MSc i økonomi og administrasjon

Masteroppgave

Eirik Graven Stokke og Tarje Størksen Otre

Bitcoin - En aktivaboble?

En økonomisk tilnærming til kryptografisk valuta

Trondheim, mai 2014

HANDELSHØYSKOLEN I TRONDHEIM

Høgskolen i Sør-Trøndelag
Handelshøyskolen i Trondheim

Eirik Graven Stokke og Tarje Størksen Otre

Bitcoin - En aktivaboble?

En økonomisk tilnærming til kryptografisk valuta

Bitcoin - An asset bubble?

An economic approach to cryptocurrency

Masteroppgave, MSc i økonomi og administrasjon
Trondheim, mai 2014

Spesialiseringsretning:	Finansiering og Investering
Veileder:	Are Oust

Høgskolen i Sør-Trøndelag
Handelshøyskolen i Trondheim

Eirik Graven Stokke
Tarje Størksen Otre

Bitcoin - En aktivaboble?

Bitcoin - An asset bubble?

MASTEROPPGAVE - Økonomi og administrasjon/siviløkonom
Trondheim, Mai 2014

Hovedprofil: Finansiering og Investering

Veileder: Are Oust

HANDELSHØYSKOLEN
I TRONDHEIM

Forord

Denne avhandlingen markerer vår slutt på masterutdanningen ved Handelshøyskolen i Trondheim. Arbeidet har vært meget spennende og utfordrende å jobbe med. Vi tar samtidig med oss en hel del lærdom, både faglig og om oss selv fra denne prosessen. Fenomenet bitcoin har vært utfordrende å fordype seg i da det er lite tidligere forskning på det relativt nye produktet. Det har vært interessant å følge diskusjonene som har florert blant vanlige folk så vel som økonomiske eksperter, samtidig som vi har jobbet med våre egne analyser.

Vi vil gjerne benytte anledningen til å rette en stor takk til vår veileder Are Oust. Han har vært konstruktiv i tilbakemeldingene, og fungert som en utmerket sparringspartner. Samtidig ønsker vi å rette en stor takk til dere som har hjulpet oss med korrekturlesing.

Innholdet i denne oppgaven står for forfatternes egen regning.

22.Mai 2014

Eirik Graven Stokke

Tarje Størksen Otre

Sammendrag

I denne utredningen ønsker vi å belyse det økonomisk innovative fenomenet bitcoin. Målet med oppgaven er å få klarhet i hva bitcoin er, og med grunnlag i dette undersøke om det er en boble. I første del av utredningen presenterer vi det tekniske som ligger bak og ser på hvordan det fungerer i det økonomiske markedet. Med bakgrunn i fremlagte teorier om valuta, råvare, betalingssystemer og svindler, analyserer vi hvilken definisjon bitcoin passer best innunder. Analysen viser oss at bitcoin ser ut til å hovedsakelig fungere som spekuleringsobjekt, men at det i fremtiden kan være som betalingssystem. Dette begrunnes i lave transaksjonskostnader, noe som muliggjør mikrotransaksjoner.

I den andre delen av utredningen forsøker vi å besvare hovedproblemstillingen vår, hvorvidt bitcoin er en boble. Vi presenterer relevant bobleteori, herunder teorier om rasjonelle og irrasjonelle bobler. Volatilitetsberegninger viser oss at bitcoin har en daglig historisk volatilitet i tidsrommet 1.januar 2012 – 26.mars 2014 på 8,5%. Vi har videre beregnet korrelasjonen mellom bitcoin sin prisutvikling og antall søk i Google til å være 0,96. Beregningene er benyttet til å analysere bitcoin opp mot bobleteori. Analysen viser oss tendenser til at det investeres i bitcoin i håp om en prisøkning i morgen, og at prisen samsvarer med publisiteten. Dette er klare indikasjoner på at markedsprisen ikke reflekterer aktivumets fundamentale faktorer. Basert på analysen fremlegger vi også våre egne beregninger på minste fundamentale verdi til bitcoin, en verdi på $252,74.

Våre analyser og funn sett opp mot relevant bobleteori tyder på at bitcoin er en boble. Fundamental verdi er ikke gjenspeilet i prisen, man kjøper i håp om gevinst i morgen og prisen korrelerer sterkt med publisiteten.

Økonometrisk testing er gjennomført i SPSS, mens øvrig databehandling er gjennomført i Excel.

Abstract

In this thesis we look at the phenomenon bitcoin from an economic perspective. Our goal is to define bitcoin and use this to conclude whether or not it can be characterized as a bubble. In the first part of our thesis we present the technical framework underpinning bitcoin and take a look on how it works in the financial market. On the basis of presented theories on currency, commodity, payment systems and frauds, we analyze what bitcoin can be defined as. The analysis shows us that bitcoin mainly works as a speculative asset today, but may rise as a provider of E-payment system in the future. This is due to the low transaction cost that enables micro transactions.

In the second part of our thesis we try to answer the main issue, whether bitcoin is a bubble or not. We present the readers with relevant bubble theory, including the rational and irrational bubbles. Volatility calculations show us that bitcoin has an estimated daily historical volatility in the period 1.january 2012 – 26.march 2014 of 8,5%. Further, we have calculated the correlation between the price of bitcoin and number of searches in Google to be 0,96. The analysis shows us that the price is strongly correlated with publicity. It seems that investments are based on the hopes of a price increase tomorrow. This clearly suggests that the market price is a poor reflection of the fundamental factors. Based on our analysis, we also present the reader with our own calculation of the smallest fundamental value of bitcoin, a value of $252,74.

Our analysis and findings, using relevant bubble theory, suggests that bitcoin is a bubble. The fundamental value is not reflected in the market price. Individuals primarily buy bitcoins hoping for a price increase, and the price is strongly correlated with the publicity.

Econometric testing is conducted in SPSS, while the rest of the computing is performed in Excel.

Innholdsfortegnelse

Liste over figurer

Liste over tabeller

1. Innledning

I dette kapittelet vil vi redegjøre for hvilke forutsetninger og bakenforliggende faktorer som oppgaven bygger på. Herunder er det naturlig å ta opp hvorfor vi mener dette er en viktig oppgave å skrive, samtidig som vi gir en innføring i hvordan oppgaven er strukturert.

1.1 Motivasjon

Bitcoin er en desentralisert kryptografisk valuta som har fått mye oppmerksomhet den siste tiden. Fra å være et ubetydelig og ukjent fenomen blant de aller fleste, har bitcoin utviklet seg til å bli et velkjent tema i media. Den eventyrlige kursutviklingen i løpet av 2013 har tvunget myndigheter og næringslivet forøvrig til å ta stilling til bitcoin. Det er fascinerende å se at ulike nasjoner konkluderer vidt forskjellig i forhold til hva bitcoin kan kategoriseres som.

"It is a bubble, there is no question about it.... It's just an amazing example of a bubble" - Robert J. Shiller 2014

Sitatet er hentet fra World Economic Forum i Davos 2014, og var svaret bobleguruen Shiller ga på spørsmålet om hvorvidt bitcoin er en boble eller ikke (Weisenthal 2014). Han begrunner dette ut fra den enorme interessen bitcoin genererer.

Fremdeles er kryptografiske valutaer som fenomen lite belyst i økonomisk forskning. Bitcoin utfordrer på mange områder den klassiske tankegangen om hvordan en økonomi fungerer. Det vil derfor være interessant å analysere bitcoin innenfor det etablerte teoretiske rammeverket.

1.2 Problemstilling

For å kunne gjøre en best mulig vurdering av bitcoin som finansielt produkt, har vi utarbeidet følgende problemstilling:

Er bitcoin en boble?

Med underproblemstillingen:

Hva er bitcoin?

1.3 Avgrensning

Eugene Fama mener at det, grunnet hypotesen om markedseffisiens, ikke kan eksistere bobler, siden all tilgjengelig informasjon er fullt ut reflektert i prisen (Cassidy 2010). Vi ønsker ikke å bidra i denne diskusjonen på noen måte, og bruker derfor Joseph Stiglitz sin definisjon av en boble i oppgaven: "Hvis høy pris i dag utelukkende skyldes at investorer tror salgsprisen vil være høy også i morgen - når fundamentale faktorer ikke rettferdiggjør en slik pris - eksisterer det en boble" (Stiglitz 1990).

