du befinner dig.

6.1 927 personer äger hälften av alla Bitcoins

Risto Pietilä en finsk entreprenör och aktiv medlem i på forumet ”bitcointalk” har utfört en utredning på hur det obalanserade ägandeskapet i den virtuella valutan Bitcoin. Utredningen baserade på data som hämtat från webbplatsen Bitcoinrichlist.com och utfördes i oktober 2013 när det existerade 12 miljoner Bitcoins. Cirkeldiagrammet (figur 9) nedan klargör för ägandeskapet på alla 12 miljoner Bitcoins. (927 people own half of the Bitcoins)



Figur 9. Ägandeskapet av Bitcoin

En av de stora orsakerna varför bara 47 individer äger hela 28,9 % av alla Bitcoins, är för att under den första perioden av Bitcoins existens utvanns det 50 Bitcoins per block och i nätverket var det mycket mindre konkurens om utvinningen av data. (927 people own half of the Bitcoins)

Hela 4,1 % av alla Bitcoins är försvunna. Det finns många olika sätt som Bitcoins kan försvinna i nätverket, men den allra största orsaken är att användare har förlorat sin plånboksfil eller har glömt bort sitt lösenord till plånboken. Det händer också att användare i misstag har skickat Bitcoins till en plånboksadress som ingen har tillgång till.

När transaktionen har blivit utförd kan den inte att upphävas, så alla skickade Bitcoins kommer vara oåtkomliga. En hel del Bitcoins har också blivit beslagtagna av myndigheter och är därför ur cirkulation i nätverket.

Jag tror att fördelningen ägandeskapet av Bitcoins kommer vara bättre balanserat framtiden, eftersom att det utförs cirka 70 000 transaktioner med Bitcoin dagligen och under den senaste perioden har det visat sig att öka i antal med företag som accepterar Bitcoins.

6.2 Värderingen av Bitcoin

Bitcoin är en valuta som endast har ett värde på grund av att vi användare kommer överens om det. Egentligen har Bitcoin inget praktiskt värde, det är bara en stor lista på Internet som räknar ut hur mycket varje användare har på sin egen plånbok. Figur 10 nedan ger en uppfattning om hur värderingen på en Bitcoin har cirkulerat ända sedan januari 2009.

Tidpunkt	Värdering	Kommentar
-Jan 2010	Inget värde	Användare skickade endast BTC till varandra för att testa systemet
Feb 2010- Juni 2011	0,01 – 0,08 $	Byteshandel öppnas och Bitcoin börjar värderas
Feb 2011 – April 2011	1 $	En BTC värderas lika mycket som en dollar
Juli 2011	31-2 $	Bitcoin rusar upp till 31 dollar per styck, men i slutet av året har värderingen sjunkit så lågt som 2 $
Hela 2012	2-13 $	Under år 2012 stiger Bitcoins värde upp till 13 $
Jan 2013 – Oct 2013	20-260 $	Värdet cirkulerar ständigt under året.
Nov 2013	150-1124 $	Det var i slutet på året som Bitcoins värde började stiga till rekordhöga nivåer. 29 november var en BTC värderad till 1124 $ och är det högsta värdet Bitcoin någonsin har haft.
Feb 2014	550 – 750 $	Värdet cirkulerat runt 600 $ per BTC

Figur 10. Bitcoins värde sedan Januari 2009

När de första Bitcoin blocken genererades var det ingen som var villig att betala för de BTC som hade skapas. 6 april 2009 auktionerade en användare i Bitcoin nätverket ut 10 000 BTC för 50 Dollar, men ingen köpare hittades. (The History of Bitcoin)

Många som köper Bitcoins idag ser det som en slags investering i väntan på att värdet ska stiga, för att sedan kunna göra vinst på affären. På Internet kan man läsa om personer som har blivit miljonärer på Bitcoin investeringar, ett bra exempel är norrmannen Kristoffer Koch som köpte 5000 BTC år 2009 för ungefär 19 €, en investering som han sedan själv glömde bort. Det var först i april 2013 som han fick höra om Bitcoin på nyheterna som han kolla upp hur mycket hans investering var värd. De visade sig att den lilla investeringen som han gjorde 2009, var värderad till hela 648 656 €. Kristoffer sålde alla sina Bitcoin's och köpte sig en lyxlägenhet i Oslo. (Man buys $27 of bitcoin, forgets about them)

7 Övriga virtuella kryptovalutor

När värdet på Bitcoin ökade noterbart och medierna började rapportera om valutan, tog det inte länge innan många konkurrerande kryptovalutor började dyka upp på marknaden. Bitcoins dominerar kryptovalutasystemet idag. När Bitcoin stiger i värde och intresse för Bitcoin ökar har nästan alltid de mindre kryptovalutorna hakat på. En av de främsta orsakerna är att de flesta kryptovalutor endast kan köpas med Bitcoin.

En kryptovaluta med revolutionerande teknik och möjligheten att köpas utan växla via Bitcoin skulle förmodligen inte bindas lika mycket till Bitcoins värde som de nuvarande alternativa kryptovalutorna. Idag finns det inte riktigt någon kryptovaluta som är tillräckligt kraftig för att klara sig på egen hand. Om det skulle vara så att Bitcoin skulle dö ut, så skulle det förmodligen också leda till att de konkurrerande kryptovalutorna gick under. (Bitcoins failure rains future for all cryptocurrencies)

Det är endast ett fåtal av kryptovalutorna som har utvecklas, som verkligen har bidragit med något innovativt. De flesta har kopierat idéerna och källkoden från Bitcoin eller den näst mest attraktiva kryptovalutan Litecoins. Kryptovalutatekniken baserar sig på öppen källkod, så är det lätt att bara använda sig av den befintliga tekniken som redan existerar.