Bitcoin er et nytt fenomen med lite tilgjengelig informasjon. Vi har derfor ikke hatt særlig mulighet til å lese tidligere forskning på området. Det skjedde mange uforutsette hendelser underveis knyttet til prismessige, lovmessige og infrastrukturmessige faktorer. Det har derfor vært en utfordring å ta hensyn til disse endringene på en god måte.

Bitcoinprisen i denne oppgaven avsluttes 1. april 2014. Endringer etter det er ikke med i våre beregninger. Det kan foreligge informasjon eller andre tall som er hentet etter denne datoen, men dette vil i så fall bli gjort rede for.

Våre vurderinger knyttet til det tekniske rundt bitcoin er gjort etter beste evne. Vi tar forbehold om eventuelle feil i tolkningen av hvordan det fungerer.

1.4 Oppbygning

Avhandlingen starter med et forholdsvis bredt bakgrunnskapittel om hva skaperen mener bitcoin er, og hvordan det fungerer for å sette leseren grundig inn i fenomenet. Videre ser vi på forskjellige teorier rundt valuta og andre definisjoner bitcoin kan kategoriseres som. Dette for å hjelpe oss til å svare på underproblemstillingen om hva bitcoin egentlig er.

Vi fortsetter med teorier som oppgaven vår baserer seg på, herunder forskjellige bobleteorier samt teori om fundamental verdi. Videre har vi et datakapittel hvor vi gir en kort beskrivelse av dataen vi har brukt. Vi går så over til kapittelet som omhandler den metodiske delen av oppgaven, og utdyper hvilken metode vi har brukt for å svare på problemstillingen.

I analysekapittelet legger vi frem våre funn, og setter dem i sammenheng med tidligere gjennomgått teori. Vi avslutter oppgaven med en diskusjon rundt problemstillingene basert på alt vi har presentert tidligere, og med en konklusjon om hvorvidt bitcoin er en boble eller ikke.

2. Bakgrunn

I dette kapittelet skal vi se på det tekniske som ligger bak bitcoin og gi en oversikt over hvordan dette fungerer i det økonomiske markedet. Vi skal også gå gjennom relevant teori som senere skal hjelpe oss til å definere bitcoin.

2.1 Inspirasjonen bak bitcoin

Bitcoin er skapt av Satoshi Nakamoto. Denne personen er ukjent for omverdenen, og navnet er et pseudonym brukt av skaperen for å skjule sin identitet. Programvaren ble sluppet i 2009 sammen med en bruksanvisning på hvordan dette fenomenet fungerer (vedlegg 1). Satoshi Nakamoto er inspirert av manifestet til Wei Dai, som av mange anses å være oppfinneren av kryptografisk valuta gjennom sitt verk om B-money (Dai 1998). Formålet med kryptografisk valuta er en voldsfri verden uten sentralisert styring. Dette skal gjennomføres ved absolutt pseudonymitet blant deltagerne i samfunnet.

2.1.1 Kryptografisk valuta - Tanken bak en digital valuta

Her vil vi først presentere manifestet til Wei Dai. Dette er inspirasjonen til bitcoin som kryptografisk valuta. Vi presiserer at informasjonen i underkapittelet er hentet fra manifestet og forenklet for leser etter best mulig evne.

"I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender and encrypted to its receiver." (Dai 1998)

Dette er tanken bak kryptografisk valuta; et nettverk hvor sender og mottaker kan gjennomføre transaksjoner med hverandre uten å vite hvem den andre parten er. Det opereres med full anonymitet hvor det eneste man kan se er pseudonymene til sender og mottaker. Hver deltager i nettverket har tilgang til en database som sier hvor mye av enheten som tilhører hvert pseudonym. Vi vil se nærmere på hvordan dette fungerer under den tekniske gjennomgangen av bitcoin. Videre i manifestet er det fem punkter som angir hvordan disse kontoene oppdateres. Punktene omhandler hvordan man sørger for at beholdningen til hvert pseudonym oppdateres fortløpende etter hvert som transaksjoner gjennomføres. Det legges

videre frem to protokoller som bygger på hverandre. Protokoll nummer én tar for seg de fem punktene.

1. Hvordan lages penger?

Alle kan lage penger gjennom å kringkaste et ikke tidligere løst beregningsproblem. Den eneste betingelsen som stilles, er at det må være enkelt å kartlegge hvor mye databehandlingskraft som er brukt. I tillegg må løsningen på beregningsproblemet ikke ha alternativ anvendelse eller verdi. Antallet monetære enheter som skapes er lik kostnaden av databehandlingsinnsats i form av en standard mengde med råvare. Tanken er at den som løser problemet mest effektivt, skal få tilbakebetalt i markedsverdi sett i forhold til arbeidsinnsats. Et sentralt moment blir å vurdere hvor mye det ville kostet å kjøpe arbeidsinnsatsen i det åpne markedet.

2. Overføring av penger

A kringkaster til nettverket at hun overfører x-antall til B. Dette legges så til databasen med mindre dette fører til negativ saldo hos en av partene. Da forkastes hele meldingen.

3. Utførelse av kontrakter

For at kontrakter skal være valide, må de inkludere en maksimal oppreisningssum for hver av deltagerne hvis det oppstår mislighold. Det bør også være en megler tilstede hvis kontrakter skulle bli misligholdt. Tanken er at hver deltager debiteres med maksimal gjenoppreisningssum. Denne krediteres en spesiell konto identifisert av en sikker hash[1]. En hash er en algoritme som benytter en datablokk som input, og genererer verdi av en viss størrelse. Kontraktene blir effektive hvis debiteringene går gjennom hos alle deltagerne basert på maksimal gjenoppreisningssum. Hvis noen får negativ balanse på sin konto basert på debiteringen, brytes kontrakten.

4. Konkluderingen av kontrakter

Hvis en kontrakt går gjennom uten problemer, sendes det ut en kringkasting i nettverket. Denne forteller at transaksjonen er gjennomført med signaturer fra deltagende parter. Deretter

[1] En hash er et nummer generert av en streng med tekst. Hasher spiller en rolle i sikkerhetssystemer, hvor de brukes til å forsikre at sendte beskjeder ikke har blitt tuklet med. Sender genererer en hash av meldingen, krypterer den, og legger hashen ved meldingen. Mottaker dekrypterer både meldingen og hashen, produserer en annen hash fra mottatt melding, og sammenligner de to hashene. Hvis det er samsvar mellom hashene, er det meget høy sannsynlighet for at meldingen ble sendt intakt (Rouse 2006a).

krediteres hver av deltagerne sin maksimale gjenoppreisningssum, kontraktskontoen avsluttes, og den avtalte transaksjonen gjennomføres.

5. Håndhevelse av kontrakter
Hvis deltagerne ikke kan komme til enighet selv ved bruk av megler, kringkaster hver av deltagerne sine tanker om gjenoppreisning og eventuelle bevis sammen med kringkastingen. Hver deltager gjør så en beslutning om oppreisning for så å modifisere sine kontoer deretter.

I protokoll nummer to er kontoene som viser hvor mye hver deltager har, holdt av et utvalg av deltagere eller servere. Formatet på kringkastingen foregår på samme måte som ved første protokoll. Forskjellen er at involverte deltakere ved hver transaksjon må verifisere at kringkastingen er mottatt og prosessert på riktig måte ved hjelp av et tilfeldig utvalg servere.

Systemet bygger på at de utvalgte serverne gjennomfører oppgavene på riktig måte. For å oppmuntre til dette kreves det at serverne setter inn penger på en konto. Denne summen utløses som bøter eller finnerlønn ved bevis på misligholdelse. Deltakere må også gjennomføre periodiske publiseringer i nettverket om hvor mye råvare som skapes og hvor mye man eier. Det må verifiseres av hver enkelt deltager at dette stemmer.

Andre inspirasjonskilder
Nick Szabos har vært involvert i arbeidet med kryptografisk valuta siden 90-tallet. Han er også inspirert av Wei Dai sine tanker om anonymitet og desentralisert styring. Han blir på linje med Wei Dai ansett som en inspirasjonskilde for skaperen av bitcoin, men da mest i forhold til det tekniske og problematikken rundt datasikkerhet. Szabos lanserer en løsning på problemet rundt betalingssvindel, hvor kjøper trekker tilbake betalingen i det selger har sendt byttegjenstanden. Betalingen benyttes deretter et annet sted (Szabos 2005). Dette løser problemet knyttet til dobbeltbruk, som ikke var utdypet godt nok av Dai i 1998.

Som nevnt tidligere, er formålet en verden uten sentralisert styring og komplett anonymitet blant befolkningen. Bitcoin ble lansert i 2009 av Satoshi Nakamoto, og kom som et svar på finanskrisen da den sentraliserte styringen til dels måtte ta på seg skylden for resesjonen (Feuer 2013).

2.2 Hva er bitcoin? – En teknisk gjennomgang

Under følger en teknisk gjennomgang av hvordan bitcoin fungerer. Dette underkapittelet reflekterer på ingen måte vårt syn på bitcoin, men er en mer lettfattelig omskriving av manualen som er skrevet personlig av skaperen Satoshi Nakamoto (vedlegg 1). Det tekniske aspektet er ikke så lett å forstå, men vi håper at dette kan bidra til økt forståelse om hvordan det hele henger sammen. Vi presiserer at dette er en forenklet gjengivelse av manualen til Nakamoto.

Introduksjon

Netthandel i sin nåværende form er nesten fullstendig avhengig av en finansiell institusjon som tredjepart ved en elektronisk betaling. Det finnes en del svakheter ved denne tillitsbaserte modellen. Irreversible transaksjoner er i utgangspunktet ikke mulig, siden finansielle institusjoner ikke kan unngå å fungere som megler i uenigheter. Meglingen øker transaksjonskostnaden, siden megleren skal ha sin del for å fungere som mellommann, og gjør muligheten for mikrotransaksjoner omtrent umulig. Tapet av muligheten til å gjøre irreversible betalinger for irreversible tjenester øker kostnaden for alle aktører. Muligheten for reversering av transaksjoner gjør at behovet for tillit sprer seg. Forhandlere må ha en naturlig skepsis til sine kunder og innhente mer informasjon enn strengt tatt nødvendig. Fysisk valuta er det eneste som kan fjerne kostnads- og betalingsusikkerheten, men ingen slike mekanismer finnes for å fjerne mellommannen i netthandel.

Det som trengs er et elektronisk betalingssystem basert på kryptografisk bevis istedenfor tillit, og som gjør det mulig for to villige parter å gjennomføre en transaksjon direkte med hverandre uten behovet for finansiell institusjon. Transaksjoner som er beregningsmessig tungvint å reversere, vil beskytte selgere fra svindel. Videre kan en mekanisme hvor pengene blir holdt et tredjested inntil den riktige verifikasjonen er mottatt enkelt implementeres for å beskytte kjøpere. Løsningen som legges frem på dobbeltbruk-problemet[2] er ved bruk av en peer-til-peer[3] distribuert tidsstempel[4] server for å generere beregningsmessig bevis på den

[2] Dobbelbruk er situasjoner hvor kjøper eksempelvis venter til varen er sendt for så å reversere kjøpet og bruke de samme myntene til å kjøpe noe annet uten å sende penger til selger.
[3] Peer-to-peer er et internett-nettverk som tillater en gruppe computerbrukere med samme nettverksprogram å koble seg til hverandre og få direkte tilgang til filer fra en annens hard drive (Rouse 2005).
[4] Tidsstempel er det digitale beviset, i form av dato og klokkeslett, på at en hendelse inntraff.

kronologiske rekkefølgen av transaksjoner. Systemet er sikkert så lenge ærlige noder[5] til sammen kontrollerer mer datakraft enn en samarbeidende gruppe av angripere.

Transaksjoner

Vi definerer en elektronisk mynt som en kjede av digitale signaturer. Hver eier overfører mynten ved å digitalt signere en hash av tidligere transaksjoner og den offentlige nøkkelen til den neste eieren, og tilfører disse til enden av mynten. En betalingsmottaker kan verifisere signaturene for å verifisere kjeden av eierskap.

Problemer oppstår hvis betalingsmottaker ikke kan verifisere at en av eierne ikke har dobbelbrukt mynten. En vanlig løsning er å introdusere en sentralstyringsmakt eller finansiell institusjon, som sjekker hver transaksjon for dobbelbruk. Etter hver transaksjon må mynten returneres til den finansielle institusjonen for at en ny skal utstedes, og bare mynter utstedt direkte fra den finansiell institusjonen, stoles på å ikke være dobbelbrukt. Problemet med denne løsningen er at skjebnen til hele pengesystemet er avhengig av institusjonen som utsteder mynter. Dette fordi hver transaksjon må gå gjennom den, akkurat som en bank.

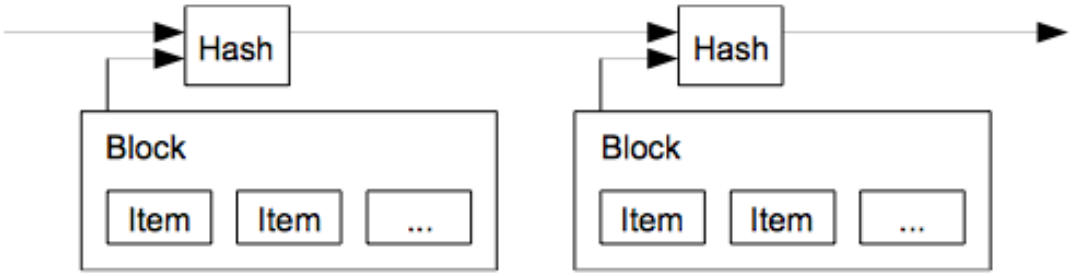
Vi trenger en måte for betalingsmottaker å vite at tidligere eier ikke signerte noen tidligere transaksjoner. For vårt formål er det den tidligste transaksjonen som teller, så vi bryr oss ikke om senere forsøk på dobbelbruk. Den eneste måten å bekrefte fraværet av en transaksjon er å være klar over alle transaksjoner. I situasjonen hvor en finansiell institusjon er utsteder, er utsteder klar over alle transaksjoner og bestemmer hvilken som kom først. For å oppnå dette uten en tillitsbasert modell må transaksjoner publiseres offentlig. Vi trenger et system hvor deltagerne er enige om i hvilken rekkefølge transaksjonene ble mottatt. Betalingsmottaker trenger bevis for at når hver transaksjon inntreffer, er majoriteten av noder enig om at den ble mottatt først.

Tidsstempelserver

Løsningen vi foreslår begynner med en tidsstempelserver. En tidsstempelserver fungerer ved å hashe en blokk med gjenstander. Deretter tidsstemples og publiseres hashen bredt, som i en avis. Tidsstempelet beviser at dataen må ha eksistert på tidspunktet for å bli tatt opp i hashen.

[5] En node er et tilkoblingspunkt i et nettverk, eksempelvis en datamaskin (Rouse 2006b).

Hvert tidsstempel inkluderer et tidligere tidsstempel i sin hash. Dette lager en kjede som for hvert nye tidsstempel forsterker den som kommer før i rekken.



Figur 1: Tidsstempelserver (Nakamoto 2009)

Proof-of-work (arbeidsbevis)

For å implementere en distribuert tidsstempelserver basert på peer-til-peer, trenger vi et arbeidsbevissystem. Arbeidsbeviset involverer å skanne for en verdi som etter å ha blitt hashet, vil begynne med et nummer av null-bits[6]. Gjennomsnittsarbeidet som trengs er eksponentielt i tallet av antall null-bits som trengs, og kan verifiseres ved å utføre en enkelt hash.

For vårt tidsstempelnettverk implementeres arbeidsbeviset ved tilvekst av en nonce[7] i blokken til en verdi er funnet som gir blokkens hash det nødvendige antallet null bits. Når datakraftinnsatsen er utvidet til å tilfredsstille arbeidsbeviset, kan ikke blokken endres uten å gjøre arbeidet på nytt. Arbeidsbeviset løser også problemet ved å bestemme representasjon i flertallsbeslutninger. Hvis flertallet var basert på én-IP-adresse-én-stemme, kunne dette ført til at folk allokerte flere IP adresser for flere stemmer. Arbeidsbeviset er essensielt én-datamaskin-én-stemme. Flertallsbeslutninger representeres av den lengste kjeden som har gjennomført den beste innsatsen for å skape et arbeidsbevis. Hvis majoriteten av datakraft er kontrollert av ærlige noder, vil den ærlige kjeden vokse raskest og utkonkurrere utfordrende kjeder. For å modifisere en tidligere blokk må en angriper omgjøre alt arbeidsbeviset til den gitte blokken og alle blokkene etter det, for så å ta igjen og gå forbi arbeidet til de ærlige

[6] En bit er den minste mulige delen av informasjon. En bit kan kun ha to tilstander: 1 eller 0.
8 bits (1 byte) = 2^8 = 256 muligheter (Shapiro 2000).
[7] En nonce er et nummer generert for spesifikk bruk, som autentisering av en økt. Det står for ”nummer brukt én gang”. En nonce er typisk en verdi som varierer med tiden, selv om det noen ganger brukes et veldig stort nummer. En nonce kan være et tidsstempel, eller et spesielt merke for å begrense eller forhindre uautorisert gjenbruk eller reproduksjon av en fil (Rouse 2008).

nodene. For å kompensere for økende datakapasitet og varierende interesse fra ulike noder over tid, bestemmes vanskeligheten for arbeidsbeviset av et bevegende gjennomsnitt som sikter mot et gjennomsnittlig antall blokker per time. Hvis de genereres for raskt, øker vanskelighetsgraden.