De kryptovalutor som bara har kopierat den befintliga tekniken eller kanske bara ändrat en liten del har haft det svårt att överleva. Det är inget som intresserar sig av dem och deras lanserande anklagas ofta för att endast försöka göra en vinst på den nya valutan. För att en kryptovaluta skall överleva behövs det stort stöd bakom den, stor datakraft, investeringar och utvecklare. (Bitcoins failure rains future for all cryptocurrencies)

Det finns några intressanta virtuella valutor, som har satt Bitcoin på prov. Den virtuella kryptovaluta tekniken är fortfarande i utvecklingsfasen, det är fortfarande mycket möjligt att en annan virtuell kryptovaluta teknik tar över.

7.1 Litecoin, LTC

Litecoin är en av de första och största konkurrenterna till Bitcoin. Litecoin är en av de få alternativa valutorna som det är möjligt att växla till utan att använda sig av Bitcoin. Litecoin har näst störta marknadsvärdet av de virtuella valutorna, det är vanligt att man gör jämförelsen med att Litecoin ses som silver och Bitcoin som guld.

Litecoin genererar ett block på 2,5 minuter, fyra gånger snabbare än Bitcoin. Det innebär att Litcoins blir snabbt tillgängliga efter en transaktion, men tekniken som används kräver dessvärre att mycket dataresurser används i onödan på non-best block. Totalt kommer skapas 84 miljoner LTC. (A $100 worth of Litecoin a year ago is worth $30,000 today)

7.2 Vertcoin, VTC

Den virtuella valutan Vertcoin skapades i januari 2014. Valutan skapades för att introducera en alternativ valuta som har hög resistans emot Asic-kort och grupp generering av block (multipool mining). Vertcoins algoritm är utvecklad så att den förändras över tid. Vilket innebär att det är mycket svårare att utveckla Asic-kort som kan operera i Vertcoins nätverk, eftersom Asic-korten är inställda att operera på en specifik typ av algoritm. (What is Vertcoin)

7.3 Dogecoin, DOGE

Dogecoin är associerad med en av Internets mest kända ”meme”. Valutan startades lite som mer av ett skämt i slutet av december 2013, men idag är det en av de mest populära kryptovalutorna(DOGECOIN). Dogecoins Community har startat ett välgörenhetsteam kallat Dogecoin Foundraiser.

Deras första projekt var att samla in tillräckligt med pengar så ett bob team från Jamaica skulle kunna delta i vinter OS 2014 i Sotji. Redan efter den andra av insamlingen hade man fått in 30000 dollar. (Jamaican Bobsledding and crypto currencies)

Dogecoin Foundraiser sponsorerade också en annan OS-idrottare, Shiva Keshavan och Josh Wise som tävlar i bilsporterns Nascar serie. (Nascar fans on reddit use dogecoin to sponsor Josh Wise)

Det har donerats över 40 miljoner Dogecoins till World Water Day, för att hjälpa till att utveckla bättre dricksvatten förhållandena i Kenya. (Kenyan water charity via Dogecoin) Det genereras upp runt 100 biljoner Dogecoins år 2014 och därefter runt 5,2 biljoner stycken per år. (DOGECOIN)

7.4 Peercoin, PPC

Peercoin är den första kryptovalutan som introducerade en kombination av proof-of-work och proof-of-stake. De första PPC genereras av lösande av block, men desto mer PCC som skapas i nätverket desto svårare kommer processen bli.

De nya PCC kommer till största del istället genereras av proof-of-work algoritmen. Användare som har 2 % av valutan kommer bli kompenserad med 2 % av alla proof-of-stake PCC. Proof-of-stake använder sig mycket mindre energi vid generering, så Peercoin behöver inte lika många servar för att hålla igång sitt nätverk. (PPCoin: Peer-to-peer Crypto-currency with proof-of-sake)

7.5 Auroracoin, AUR

För fem år sedan kraschade Islands valuta, för regeringen var det omöjligt att kontrollera inflationen. På grund av krisen med den isländska kronan måste alla islänningar växla all utländsk valuta som de tjänat tillbaka till den isländska kronan. System har gjort att Island tappat mycket av affärskontakter med företag från andra länder. Utländska investerare har tappat intresset för Island då de kanske inte har möjligheten att växla till sina investeringsvinster till dollar eller euro. (A nation breaks the shackles of fiat currency)

Kryptovalutor gör det möjligt att skicka pengar vart som helst på jorden med minimal kostnad. Auroracoin skapades för att bli Islands egen kryptovaluta, så att islänningar och utlänningar skulle ha det lättare att göra affärer tillsammans. 50 % av alla AUR är genererade före kryptovalutan blir publik, alla de AUR som är genererade kommer bli utdelade åt Islands befolkning. När Auroracoin blir publik är det sen upp till dess Community och dess utvecklare att fortsätta stöda valutan. För att den här virtuella valutan ska fungera är det viktigt att det utvecklas ny programvara så att Islands befolkning kan använda valutan i deras vardagliga liv. (A nation breaks the shackles of fiat currency)

8 Bannlysningar och regleringar emot Bitcoin

Länder, institut och centralbanker har börjat undersöka och följa de virtuella valutorna, eftersom de har skapats en så pass stor okontrollerad marknad kring dem.