Nettverk

Stegene for å kjøre nettverket er følgende:

1. Nye transaksjoner kringkastes til alle noder.
2. Hver node samler nye transaksjoner i en blokk.
3. Hver node jobber med å finne et vanskelig arbeidsbevis for blokken.
4. Når en node finner arbeidsbeviset, kringkastes blokken til alle nodene.
5. Noder aksepterer blokken kun hvis alle transaksjonene i den er valide og ikke allerede brukt.
6. Noder uttrykker sin aksept av blokken ved å jobbe med å lage den neste blokken i kjeden, de bruker da hashen til den aksepterte blokken som forrige hash.

Noder ser alltid på den lengste kjeden som den rettmessige, og vil alltid jobbe med å utvide denne. Hvis to brukere kringkaster forskjellige versjoner av den neste blokken samtidig, kan noen noder motta ulike blokker først. I dette tilfellet jobber de med den de mottok først, men tar vare på den andre grenen i tilfelle den blir lengre. Båndet vil bli brutt når det neste arbeidsbeviset blir funnet, og den ene grenen blir lengre; nodene som da jobbet med den andre grenen bytter til den lengste. Nye transaksjoner som kringkastes når ikke nødvendigvis ut til alle nodene. Så lenge de når mange nok noder, vil de gå inn i en blokk ikke lenge etter. Blokk-kringkastere er også tolerante av manglende beskjeder. Hvis en node ikke mottar en blokk, vil noden etterspørre blokken når den mottar neste blokk og oppdager at det mangler en.

Incentiv

Den første transaksjonen i en blokk er en spesiell transaksjon ved at den markerer begynnelsen av en ny mynt som er eid av skaperen av blokken. Dette tillegger et incentiv for noder å støtte nettverket, og tilrettelegger for en måte å distribuere myntene inn i sirkulasjon, siden det ikke er noen sentralmyndighet til å distribuere dem. Den jevne tilstrømmingen av en konstant mengde av nye mynter er lik den for gullgravere som utvider ressursene ved å tilføre nytt gull til sirkulasjonen. I vårt tilfelle er det datakraft-tid og elektrisitet som utvides.

Incentivet kan også finansieres ved hjelp av transaksjonsavgifter. Hvis sluttverdien av en transaksjon er mindre enn innskuddsverdien, er differansen en transaksjonsavgift som tillegges incentivets verdi av blokken som inneholder transaksjonen. Når et forhåndsbestemt antall mynter er i sirkulasjon, kan incentivet i sin helhet forandres til transaksjonsavgifter og bli totalt inflasjonsfritt.

Incentivet kan hjelpe til å oppmuntre noder til å forbli ærlige. Hvis en grådig angriper klarer å samle mer datakraft enn alle de ærlige nodene, må han velge mellom å bruke sin datakraft til å svindle folk ved å stjele tilbake sin betalinger, eller å bruke det til generere nye mynter. Det er mulig han finner at ut det er større profitt i å spille etter reglene. Slike regler favoriserer den med flere nye mynter enn noen andre til sammen, heller enn å undergrave systemet og gyldigheten av hele sin egen formue.

Tilbakekreve lagringsplass

Når den siste transaksjonen i en mynt er begravd under nok blokker, kan tidligere transaksjoner forkastes for å spare diskplass. For å organisere dette uten å ødelegge blokkens hash, kan transaksjonene hashes i et Merkle-tre[8], med bare roten inkludert i blokkens hash. Gamle blokker kan således bli komprimert ved å kutte av grener av treet. De innvendige hashene trenger ikke å bli lagret.

Forenklet betalingsverifikasjon

Det er mulig å verifisere betalinger uten å kjøre en fullstendig nettverksnode. En bruker trenger kun å holde en kopi av blokk-overskriftene til den lengste kjeden av arbeidsbevis. Denne kan han få ved å etterspørre nettverksnoder frem til han er overbevist at han har den lengste kjeden, og opprettholde Merkle-grenen som linker transaksjonen til blokken den er tidsstemplet i. Han kan ikke sjekke transaksjonen på egenhånd, men ved å linke den til et sted i kjeden, kan han se at nettverksnoden har akseptert den, og blokkene som tillegges i ettertid bekrefter videre at nettverket har akseptert den. Verifikasjonen er troverdig så lenge ærlige noder kontrollerer nettverket, men er mer sårbar hvis nettverket blir overmannet av en angriper. Mens nettverksnoder kan verifisere transaksjoner selv, kan den enklere metoden bli lurt av en angripers fabrikkerte transaksjon så lenge en angriper kan fortsette å styre nettverket. En strategi for å beskytte seg vil være å akseptere varsler fra nettverksnoder når de

[8] Merkle-trær er binære trær av hasher (Szydlo 2004).

oppdager en ugyldig blokk. Dette sørger for at brukerens programvare laster ned hele blokken og varslede transaksjoner for å bekrefte inkonsistensen. Bedrifter som mottar hyppige betalinger, kommer sannsynligvis til kjøre sine egne noder for mer uavhengig sikkerhet og raskere verifikasjon.

Kombinering og splitting av verdi

Selv om det vil være mulig å håndtere mynter individuelt, vil det være uhåndterlig å lage en separat transaksjon for hver cent i en transaksjon. For å tillate at verdi splittes og kombineres, inneholder transaksjoner flere inputs og outputs. Normalt vil det enten være én enkelt input fra en større tidligere transaksjon eller flere inputs som kombinerer mindre summer. På det meste kan det være to outputs; én for betalingen og én for å returnere vekslepengene tilbake til sender. Siden man aldri får behov for å hente ut én enkelt transaksjonshistorie, er det ikke noe problem at transaksjonene er avhengig av hverandre.

Personvern

Den tradisjonelle bankmodellen oppnår en viss grad av personvern ved å begrense tilgang til informasjon om involverte parter og den tillitsbaserte tredjeparten. Nødvendigheten av å annonsere alle transaksjoner offentlig utelukker denne metoden, men personvern kan fortsatt opprettholdes ved å bryte informasjonsflyten et annet sted. Løsningen er å holde de offentlige nøklene anonyme. Offentligheten kan se at noen sender en mengde mynter til noen andre, men uten informasjon som linker transaksjonen til identifiserbar mottaker. Dette er likt med nivået av informasjon som gis ut ved aksjebørser, hvor tiden og størrelsen av individuelle handler offentliggjøres, men uten å fortelle hvem de to deltagerne er. Som ekstra beskyttelse skal et nytt nøkkelpar brukes for hver transaksjon for å sørge for at nøkkelparet ikke blir linket til en kjent eier. Enhver form for link er derimot uunngåelig ved fler-input transaksjoner som nødvendigvis avslører at deres input er eid av samme eier. Risikoen er at hvis en eiers nøkkel avsløres, kan linkingen avsløre andre transaksjoner som tilhører den samme eier.

Kalkulasjoner

For å vise hvor vanskelig det vil være for en eventuell angriper å generere en alternativ kjede raskere enn den opprinnelige ærlige kjeden, er det utført en del kalkulasjoner. Selv om en angriper vil være i stand til å lage en alternativ kjede, gjør ikke det at systemet er åpen for vilkårlige endringer, eksempelvis å ta penger som aldri tilhørte angriperen i utgangspunktet. Noder vil aldri akseptere en ugyldig transaksjon som betaling eller en blokk. En angriper kan

bare prøve å endre en av sine egne transaksjoner for å ta tilbake penger han nettopp brukte. Dette er det fenomenet vi tidligere har snakket om, dobbelbruk. Det vil altså ikke være mulig å stjele eller endre transaksjoner som angriperen ikke selv har deltatt i. Resultatene viser at sannsynligheten for at en angriper kan ta igjen den ærlige kjeden, faller eksponentielt med antall blokker han er bak.