8.1 Behandlingen av virtuella valutor i USA

I USA har de virtuella valutorna haft bra framgång. Det har lett till att Financial Crimes Enforcement Network (FinCEN), en byrå som behandlar USA:s finansiella situationer, gett ut ett icke bindande dokument om hur de virtuella valutorna ska behandlas. De virtuella valutorna behandlas annorlunda från de traditionella valutorna i USA. (FinCEN’s Regulations)

Om en användare köper/säljer gods eller tjänster med en virtuell valuta, behandlas köparen inte under FinCEN's reglemente. Däremot behandlas företag, organisationer och växelbörser under FinCEN's reglemente, när de virtuella valutorna används som ett finansinstrument. Det betyder att de skall upprätthållas registrering, rapportering och följande av vissa regler. (FinCEN's Regulations)

Eftersom de virtuella valutorna inte beaktas som ”riktiga” valutor i USA, så behöver inte de virtuella växelbörserna inte följa de regler som är utsatta för ”riktiga” valutabörser. (FinCEN's Regulations)

8.2 Europeiska centralbanken tre kriterier för pengar

Enligt Europeiska centralbanken så ska pengar, oavsett typ vara associerade med tre olika typer av funktioner:

1. Medium of exchance: Pengar används för att slippa olämpligheterna med byteshandel.

2. Unit of account: Pengar användas standard numerisk siffra som bedömer värdesättningen på varor, tjänster, tillgångar och skulder.

3. Store of value: Pengar ska kunna sparas och användas i framtiden.

För att de någon av de virtuella valutorna ska kunna godkänns och beaktas som en seriös valuta så måste de klara av de här tre kriterierna. Det stora problemet med de virtuella valutorna är att värdet ändrar avsevärt mycket. För att de stora bankaktörerna ska betrakta Bitcoin som en ”riktig” valuta, så krävs det att dess volatilitet måste minska betydligt. Ännu idag har Bitcoins värde en tendens att öka eller sjunka med över 20 % inom bara 24timmar. (European Central Bank,Virtual Currency Schemes)

Figur 11 nedan illustrerar hur mycket värdet har förändras på en Bitcoin under en kort tidsperiod.

Tabell 11. Bitcoins volatilitet

I Europa har länder som Tyskland, Sverige och Finland har erkänt valutan som ett legalt betalningsmedel. Om någon vill utföra handel med valutan så är det fullt möjligt. Bitcoin har inte definierat som en traditionell valuta utan istället som ett finansinstrument.

Vissa länder har varit skeptiska och negativa emot de virtuella kryptovalutorna. Thailand och Ryssland är två länder som har olagligt stämplat de virtuella valutorna. I Kina är handel med Bitcoin inte olagligt, men däremot har regeringen varnat för att stoppa alla bank- och växeltjänster. (Russia bans Bitcoin)

På Internet har det varit mycket skriverier om hur Kinas regering och banker har bestämt sig för att behandla de virtuella valutorna, de flesta artiklar har dock endast varit spekulationer och teorier som inte har varit tillförlitliga.

Japan har varit i centrum när det kommit att handla om hanteringen av Bitcoin. Den största växelplatsen för Bitcoin heter Mt Gox och är lokaliserad i Tokyo. Japans regering har försökt komma med förslag till möjligheter för hur man skall kunna beskatta de virtuella valutorna. Med tanke på att Bitcoin transaktioner är anonyma, så är det ett stort problem för regeringar som vill beskatta och godkänna Bitcoin som en riktig valuta.

Enligt Japans vice finansminister, Jiro Aichi, så skall lagstiftning av den virtuella kryptovalutan Bitcoin hanteras på internationell nivå. (Japan says any bitcoin regulation should be international)

8.3 Vad finska lagar säger om virtuella valutor

När man växlar en virtuell valuta till en klassik valuta så realiseras beskattningen av den virtuella valutans värdeändring. Om det skett en positiv värdeändring så betraktas inkomsten, som om den skulle ha influtit av egendom och därför beskattas den som kapitalinkomst. Eftersom en virtuell valuta inte är ett värdepapper så kan man inte dra av en förlust i inkomstbeskattningen. Om man köper varor med Bitcoin och gör en vinst på dem så måste man beskatta vinsten. Vid datautvinning av Bitcoin ses det inte som kapitalinkomst enligt skattelagen utan räknas istället som förvärvsinkomst. (Finlands författningssamling, Skatteförvaltningen)

Exempel 1.
Om du har köpt Bitcoin för 100 € och du sedan säljer dem vidare till klassiska valutor när de värderas till 200 €, så betalar du kapitalsinkomstkatten på 100 € vinsten. Kapital-inkomstskatten är 30 %, skatten blir 30 €.

Exempel 2.
Jan köpte Bitcoins för 100 € när en Bitcoin kostade 1 € styck. Så Jan har totalt 100 Bitcoin, Jan köpte sedan varor på webbutik för 20Bitcoin, vid tidpunkten då Bitcoins var värderades till 100 € styck. Varorna kostade alltså totalt 2000 €.
Jan måste betala kapitalinkomstskatt på sitt köp eftersom Bitcoinsen har mycket högre värde vid inköpet. 2000-20=1980
Förändringen i värdet är 1980 €, så Jan måste betala kapitalinkomstskatt för 594 € (30 % av förändringsvärdet).

8.4 Plånböcker bannlysta på App store

Apple är väldigt stränga med vilka applikationer som får finnas på deras webbutik och de virtuella kryptovalutors plånböcker är inget undantag i det här fallet. Alla plånböcker för virtuella valutor har blivit borttagna från App Store och de är nu portade från App Store. Eftersom Apple har en oerhört stor kundkrets och inflytande på den digitala marknaden har det naturligtvis hämmat Bitcoins tillväxt. (Apple deletes blockchain)

9 Bitcoin i Praktiken

För att få en fullständig uppfattning om hur Bitcoin fungerar som ett finansmedel bestämde jag mig för att göra två intervjuer med företag som gör affärer med valutan och där med också accepterar valutan som betalningsmedel. De två företagen jag intervjuade var Zas Data från Kimito i Finland och Webhallen som är Sveriges största företag som accepterar Bitcoin. Jag fick reda på att företagen tog emot Bitcoin via nyhetsartiklar på Internet.

Webhallen använder sig av Bitpay, en tjänst via Internet som tar sköter deras transaktioner och valutakurser. Bitpays tjänster kostar bara en liten summa varje månad och då slipper butiken själv växla Bitcoin till statliga pengar. För Webhallen har omsättningen med Bitcoin motsvarat ungefär som någon av deras mindre fysisk affärer. Detta har varit över deras förväntan och kundernas respons har varit i stort sett bara varit positiv.