Tabellen viser gitte verdier for q og z som fører til at det er en sannsynlighet på 0,001 for at en angriper klarer å ta igjen blokkrekka.

Sannsynlighet for at angriper finner neste blokk	Antall blokker angriper er bak den ærlige kjeden
q = 0.10	z = 5
q = 0.15	z = 8
q = 0.20	z = 11
q = 0.25	z = 15
q = 0.30	z = 24
q = 0.35	z = 41
q = 0.40	z = 89
q = 0.45	z = 340

Tabell 1: Sannsynligheter for at angriper tar igjen blokkrekka

Beregningene viser at sannsynligheten er under 0,1% for at en angriper tar igjen den ærlige rekken gitt ved sannsynligheten q for at angriperen finner den neste blokken i rekken når han er z blokker bak. Hvis q eksempelvis er 0,3, altså at det er 30% sannsynlighet for at angriperen finner den neste blokken og han er 24 eller flere blokker bak i utgangspunktet, er det under 0,1% sjanse for at angriperen tar igjen den ærlige rekken.

Konklusjon

Vi har foreslått et system for elektroniske transaksjoner som ikke baserer seg på tillit. Vi startet med det vanlige rammeverket av mynter laget fra digitale signaturer, noe som gir sterk eierskapskontroll, men er ukomplett uten en måte å forhindre dobbelbruk. For å løse dette, foreslo vi et peer-til-peer nettverk ved bruk av arbeidsbevis for å lagre en offentlig historie av transaksjoner som raskt blir beregningsmessig upraktisk for en angriper å endre hvis ærlige noder kontrollerer majoriteten av datakraften. Nettverket er robust i sin ustrukturerte enkelhet. Noder jobber alle samtidig med liten koordinasjon. De trenger ikke å identifiseres siden beskjeder ikke er rutet til ett bestemt sted, og trenger kun å leveres på en best mulig måte.

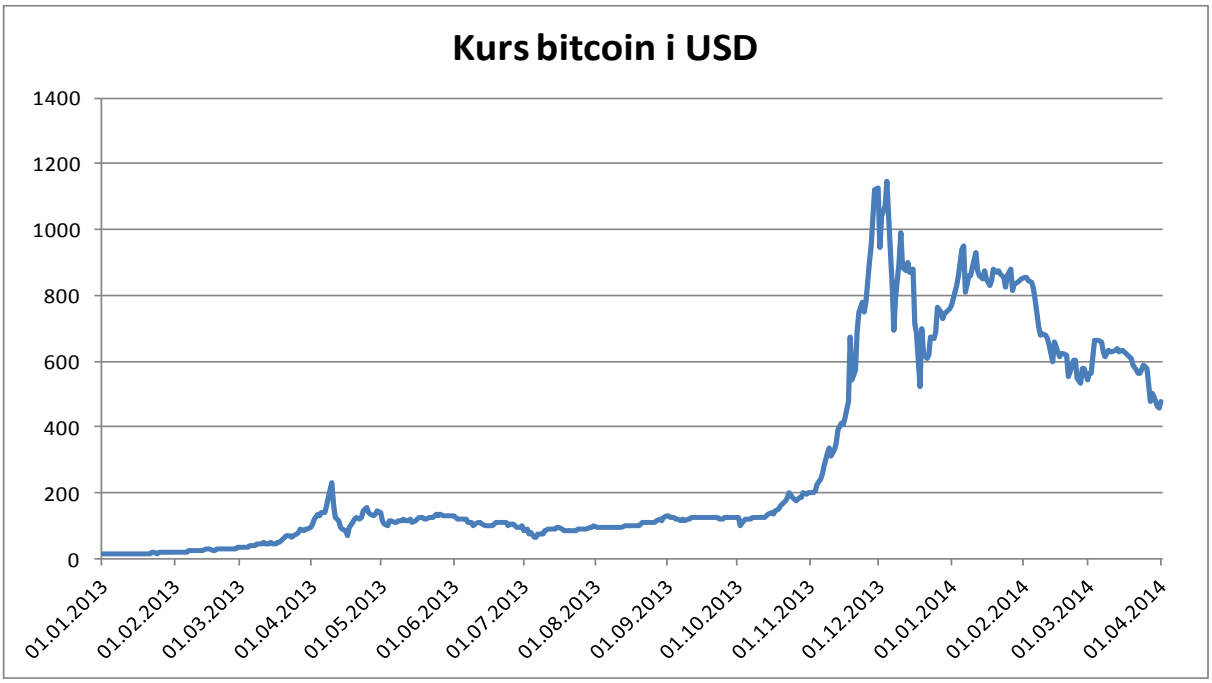
Noder kan forlate og komme tilbake igjen til nettverket som de ønsker, de aksepterer arbeidsbeviset som bevis på hva som skjedde når de var fraværende. De stemmer med sin datakraft, og uttrykker sin aksept av gyldige blokker ved å jobbe med å utvide blokkene. De avslår ugyldige blokker ved å ikke jobbe på dem. Regler som trengs og incentiver kan utøves med denne konsensusmekanismen.

2.3 Hvordan fungerer bitcoin i det økonomiske markedet?

Vi har sett på hvordan bitcoin fungerer rent teknisk. Under følger en kort gjennomgang av kursutviklingen og de forskjellige måtene å tilegne seg bitcoin.

2.3.1 Pris

Bitcoin verdsettes som regel mot amerikanske dollar. Under ser vi prisutviklingen fra 1. januar 2013 til 1.april 2014.

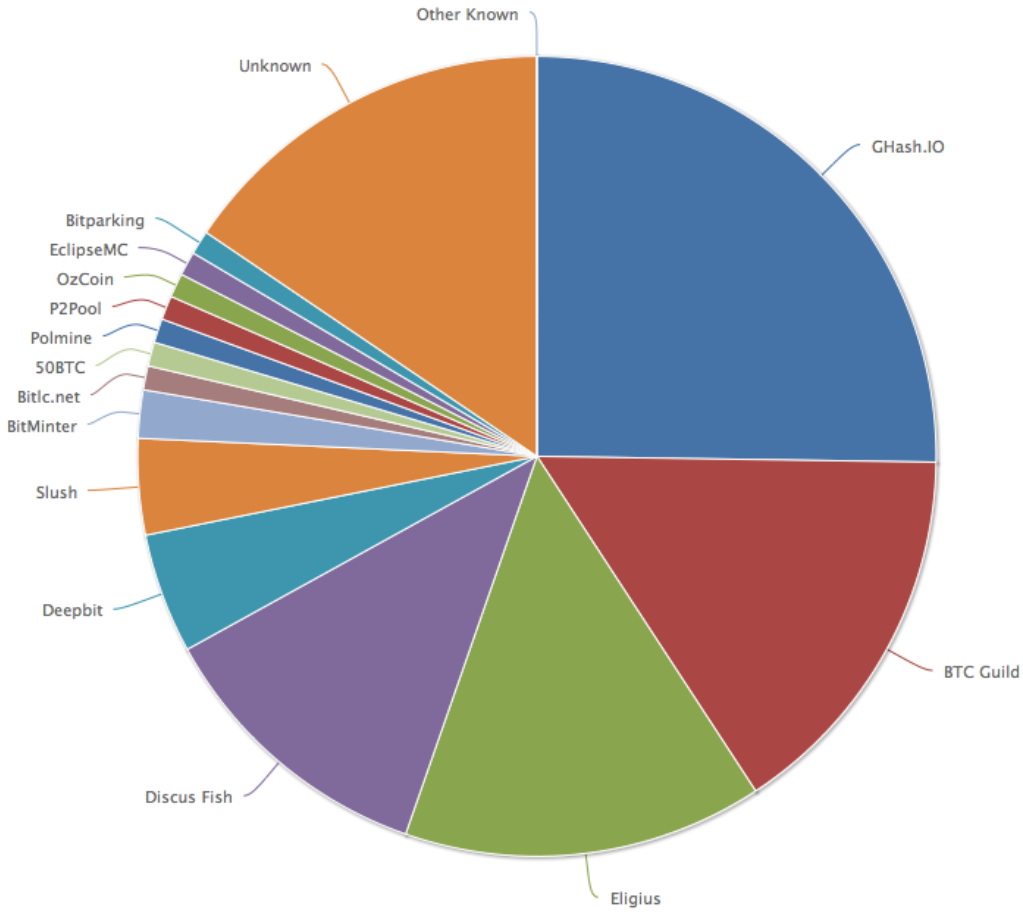


Figur 2: Kursutvikling (Quandl 2014)

2.3.1 Mining

Nye mynter kan utvinnes gjennom mining. Her bruker man datakraft til å løse algoritmer som igjen gir en belønning i form av bitcoin. Dette kan for enkelthets skyld sammenlignes med å

grave etter gull fordi belønningen baseres både på innsats og flaks. Det er et innebygd tilbudsstak på 21 millioner mynter. Det anslås at nesten alle myntene vil være hentet ut rundt år 2030 (London og Melbourne 2011). I vedlegg 4 viser vi hvordan vanskelighetsgraden på miningen har utviklet seg. Før kunne man utvinne mynter på en vanlig datamaskin, men det har etter hvert blitt nødvendig med spesiallaget utstyr for denne jobben. På Island er det satt opp flere maskiner som utelukkende benyttes til utvinning av bitcoin, og dette gjør de 24 timer i døgnet (Alden 2013). Valget av Island ble tatt på grunnlag av den arktiske luften som fungerer som billig nedkjøling av maskinene. Det er en avveiing mellom strømkostnader og hvor mye avkastning man får på miningen, som avgjør lønnsomheten ved å fremstille flere.



Figur 3: Oversikt over utvinnerne i markedet (Blockchain 2014b)

Figur 3 viser hvilke aktører som står for utvinning av nye mynter. Vi ser at det er flere store aktører hvor GHash.IO er størst med om lag en fjerdedel av den totale miningen. Det har vært en stor økning i datakraften som benyttes til å utvinne nye mynter. Nettverket utklasset

allerede i mai 2013 de 500 sterkeste datamaskinene i verden til sammen i total datakraft (Brunner 2013).

2.3.2 Børs

Kjøp og salg foregår på egne børser på internett. MtGox var den største børsen frem til starten av 2014. Da ble det avdekket at hackere hadde benyttet seg av et sikkerhetshull og stjålet flere hundre tusen mynter (BBC 2014b). Som en følge av dette ble MtGox nedlagt. I ettertid har to andre børser, BitStamp og btc-e, overtatt mye av markedet. Norges første børs for handel av bitcoin heter Justcoin. Den fungerer imidlertid bare som et bindeledd mellom kjøper og selger (Justcoin 2014).

I begynnelsen av desember 2013 ble rundt 58 % av kjøp og salg med bitcoin foretatt i kinesiske yuan. 37 % ble gjennomført med amerikanske dollar og under 2 % med euro (Boehler 2013).

2.3.3 Salg

Man kan selge varer eller tjenester mot betaling i bitcoin. Senere i avhandlingen kommer vi mer inn på hvordan dette fungerer i praksis.

2.4 Hva kan bitcoin brukes til?

Bitcoin kan enten benyttes som spekuleringsmiddel, eller til å kjøpe produkter og tjenester hos tilbydere som aksepterer bitcoin som betalingsmiddel. Myntene man har anskaffet seg oppbevares i programvare som kalles lommebøker.

2.4.1 Lommebok

Lommebøker for bitcoin lagrer private nøkler som man trenger for å få tilgang til en spesifikk adresse i bitcoin-kjeden. Disse nøklene gjør det mulig for eieren å bruke midlene sine (Coindesk 2014c). Det oppbevares aldri bitcoin i lommeboka. Det som oppbevares, er sikre private nøkler som benyttes til å få tilgang til brukerens offentlige adresse. Dette muliggjør signering av transaksjoner.

Lommebøkene kommer i flere varianter og finnes på de fleste plattformer. Dette gjelder datamaskiner, mobiler, i nettleseren og som egen hardware. Mobillommeboken har størst praktisk betydning av de ulike lommebøkene. Det er denne man tar med seg for å betale i fysiske butikker. Lommeboken fungerer som en applikasjon på mobilen, og gjør det mulig for brukeren å betale direkte med telefonen. I noen tilfeller kan man også legge telefonen mot en avleser og betale på den måten fremfor å taste inn nødvendig informasjon. En vanlig egenskap ved de fleste lommebøkene er at de ikke laster ned hele blokkrekken. De laster bare ned deler av rekken i form av blokk-overskrifter, som vist i den tekniske fremleggingen. Programvaren stoler derfor på at andre sikre noder i nettverket garanterer for at blokkrekken er korrekt (Coindesk 2014c). Lommebøker på datamaskinen laster derimot ned hele kjeden for å verifisere betalingen. Dette vil bli mer kostbart på en mobil enhet siden man da må benytte mobilnettverket.

For å kunne gjennomføre en transaksjon er man nødt til å ha de private nøklene knyttet til en konto. Dersom man mister tilgangen til en lommebok, mister man derfor også tilhørende mynter for alltid. Det er umulig å få tilbake de private nøklene. Det er flere tilgjengelige måter å sikre seg på gjennom krypterte passord på lommeboken og det å ha back-up av hele lommeboken. Den sikreste måten er derimot noe som kalles kaldlagring, hvor man lagrer lommeboken på en datamaskin som ikke er tilkoblet et nettverk (Coindesk 2014c). Når man vil gjennomføre transaksjoner, overfører man fra kaldlagring til en varm lommebok som er tilkoblet internett. På denne måten risikerer man bare å miste beløpet som skal overføres fremfor hele beholdningen.

2.4.2 Kjøp av varer og tjenester

Bitcoin brukes i mange ulike markeder verden over. Det er foreløpig mest utbredt som betalingsmiddel for e-tjenester, men kan også benyttes til å kjøpe fysiske varer (Coindesk 2014d). Overstock er den største aktøren som tilbyr betaling av varer med bitcoin. Dette er en amerikansk nettbutikk som tilbyr et bredt spekter av varekategorier, eksempelvis smykker og elektronikk. Selskapets totale omsetning i 2013 var over 1 milliard USD (Overstock 2014). Etter om lag to måneder hadde de omsatt for over 1 million USD ved betalinger foretatt i bitcoin (Wilhelm 2014). En annen måte å benytte bitcoin på, er ved kjøp av gavekort. Man får eksempelvis kjøpt gavekort som kan benyttes hos blant annet Walmart, Amazon og Nike (Coindesk 2014d). Gavekortene begrenser seg derimot stort sett til landet de er utstedt i.

Antallet fysiske butikker som tilbyr betaling med bitcoin har økt etter hvert, og det finnes tilgjengelige oversikter over hvilke aktører dette gjelder. Spendbitcoin er en nettside hvor bedrifter selv kan gå inn og registrere at de aksepterer bitcoin (Spendbitcoin 2014). En take-out leverandør som heter Foodler, tilbyr sine kunder å bruke bitcoin som betalingsmiddel (Foodler 2014). Der kan man få mat levert i over tre tusen forskjellige byer verden over.

2.5 Valuta

Vi har nå sett på hvordan bitcoin fungerer i markedet. Videre skal vi presentere relevant valutateori og hvilke oppgaver en sentralbank utfører. Denne gjennomgangen legger grunnlaget for analysen om hvorvidt bitcoin kan defineres som valuta.

2.5.1 Valutateori

I følge Milton Friedman kan hva som helst være penger, eksempelvis stein, jern og gull (Friedman 1992). Det som gjør disse tingene til penger er ikke hva de er, men hva de brukes til. De kan ha en verdi i seg selv på samme måte som gull og andre råvarepenger, eller de kan være verdiløse slik som banknoter og bankinnskudd. En penges verdi kan derfor være forskjellig fra enhetens fundamentale verdi. Verdien av penger er hva folk verdsetter dem til i en byttehandel i forhold til noe annet. Alle penger er kredittpenger når de benyttes som et byttemiddel (Friedman 1992). Kredittpenger kan i bunn og grunn være hva som helst så lenge de symboliserer verdien på gjenstanden som er gitt vekk. Pengene blir en lagringsplass for verdi siden de holdes som tegn på lik verdi med den gjenstanden som ble gitt bort. Råvarepenger er det som har blitt brukt mest tidligere, men verdien av penger er ikke alltid den samme som dens verdi som råvare. Fundamental verdi av råvaren og verdi som pengeenhet kan påvirke hverandre.

Kvantitetsteorien dreier seg om verdien av penger, eksempelvis hva som kan kjøpes for en norsk krone i markedet (Friedman 1992). Denne sier oss at verdien avhenger av hvor mye penger det er, hvor mye som holdes ute av sirkulasjon, og hvor mange bytter sirkulerende penger vanligvis dekker. Den uttrykkes ved MV = PT, hvor ”M” er den reelle kvantiteten av penger også kjent som pengemengden. ”V” er et tegn på hastigheten, hvor hurtig penger sirkuleres eller hvor lenge de holdes ute av sirkulasjon. ”T” er antallet transaksjoner og ”P” er prisnivået.