Zas data använder sig inte av internettjänst vid försäljning, istället uppmanar de sina kunder att kontakta dem via e-mail eller att komma in till butiken för att sedan förhandla vidare om köpet. Zas data använder sig av det finska företaget Bittirahas kurs. Zas data har endast haft ett fåtal försäljningar med Bitcoin, däremot så utför de inköp med Bitcoin flera gånger i veckan.

Företagen bestämde att använda sig av Bitcoin för att det är väldigt enkelt att implementera, använda och det för att det är ”i ropet”. Båda företagen tycker inte volatiliteten har fört med sig något negativt för deras affärer.

Kundresponsen har i stort sett bara varit positiv, ett fåtal som har kritiserat företagen för att stöda svarta marknader och kriminella aktiviteter. Zas data och Webhallen har hittills varit nöjda med Bitcoin och tror att valutan kommer expanderas i Finland.

10 Stölder i Bitcoins nätverket

Bitcoins nätverk är i sig ett väldig säkert, det har bevisats under de fem år som nätverket existerat. Men att Bitcoins nätverk är säkert betyder inte att stölder av BTC inte har skett. Problemet med Bitcoin är att det finns många opålitliga företag och växeltjänster som hanterar valutan. I vissa fall har företagen själva stulit användares BTC och andra har de blivit attackerade av hackare. (Nearly 150 breeds of Bitcoin)

GBL var en byteshandel som opererade i Kina, företaget opererade under falska identiteter. De visade sig att GBL aldrig hade registrerat sitt företag och de hade officiellt aldrig fått tillåtelse att hålla igång byteshandeln.

Webbsidan stängdes ner och de okända ägarna tog besparingar från cirka 1000 stycken användare och försvann. ($4,1m goes missing as Chinese bitcoin trading platform GBL vanishes)

10.1 Skadlig programvara

De skadliga programvarorna har visat sig vara ett växande problem för de virtuella valutorna, enligt en rapport från Kasperky Lab har attackerna emot Bitcoin fördubblas under 2013. Idag finns det närmare 150 olika typer av skadlig programvara som vars uppgift är att stjäla BTC från användare i nätverket. De skadliga programvarorna attackerar för det mesta Bitcoin plånböcker. (Kryptovalutorna växer sig starkare).

De flesta attacker utförs mot de privata nycklarna som Bitcoin plånböcker sparar, den skadliga programvaran letar upp den privata informationen som skickas sedan över till tjuven, som i sin tur använder informationen för att tömma plånboken. För att komma åt en plånboks innehavares BTC som har låst sin krypterade privata nyckel med ett lösenord, så finns det skadeprogram som spelar in när innehavaren slår in sitt lösenord. Det har också utvecklas skadeprogram som ändrar plånboks innehavares angivna Bitcoin adress, så att alla BTC till istället skickas direkt till tjuvens egna plånbok. (Nearly 150 breeds of Bitcoin)

Skadeprogram som använder sig av en fjärrserver för att skicka data, är det mest svår-upptäckta för vanliga antivirusprogram. Det bästa sättet att skydda sina BTC är att ha dem sparade på en plånbok som inte är uppkopplad till internet och installerad på ett annat operativsystem än Windows. Över 99 % av alla utförda attacker emot Bitcoin sker på operativsystemet Windows. (Nearly 150 breeds of Bitcoin)

10.2 Mt Gox

Den 28 februari 2014 skickade Mt Gox, Bitcoins största växeltjänst, in en konkursansökan i Japan. Konkursorsaken var förlusten på 750 000 BTC av användarnas och 100 000 BTC av sina egna Bitcoins. (Mt. Gox files for bankruptcy) Förlusten värderades till ungefär 480 miljoner dollar och totalt hela 7 % av alla dagens existerande BTC i Bitcoins nätverk. Det har spekulerats mycket kring hur de lyckades förlora en sådan stor summa Bitcoin. (Mt. Gox files for bankruptcy)

Mt Gox påstår själva att de har varit något slags fel i systemet som användes, som de nu försöker åtgärda. Vissa har spekulerat i att de har själva har tappat bort den privata nyckeln till plånboken eller att det var någon på företaget som stulit alla BTC. (Mt. Gox files for bankruptcy)

Användare på Mt Gox försökte redan innan konkursansökan att skicka sina Bitcoins till sina lokala plånböcker från Mt Gox, men webbsidan opererade oerhört långsamt och hade problem med ”transaction malleability” och ”DDoS attacker”. (What is transaction malleability and did it kill MtGox)

Transaction malleability har varit ett känt problem ända sedan 2011, problemet är Bitcoin plånböcker som måste hantera massor med transaktioner i stora summor. Då går inte att använda sig de officiella Bitcoins plånböckerna. Så stora företag har istället utvecklat egna snabbare plånböcker, som klarar av att operera tillräckligt snabbt. Transaktionerna i de här plånböckerna konfirmeras med transaktionens id, istället för när transaktionens block har blivit utfört. Problemet är att i nätverket är att det är möjligt att manipulera på transaktionens id. (What is transaction malleability and did it kill MtGox)

11 Olagliga verksamheter

Många kriminella aktörer har försökt att dölja olagliga affärer och verksamheter i de nätverk som de virtuella valutorna erbjuder. Kriminella ligor, bedragare eller penga-tvättare har alla fått en ny plattform att använda sig av. Det är en svår uppgift att kontrollera och ha översikt över hela det nätverket som de virtuella valutorna har skapat.
Att stjäla bankkort för att sedan använda dem för att köpa stora summor av BTC är en trend som vart vanlig bland brottslingar i USA.

Polisen har haft svårt att lösa dessa fall eftersom ägaren av den virtuella plånboken inte är kopplad till en riktig identitet och det är en väldigt besvärlig situation då en transaktion av BTC inte kan upphävas. Det är möjligt för banken att reversibla pengarna till ägaren av ett bank-/kreditkortet, men den som sålde sina BTC kan inte reversibla dem till sitt eget konto och förlorar sina Bitcoins. (Stolen target credit cards are selling for 20-100 dollars each)

I har Bitcoins nätverk fått så pass mycket ögon riktade emot sig så att olika kriminella ligorna eller bedragare förmodligen använder inte använder sig av nätverket i lika stor omfattning. I Bitcoins nätverk är det möjligt att gå igenom varje utförd transaktion, så ifall en bov blir kopplad till en plånboksadress är det möjligt att leta fram flera som har gjort affärer med honom. Det är dock inte lätt att få fram vem som äger plånboken, eftersom de inte krävs något namn för att få en plånboksadress.

Det är möjligt att olika kriminella ligor eller bedragare nu istället använder sig av de mindre alternativa krypterade valutorna som inte kontrolleras lika intensivt som Bitcoin. (Kryptovalutorna växer sig starkare)

11.1 Silkroad

Silkroad,”eBay for drugs”, startades i februari 2011. Webbsidan är en Internet marknadsplats, där användare kan idka handel helt anonymt med hjälp av Bitcoin och Tor anonymitets service. Tor anonymitets service gömmer användares IP-adress och anonymiserar, med utnyttjande av servicen är det mycket svårare att spåra och analysera datatrafiken. (Feds seize silk road)

Marknaden användes till största del för att köpa och sälja droger. Februari 2013 dömdes en australiensisk knarklangare för det första brottet som bevisade sig vara relaterat med Silkroad. Den australiska polisen som hittade spår till Silkroad på hans hemdator. Fram till mars 2013 hade användare på Silkroad sålt totalt 10 000 produkter varav 70 % av dem droger. (Feds seize silk road)

Den 2 oktober 2013 slog FBI till emot den illegala hemsidan. Ross Ullbricht, ägaren av Silkroad, anklagades för narkotikahandel, beställning av dråp, dataintrång och penningtvätt. Silkroad webbsidan stängdes ner och FBI beslagtog 26 000 BTC från användarkonton, vilket var värt ungefär 3.6 miljoner dollar vid den tidpunkten. FBI beslagtog också en Bitcoin plånbok som innehöll 144 000 BTC, vilket de anade att var Ullbrich egna. (The feds are ready to sell 25 million dollar of bitcoin sized from the silk road)

12 Diskussion

För mig är de virtuella krypterade valutorna ett intressant ämne. De har utvecklat ny plattform som erbjuder möjligheter för transaktioner, med hjälp av data kodning och avancerad matematik. Jag ville själv få lite mera insikt över hur just detta virtuella system fungerar, varför någon skulle använda sig av dem och vilka problem de har.

Undersökningen som jag har utfört om de virtuella valutorna har fått mig att inse hur nätverken fungerar och vad för tanke som ligger bakom dem. Jag har också tagit reda på hur vår egen regering har behandlat de virtuella valutorna.

Undersökningen om Bitcoin har inte varit en allt för enkel uppgift, då det knappt finns några böcker om ämnet. För det mesta har jag använt mig av olika artiklar på Internet för att få tag på relevant information. Ibland har det visat sig vara väldigt svårt att veta om en artikel verkligen är trovärdig eller om det bara är påhitt för att förändra på Bitcoins värde eller rykte. Många artiklar och informationskällor om Bitcoin har visat sig att inte vara allt för tillförlitliga, det är ett nytt komplicerat ämne som inte är allt för lätt att sätta sig in i. Informationen som är hämtad från Internet har jag valt ut genom att granska användar-antalet webbplatserna, jag har även tagit i beaktande hur pass välkänd webbplatsen är. Artiklar som jag har valt ut för min undersökning har en eller flera författare förekommit, för öka källans är trovärdighet.

Bitcoin används globalt, så det är väldigt svårt att spekulera om hur valutan kommer att klara sig i framtiden. Om till exempel Kinas regering skulle bestämma sig för att olagligstämpla de virtuella valutorna skulle de vara en stor katastrof för Bitcoin. Det är inget som man egentligen kan spekulera i allt för mycket om här i Finland och på Internet florerar det massor med rykten, men det är väldigt svårt att veta vad som stämmer.

Det är nästan omöjligt att veta i dagsläget hur de virtuella valutorna kommer utvecklas och användas i framtiden, det är upp till var och en använda sig av det penningsystemet som man själv känner sig mest bekväm med. Jag tycker inte det är rätt av staterna och bankerna att sätta stopp för Bitcoin, hellre skulle jag se dem vara med och utveckla eller själv försöka dra nytta av de nya valutorna.

Min förståelse varför valutan Bitcoin har blivit såpass populärt har blivit mycket större, i början av mitt arbete såg jag valutan mest som ett typiskt pyramidspel. Men nu efter att jag undersökt inom ämnet har jag fått klarare förståelse för de virtuella valutorna har många användare i sitt nätverk.