Denne ligningen benyttes til å forklare hvordan inflasjon og deflasjon i markedet gjør penger mindre eller mer verdifulle over tid. Kvantitetsteorien forklares ut fra studier som viser at inflasjon og deflasjon historisk sett har oppstått uavhengig av økonomisk vekst og resesjon (Friedman 1992).

Inflasjon og deflasjon oppstår når det samlede prisnivået går henholdsvis opp og ned. Inflasjon vil oppstå hvis V og T holdes konstant samtidig som M går opp, dersom tilførselen av penger øker uten andre endringer. Inflasjon kan også oppstå hvis V går opp (folk bruker penger raskere) eller hvis T synker (økonomien krymper), mens de andre variablene holdes konstant. Det meste av inflasjon skyldes derimot en uavhengig økning av pengemengden. Deflasjon forekommer vanligvis fra en av to grunner; enten fordi økonomien vokser og antall transaksjoner øker, eller pengemengden synker.

Den kjente nobelprisvinneren Paul Krugman trekker frem en fortelling om et barnepass-samarbeid som et klassisk eksempel på kvantitetsteorien (Gobry 2013). En rekke personer ble enige om å sitte barnevakt for hverandre for å slippe og betale ukjente for jobben. For å sørge for at alle gjorde sin del, bygget de en alternativ valuta basert på kuponger til verdi av én time barnepass. Et problem som oppstod, var at folk prøvde å samle opp kuponger for å ha i reserve, noe som ødela hele samarbeidet. Jo flere som prøvde å samle opp kuponger, jo mindre var folk villige til å gå ut og få barnepass. Siden det var mindre kuponger i sirkulasjon, var konsekvensen at færre barn ble passet. Barnepass-samarbeidet hadde havnet i en resesjon. Det var en klassisk likviditetsfelle. Løsningen ble å utstede flere kuponger, noe som førte til at samarbeidet blomstret igjen.

Per 28. april 2014 er den gjennomsnittlige minetiden per blokk cirka 8 minutter og 22 sekunder, og hver blokk gir en premie på 25 mynter eller ca $11 000 (Coindesk 2014a). Dette vil si at pengemengden øker med 25 bitcoin hvert åttende minutt i gjennomsnitt, eller omtrentlig 4400 per dag. Etter hver 210 000 blokk som blir utvinnet, blir premien halvert (BBC 2012). Det har blitt minet 298 000 blokker siden oppstarten. I likhet med den norske kronen forsvinner det et visst antall bitcoin etter hvert som tiden går. Det finnes eksempler på personer som av ulike årsaker mister tilgangen til lommebøkene der bitcoin-nøklene er lagret (Harrison 2013). Disse myntene havner dermed ute av sirkulasjon, og vil trolig ikke kunne

sirkulere igjen. Det er umulig å finne et eksakt tall på hvor mange mynter dette gjelder, ettersom ingen kontoer blir fjernet fra infrastrukturen. De blir bare stående urørte.

Skatteetaten i USA definerer en virtuell valuta som en representasjon av verdi som fungerer på lik linje med et byttemiddel, en såkalt unit of account, og/eller lagringsplass for verdi (Internal Revenue Service 2014a). En unit of account er en grunnleggende egenskap ved penger. Den gir en måleenhet som brukes til å definere, ta opp og sammenligne verdi. En dollar er ikke bare en dollarseddel, men også en dollars verdi i andre former som for eksempel bankinnskudd. I tillegg gjelder dette for goder og tjenester med en markedsverdi målt i dollar (Doepke og Schneider 2013).

I de norske lover, herunder Lov om Norges Bank og pengevesenet mv., også kjent som Sentralbankloven, er den norske myntenheten og dens egenskaper definert. Vi gjengir derfor hvordan Norge definerer en unit of account.

§4.Pengeenheten og dens internasjonale verdi
Den norske pengeenhet er en krone. Kronen deles i hundre øre.
Kongen treffer vedtak om den kursordning som skal gjelde for kronen og om endringer i kronens kursleie.
Vedtak om endringer i kursordningen for kronen og i dens kursleie skal meddeles Stortinget (Lovdata 2011).

§13.Pengesedler og mynter
Banken har enerett til å utstede norske pengesedler og mynter.
Banken treffer bestemmelse om sedlenes og myntenes pålydende og utforming.
Banken kan bestemme at andre kan produsere pengesedler og mynter etter avtale med banken (Lovdata 2011).

§14.Tvungent betalingsmiddel
Bankens sedler og mynter er tvungent betalingsmiddel i Norge. Ingen er pliktig til i én betaling å ta imot mer enn tjuefem mynter av hver enhet.
Sterkt skadde sedler og mynter er ikke tvungent betalingsmiddel.
Banken gir nærmere forskrifter om erstatning for bortkomne, brente eller skadde sedler og mynter.

Selv om en avtale inneholder klausul om betaling av en pengeforpliktelse i gullverdi, kan skyldneren frigjøre seg med tvungne betalingsmidler uten hensyn til denne klausul (Lovdata 2011).

Kronen er juridisk lovfestet i Norge, og er et tvungent betalingsmiddel. Dette vil si at man må akseptere kronen som betalingsmiddel av gjeld her i landet. Skatteetaten har uttalt at penger ofte defineres som alminnelig godtatt eller gyldig betalingsmiddel, og de skal også ha funksjon som verdimål og verdioppbevaringsmiddel (Heggstad 2014).

2.5.2 Sentralbankens oppgaver i forhold til valuta

Et viktig moment i forhold til senere analyser og drøfting er hvordan en valuta påvirkes av sentralbanken. Vi oppsummerer derfor Norges Bank sine plikter og oppgaver som sentralbank her.

Pengepolitikken skal bidra til stabilitet i den norske krones nasjonale og internasjonale verdi, og det er derfor viktig at det er forutsigbarhet knyttet til valutakursutviklingen (Opstad 2012). Pengepolitikken skal samtidig understøtte finanspolitikken ved å bidra til og stabilisere utviklingen i produksjonen og sysselsettingen. Norges Bank sin operative gjennomføring av pengepolitikken skal rettes mot lav og stabil inflasjon. Det operative målet for pengepolitikken skal være en årsvekst i konsumprisene som over tid er nær 2,5%. Det skal i utgangspunktet ikke tas hensyn til direkte effekter på konsumpriser som skyldes endringer i rentenivå, skatter, avgifter og særskilte midlertidige forstyrrelser. Med andre ord er sentralbankens oppgaver å styre pengemengden ved rentesetting og trykking av penger.

2.6 Råvare

En råvare er uniform i kvalitet mellom bedrifter som produserer og selger det (McDonald 2013). Råvarer er homogene varer ettersom man ikke kan se forskjell på dem ut fra hvem det er som har produsert dem. Som regel produseres og selges de av mange ulike bedrifter. I tillegg innehar råvarer fysiske egenskaper, eksempelvis som input i produksjon av varer og tjenester.

2.7 Ponzi-svindel

En Ponzi-svindel er en investeringssvindel som involverer utbetaling av påstått avkastning til eksisterende investorer med innskudd fra nye investorer (U.S. Securities and Exchange Commission 2014). Ponzi-svindler lokker nye investorer med høy avkastning i forhold til de påkrevde investeringene.

Ofte kjennetegnes slike svindler ved:

- Høy avkastning med liten risiko.
- Konsistent avkastning.
- Uregistrerte investeringer.
- Ulisensierte selgere.
- Hemmelighetsfulle og/eller komplekse strategier.
- Problemer med papirarbeid.
- Vanskelig å motta betalinger.

2.8 Elektronisk betalingssystem

Dette er et system som viker fra det tradisjonelle betalingssystemet i butikk hvor man kan ta, se og vurdere varen før man betaler for den med kontanter, sjekk eller betalingskort (Organisation for Economic Co-operation and Development 2006). Et elektronisk betalingssystem skjer i sin helhet over nettet, og baserer seg i større grad på tillit enn tradisjonelle løsninger. Årsaken er at man ikke får med seg den kjøpte varen med en gang betalingen er foretatt.