Det här är de största positiva aspekterna om de virtuella valutorna, som jag har tagit reda på i min undersökning:

+ Anonyma transaktioner som utförs snabbt, oavsett avstånd och mängd

+ Behöver inte förlita sig på finansiella institut, utan istället har eget ansvar över sin säkerhet och ekonomi

+ Värderingen av Bitcoin styrs inte av någon form av myndighet

+ Ingen risk för inflation

+ Lätt att skaffa och använda

+ Bitcoin ställer inga finansiella krav på sina användare

+ Låga transaktions konstanter

+ En utförd transaktion går inte att upphäva

+ Mycket utvecklings möjligheter, teknikens är fortfarande i utvecklingsfasen

+ Möjligt att kolla upp hur mycket varje plånbok innehåller genom att granska datafilen

+ Möjligheten att kolla upp alla transaktioner som har utförs i nätverket

Det här är de största negativa aspekterna om de virtuella valutorna, som jag har tagit reda på i min undersökning:

- Ingen myndighet som kan hjälpa dig ifall dina pengar har blivit förlorade

- Bitcoin har blivit ihopkopplat med många illegala affärer, och därför fått ryktet att finansiera den svarta marknaden

- Antalet Företag som accepterar Bitcoin som ett betalningsmedel är begränsad i dagens läge, det är i stort sett omöjligt att enbart leva med valutan

- Virtuella valutor har blivit bannlysta och stämplade som olagliga i många länder och regioner

- Virtuella valutors värde har haft en tendens att vara väldigt ostabilt

- Svårt att kontrollera beskattningen av betalningssystemen, eftersom transaktionerna är anonyma i nätverken

- Många företag som har hanterat virtuella valutor har skött sin verksamhet väldigt slarvigt

- Det har utvecklas en hel del skadeprogram vars syfte är att stjäla användares virtuella valutor

- Stor del av alla Bitcoins innehas av ett få antal personer

- Tappat sitt decentraliserade kännetecken eftersom utvinningen av data idag endast sköts av ett fåtal företag

13 Slutord

Den digitala valutan Bitcoin är fortfarande ganska okänd och främmande, men vi får fortfarande inte glömma att valutan är relativt ny och att tekniken fortfarande i utvecklingsfasen. En anledning till varför Bitcoin har fått så mycket popularitet idag är för att många har tappat förtroendet för hur våra regeringar och banker sköter om de statliga valutorna.

Det finns vissa fördelar med virtuella krypterade valutor över vårt nuvarande banksystem, men också en hel del svagheter. Om du tappar bort din information till din virtuella plånbok kommer du aldrig mer kunna komma åt dina besparingar, det finns ingen myndighet som kan hjälpa dig i den besvärliga situationen. Det är helt upp till var och en att sköta sin säkerhet, tanken är att det är användaren själv som ska ha full kontroll och ansvar för sin egen ekonomi.

Den virtuella valutan skickas anonymt från användare till användare genom Internet. De största fördelarna med valutans transaktioner är snabbheten, den låga kostnaden och att de inte finns något behov av en mellanhand. Värdet på Bitcoin bestäms helt utav utbud och efterfrågan, värdet har haft en tendens att vara väldigt rörligt. Bitcoin är en valuta som varken banker och regeringar kan kontrollera, så egentligen kan Bitcoin ses lite som en konkurrent till bankerna.

För många regeringar och banker har det varit ett svårt att riktigt bestämma sig för hur de virtuella valutorna skall hanteras. Enligt myndigheter är ett av Bitcoins stora problem dess volatilitet.

I Finland är Bitcoin inte olagligt, men det räknas inte heller som en ”riktig” valuta. Ett av de stora problemen med Bitcoin är att valutan kopplas ihop med brottslighet och illegal handel. De första fem åren av valutans existens har präglas av flera skandaler. De virtuella valutorna skulle verkligen behöva seriösa, pålitliga och kunniga företag som skulle erbjuda lätt använda, snabba och säkra webbsidor där användare tryggt kan växla olika valutor.

I Norden har det dykt upp några företag som accepterar Bitcoin, men inte tillräckligt många för att någon enbart skulle klara av att leva genom att endast använda sig av valutan. De är på Internet de flesta affärer med Bitcoin sker, en av orsakerna är att det är väldigt lätt att implementera, den låga kostanden, snabbheten i transaktionen oavsett avståndet och att det skyddar företag från bedrägeri.

Bitcoin har under det senaste året haft ett par konkurrerande alternativa virtuella kryptovalutor, men de flesta har dött ut direkt. Det finns idag inte en alternativ virtuell krypterad valuta som är tillräckligt konkurrenskraftig för att slå ut Bitcoin, och Bitcoin är i sin tur idag inte tillräcklig stark nog för att konkurrera med våra statliga valutor.

De båda företagen som jag intervjuade har hittills varit väldigt nöjda med sina Bitcoin affärer och använder den digitala valutan dagligen. Tekniken som utvecklas för de virtuella krypterade valutorna har utvecklat är mycket intressant. Bitcoin kan ses som en pionjär när det gäller de virtuella digitaliserade valutorna. Det är ett nytt finansmedel som många anser ha kommit för att stanna på marknaden.

KÄLLFÖRTECKNING

LITTERATUR

Svenning C., 2003. *Metodboken - samhällsvetenskaplig metod och metodutveckling: klassiska och nya metoder i informationssamhället: källkritik på Internet.* (5 uppl.) Eslöv: Lorentz

E-BÖCKER

Bitcoin: A Peer-to-peer electronic cash system, Satoshi Nakamoto [Online] https://bitcoin.org/bitcoin.pdf [refererad 25.3.2014]

Devon Willcox 1.3.2014 Bitcoin Beginners Guide: Everything You Need To Know To Become Rich With Bitcoins Clydebank Publishing
ASIN: BB00HSTM7W0

Kashmir Hill. 19.1.2014. Secret Money, Living on Bitcoin in the real world. Forbes Media
ASIN: B00IQI5IQY

VIDEO

Hidden Secrets of Money – The Biggest Scam In The History Of Mankind, 15.10.2013. Mike Maloney, GoldSilver.com [Online] https://www.youtube.com/watch?v=iFDe5kUUyT0 [refererad 15.3.2014]

ELEKTRONISKA KÄLLOR

$4,1 goes missing as Chinese bitcoin trading platform GBL vanishes, Kadhim Shubber [Online] http://www.coindesk.com/4-1m-goes-missing-chinese-bitcoin-trading-platform-gbl-vanishes/ [refererad 25.3.2014]

927 people own half of the Bitcoins, Rob Wile [Online] http://www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12 [refererad 8.5.2014]

A $100 worth of Litecoin a year ago is worth $30,000 today, Kashmir Hill [Online] http://www.forbes.com/sites/kashmirhill/2014/01/13/a-100-worth-of-litecoin-a-year-ago-is-worth-30000-today/ [refererad 29.3.2014]

A nation breaks the shackles of fiat currency, Baldur Friggjar Odinsson [Online] http://auroracoin.org/ [refererad 30.3.2014]

Allt det senaste om Bitcoin, SvD Näringsliv, Så fungerar kryptovaluta i din virtuella plånbok [Online] http://www.svd.se/naringsliv/pengar/sparande/allt-det-senaste-om-bitcoin_8794482.svd?sidan=1 [refererad 29.3.2014]

Apple deletes blockchain, Lauren Orsini [Online] http://readwrite.com/2014/02/06/apple-blockchain-last-bitcoin-wallet-ios-app-store-iphone#awesm=~oBHvHC9NBwwSvW [refererad 30.3.2014]

Bitcoin miners building 10 megawatt data center in Sweden, Rich Miller [Online] http://www.datacenterknowledge.com/archives/2014/02/06/bitcoin-miners-building-10-megawatt-data-center-sweden/ [refererad 28.3.2014]

Bitcoins failure rains future for all cryptocurrencies, Carmy Levy [Online] https://ca.finance.yahoo.com/blogs/dashboard/bitcoin-failure-ruins-future-cryptocurrencies-155727898.html [refererad 28.3.2014]

BitcoinWebHosting.net. The History of Bitcoin, The world's first decentralized digital currenc (u.å) [Online] http://historyofbitcoin.org/ [refererad 22.3.2014]

DOGECOIN: how a thing that started as a joke become the hottest digital currency in the world, Rob Wile [Online] http://www.businessinsider.com/what-is-dogecoin-2013-12 [refererad 27.3.2014]

EU:s bankmyndighet varnar för Bitcoin, Huvudstadsbladet FNB-TT [Online] http://hbl.fi/nyheter/2013-12-13/542101/eus-bankmyndighet-varnas-bitcoin [refererad 25.3.2014]

Feds seize silk road, everybody's favorite illegal drug website, Adam Clark Estes [Online] http://gizmodo.com/feds-seize-silk-road-everybodys-favorite-illegal-drug-1440172693 [refererad 29.3.2014]

Forskningsmetodik och Avhandlingsarbete, Ralf Östermark [Online] http://web.abo.fi/fak/esf/gha/lectures/afa/forskningsmetodik/forskningsmetodik.pdf [refererad 10.5.2014]

How Bitcoin works under the hood, Scott Driscoll [Online] http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html [refererad 25.3.2014]

Jamaican Bobsledding and crypto currencies, Marc Chandler [Online] http://www.investing.com/analysis/jamaican-bobsledding-and-crypto-currencies-199612 [refererad 28.3.2014]

Japan says any bitcoin regulation should be international, Sophie Knight, Takayaka Yamaguchi [Online] http://www.reuters.com/article/2014/02/27/us-bitcoin-mtgox-idUSBREA1Q1YK20140227 [refererad 27.3.2014]

Kryptovalutorna växer sig starkare, Mats Lewan. 6 maj, 2014 [Online] http://www.nyteknik.se/nyheter/it_telekom/allmant/article3823967.ece [refererad 8.5.2014]

Man buys $27 of bitcoin, forgets about them, Samuel Gibbs [Online] http://www.theguardian.com/technology/2013/oct/29/bitcoin-forgotten-currency-norway-oslo-home [refererad 25.3.2014]

Meet the manic miner who wants to mint 10% of all new bitcoins, Jon Brodkin [Online] http://arstechnica.com/information-technology/2014/03/meet-the-manic-miner-who-wants-to-mint-10-of-all-new-bitcoins/ [refererad 8.5.2014]

Mt. Gox files for bankruptcy, hit with lawsuit, Yoshifumi Takemoto, Sophie Knight [Online] http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228 [refererad 30.3.2014]

Nascar fans on reddit use dogecoin to sponsor Josh Wise, Chris Estrada [Online] http://motorsportstalk.nbcsports.com/2014/03/25/nascar-fans-on-reddit-use-dogecoin-to-sponsor-josh-wise/ [refererad 28.3.2014]

Nearly 150 breeds of Bitcoin, Andy Greenberg [Online] http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/ [refererad 28.3.2014]

Plånböcker, David Hedqvist [Online] http://www.bitcoin.se/planbocker/ [refererad 29.3.2014]

PPCoin: Peer-to-peer Crypto-currency with proof-of-sake, Sunny King, Scott Nadal [Online] http://www.peercoin.net/assets/paper/peercoin-paper.pdf [refererad 25.3.2014]

Russia bans Bitcoin, Max Lott [Online] http://www.foxnews.com/tech/2014/02/07/russia-bans-bitcoin/ [refererad 29.3.2014]

Silkroad, the virtual drug marketplace, Marie Clarie Van Hout, Tim Bingham [Online] http://www.gwern.net/docs/sr/2013-van-hout.pdf [refererad 2.4.2014]

Stolen target credit cards are selling for 20-100 dollars each, Kashmir Hill [Online] http://www.forbes.com/sites/kashmirhill/2013/12/20/target-credit-cards-are-selling-for-20-100-each/ [refererad 30.3.2014]

Such Generosity: most expensice tweet ever sends $11,000 to Kenyan water charity via Dogecoin, Matt Hickley [Online] http://www.forbes.com/sites/matthickey/2014/03/17/such-generosity-most-expensive-tweet-ever-sends-11000-to-kenyan-water-charity-via-dogecoin/ [refererad 29.3.2014]

The feds are ready to sell 25 million dollar of bitcoin sized from the silk road, Kashmir Hill [Online] http://www.forbes.com/sites/kashmirhill/2014/01/16/the-feds-are-ready-to-sell-the-silk-road-bitcoin-kind-of/ [refererad 30.3.2014]

The history of bitcoin from its very beginning in 2008, Bitcoinberlin [Online] https://bitcoinsberlin.com/the-history-of-bitcoin-from-its-very-beginning-2008-2/ [refererad 25.3.2014]

What is transaction malleability and did it kill MtGox, Alistair Charlton [Online] http://www.ibtimes.co.uk/what-transaction-malleability-did-it-kill-mtgox-1438411 [refererad 30.3.2014]

What is Vertcoin, David Muller [Online] http://vertcoin.org/Vertcoin-DavidMuller.pdf [refererad 25.3.2014]

Who Is Satoshi Nakamoto, Mysterious Bitcoin Founder? John Kelleher [Online] http://www.investopedia.com/articles/general/032614/who-satoshi-nakamoto-mysteriousbitcoin-founder.asp [refererad 15.4.2014]

Virtuella valutor värdefulla för kriminella, Adam Erlandsson [Online] http://www.svd.se/naringsliv/nyheter/varlden/virtuella-valutor-vardefulla-for-kriminella_8627322.svd [refererad 25.3.2014]

OFFICIELLA DOKUMENT

Department of the treasury, Financial Crimes Enforcement Network
Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 18.3.2013
http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [Online] [refererad 29.3.2014]

European Central Bank
Virtual Currency Schemes, 10.2012
https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [Online] [refererad 25.3.2014]

Finlands författningssamling, Skatteförvaltningen 503/201
Inkomstbeskattning av virtuella valutor 28.8.2013, [Online]
http://www.vero.fi/sv-FI/Detaljerade_skatteanvisningar/Inkomstbeskattning_av_personkunder/Inkomstbeskattning_av_virtuella_valutor(28454) [refererad 30.3.2014]

FIGURFÖRTECKNING

TABELLFÖRTECKNING

Ordbok

Transaction malleability - är en term när en transaktion inte innehåller all data, som en transaktion borde innehålla i Bitcoins nätverk.

Distributed denial of service (DDoS) - är en attack emot ett datasystem som utförs av flera personer. Attacken går ut på att skicka stora mängder ovänligdata till mottagares datasystem ända tills det kollapsar av överbelastning.

BTC (฿) – Förkortning till Bitcoin

Peer to Peer-Nätverk (P2P) - Ett icke-hierarkiskt nät d.v.s. ett nätverk av individuella värdar som godkänner hur protokollet implementeras och används

Internet community - Virtuell nätmötesplats

Kryptografiskt hash funktion – En algoritm/ matematisk funktion som förvandlar ett sorts data så att den inmatade informationen inte skall gå att få fram. Används ofta vid lösenordsdatabaser.

Bilaga

Intervjuer

Zas Data
Kimito, Finland
Conny Holtegaard

Webhallen
Stockholm, Sverige
Anton Nilsson

- Varför valde ni att använda valutan bitcoin?

Zas Data

Som en valuta ger den intressanta/spännande möjligheter. Du kan sälja med värdet X idag och imorgon är pengarna värda Y. Få IT butiker har Bitcoin som betalningsmedel.

Webhallen

Enkelt svar: för att vi kan, för att det var lätt att implementera och ”i ropet”.

- Hur har responsen varit från era kunder?

Zas Data

Positiv, det är ju inte bort från någon. Mvs betalas normalt osv.. Viss förundran bland kunder som inte har hört om Bitcoin i annat sammanhang än illegal handel av olika "piristeitä".

Webhallen

99% väldigt positiv, 1 % klagomål på att vi skulle sponsra någon slags svart marknad.

- Hur går betalningssättet gått till?

Zas Data

Kunden kontaktar oss via epost eller kommer in i butiken och berättar vilken/vilka produkter han/hon vill köpa. Vi kommer överens om priset och sedan kollar vi kurssen på bittiraha.fi. Kunden betalar direkt från sin "wallet" eller med bitcoin/wallet app i telefon.

Webhallen

Kunden betalar genom bitpay, rent praktiskt är det nog lättast att bara gå till vår check out för att se hur det ser ut i kundvyn.

- På vilket sätt har ni räknat ut hur mycket bitcoin varorna/tjänsterna kostar?

Zas Data
Direkt omvandling med kursen på bittiraha.fi

Webhallen
Det gör vi inte, vi tar betalt genom Bitpay som konverterar priset till SEK och betalar oss exakt det som vi vill ha betalt i SEK.

- Är det besvärligt när valutan är så rörlig i sin värdering?

Zas Data:
Nej, tvärtom egentligen. En dålig affär kan visa sig vara mycket lönsam en dag/vecka/månad senare. Det är en risk att ta emot Bitcoins när värdet ändrar hela tiden men man måste inte växla dem till euron direkt. Det är som vilken valuta affär som helst.

Webhallen
Tack vare Bitpay är det inte något som berör oss.

- Har det varit många kunder som har använt sig av bitcoin som betalningsmedel?

Zas Data
Ett fåtal transaktioner har vi gjort. Däremot handlar ZAS Data med Bitcoin flera gånger i veckan.

Webhallen
Ja, helt klart över förväntan. Den dagliga omsättningen motsvarar en av våra mindre butiker.

- Har bitcoins som betalningsmedel fungerat bra för Er under den här första perioden?

Zas Data
Ja.

Webhallen
Ja, det skulle jag absolut säga.

- Tror Ni att bitcoin kommer expanderas inom Finland?

Zas Data, Finland
-Det är väl fullt möjligt. Bör dock tas i beaktande att kursen på btc har gungat hårt det senaste 2-3 månaderna.

Webhallen, Sverige
-Jadå. För oss är tanken att vi ska erbjuda det i alla länder där vi är aktiva.