Betalingssystemer tilbys av tradisjonelle markedsdeltakere, banker og kredittkortselskaper, telekommunikasjonsselskaper og nye finansielle tjenesteleverandører. Store banker er i tillegg til selskapene Visa og MasterCard hovedleverandørene av elektroniske betalingssystemer.

3. Teori

I dette kapittelet presenteres litteratur som er relevant for å besvare problemstillingen. Vi ser i hovedsak på ulike definisjoner og teorier knyttet til aktivabobler.

3.1 Bobleteori

Det eksisterer ulike oppfatninger av hvordan bobler bør defineres. Shiller definerte en aktivaboble som en situasjon der midlertidig høy pris skyldes stor entusiasme blant investorer fremfor konsistente estimater av realverdi (Shiller 2005). Det vil dermed oppstå et avvik mellom fundamental verdi og markedsverdien til aktivumet på grunn av spekulativ atferd. Den fundamentale verdien forklares som forventet nåverdi av all fremtidig avkastning.

Stiglitz definerer en boble på følgende måte:
Hvis høy pris i dag utelukkende skyldes at investorer tror salgsprisen vil være høy også i morgen - når fundamentale faktorer ikke rettferdiggjør en slik pris - eksisterer det en boble (Stiglitz 1990).

Kindleberger sin definisjon lyder som følger:
Prisen på en eiendel stiger i en takt som er høyere enn det som kan forklares ut fra fundamentale faktorer i markedet (Kindleberger og Aliber 2011).

Bobleteori deles gjerne inn i rasjonelle og irrasjonelle bobler (Steigum 2006). Teori om rasjonelle bobler bygger på klassisk finansteori. Dette bygger på forutsetninger om rasjonell atferd, rasjonelle forventninger og symmetrisk informasjon mellom aktørene. Dersom disse forutsetningene er oppfylte, skal aktivumets fundamentale verdi tilsvare markedsverdien. Tanken er at alle avvik fra den fundamentale verdien skal forklares som brudd på rasjonalitetsforutsetningene. Blanchard og Watson er uenige i dette, og mener at det kan oppstå rasjonelle avvik mellom fundamental verdi og markedspris.

3.1.1 Rasjonell bobleteori

Vi benytter Blanchard og Watson sin forklaring av rasjonalitet innen bobleteori (Blanchard og Watson 1982). Rasjonelle forventninger og atferd skal sammen med likevektspriser implisere at aktørens aktivaposisjon er frivillig valgt. Aktøren kan derfor ikke øke sin forventede nytte ved å endre porteføljen sin, gitt aktørens private informasjon og informasjonen som

synliggjøres gjennom markedsprisen. En viktig forutsetning er at alle aktører har lik informasjon etter å ha observert prisen, det vil si perfekt informasjonssymmetri mellom aktørene. Dette gjør at vi kan formulere betingelsen for arbitrasjefrihet. Dersom:

$$R_t = \frac{P_{t+1} - P_t + x_t}{P_t}$$

så må

$$E(R_t|\Omega_t) = r$$

$$E(P_{t+1}|\Omega_t) - P_t + x_t = rP_t$$

P_t er prisen på aktivumet og x_t er aktivumets avkastning. Dermed blir R_t avkastningsraten på tid t. Ω_t er angitt som informasjon på tidspunkt t, og forventes å være lik blant aktørene i markedet. Betingelsen viser at den forventede avkastningsraten er lik avkastningssatsen på eiendelen r.

I et slikt marked kan en rasjonell boble oppstå dersom investorer er villige til å betale mer enn den observerbare fundamentale verdien tilsier. En slik situasjon kan oppstå dersom forventningen om fremtidig prisvekst for eiendelen overstiger investorenes avkastningskrav (Lansing 2007). For at en rasjonell boble skal bestå, er det en nødvendig betingelse at prisen på aktivumet øker mer enn avkastningen til evig tid. Videre er det nødvendig med et uendelig antall deltakere i markedet, ellers vil man gå tom for rasjonelle investorer som er villige til å kjøpe til markedspris og selge senere til en høyere pris. Dette knytter seg til tanken om "greater fool theory" (Kindleberger og Aliber 2011). Noen kjøpere vil gå til anskaffelse av risikable aktiva selv om de vet at det eksisterer en aktivaboble. Formålet vil være å likvidere posisjonen før boblen sprekker, og profittere på at det vil være "en større idiot" som står klar til å investere.

Dersom forutsetningen om informasjonssymmetri mellom aktørene ikke holder, vil ikke aktørene ha samme oppfatning av aktivumets fundamentale verdi. I slike tilfeller vil det oppstå individuelle bobler basert på hvordan hver enkelt aktør tolker informasjonen som synliggjøres i markedet (Blanchard og Watson 1982). Dette løses gjennom forutsetningen om at den gjennomsnittlige rasjonelle forventningen blant investorene må være korrekt.

Werner De Bondt peker på spesielt to områder der det tradisjonelle rasjonalitetsparadigmet ikke byr på tilstrekkelig gode forklaringer (De Bondt 2002). For det første er prediksjonene av markedsutviklingen ikke i overensstemmelse med det man observerer i praksis. I tillegg er det svært sjelden at alle forutsetningene for rasjonalitet er oppfylt. De Bondt eksemplifiserer dette gjennom å vise til at det er mer enn de personlige faktorene som spiller inn på beslutningstaking. Dette omhandler blant annet at ulike fremstillinger av samme problemstilling vil kunne føre til forskjellige valg. Mennesker klarer ikke å ta rasjonelle beslutninger i situasjoner med usikkerhet, selv om man har informasjon om sannsynligheten knyttet til ulike utfall. Rasjonalitetsparadigmet stemmer dermed ikke overens med hvordan beslutningstaking foregår i virkeligheten.

3.1.2 Irrasjonell bobleteori

Hovedskillet mellom de to typene bobleteori ligger i hvordan teoriene behandler rasjonalitetsaspektet. Irrasjonell bobleteori bygger på atferdsfinans som omhandler studier av finansiell beslutningstaking gjennom å benytte emner innenfor psykologien (De Bondt 2002). Her legger man til grunn at mennesker er begrenset rasjonelle. Dette betyr at menneskets rasjonalitet preges av begrenset informasjon og tid, samt at det er en begrensning i hvor mange utfall hjernen er i stand til å vurdere (Herbert 1978).

Begrenset rasjonalitet legger grunnlaget for Shiller sin definisjon av spekulative aktivabobler (Lansing 2007). Som vi nevnte tidligere, dreier det seg om situasjoner der aktiva med stigende priser tiltrekker seg nye investorer, og de oppmuntres til å tro på fortsatt prisvekst (Shiller 2005). Det oppstår dermed en tilbakemeldingsprosess hvor eksisterende investorer, som profitterer på prisøkningen i aktivumet, lokker flere mennesker til å investere. Dette fører til en situasjon der stadig flere investorer kjøper seg inn og som en konsekvens av det vil prisen stige. Dette kan vi kalle en irrasjonell begeistring ettersom investeringsviljen oppstår som følge av ønsketenkning fremfor reelle verdivurderinger (Shiller 2005).

Videre forteller Shiller om hvordan det i markedet foregår flokkatferd blant individene (Shiller 2005). Dette oppstår på grunn av såkalte informasjonskaskader. Disse kaskadene blir forklart som bølger av irrasjonell atferd (Secher 2013). Individer vil gjennom observasjon av andre påvirkes til å ta irrasjonelle kollektive valg, selv om enkeltindividet selv tror det handler

rasjonelt. Dette kan knyttes til oppbyggingen av en boble ettersom det kan oppstå en kollektiv feilvurdering av den fundamentale verdien.

3.1.3 Kindleberger om bobler

Det finnes i følge Kindleberger tre ulike typer spekulative bobler. Den første typen er den som går igjen mest i teoretisk litteratur på området (Kindleberger og Aliber 2011). I dette mønsteret øker prisene med en akselererende rate, for så å synke kjapt tilbake til antatt fundamentalt nivå etter å ha nådd sin høyde. Det generelle argumentet for spekulative bobler er at de er selvoppfyllende profetier. Prisen stiger fordi agenter forventer at den skal gjøre det, og denne pågående forventningen skaper den stigende etterspørselen som igjen øker prisen. Hvis prisen slutter å stige på grunn av et eksogent sjokk, vil forventningene svekkes, og den spekulative etterspørselen forsvinner. Deretter sendes prisen raskt tilbake til det fundamentale nivået, hvor det ikke er noen forventing om prisstigning. Dette karakteriserer Minsky og Kindleberger ofte som panikk blant agenter.

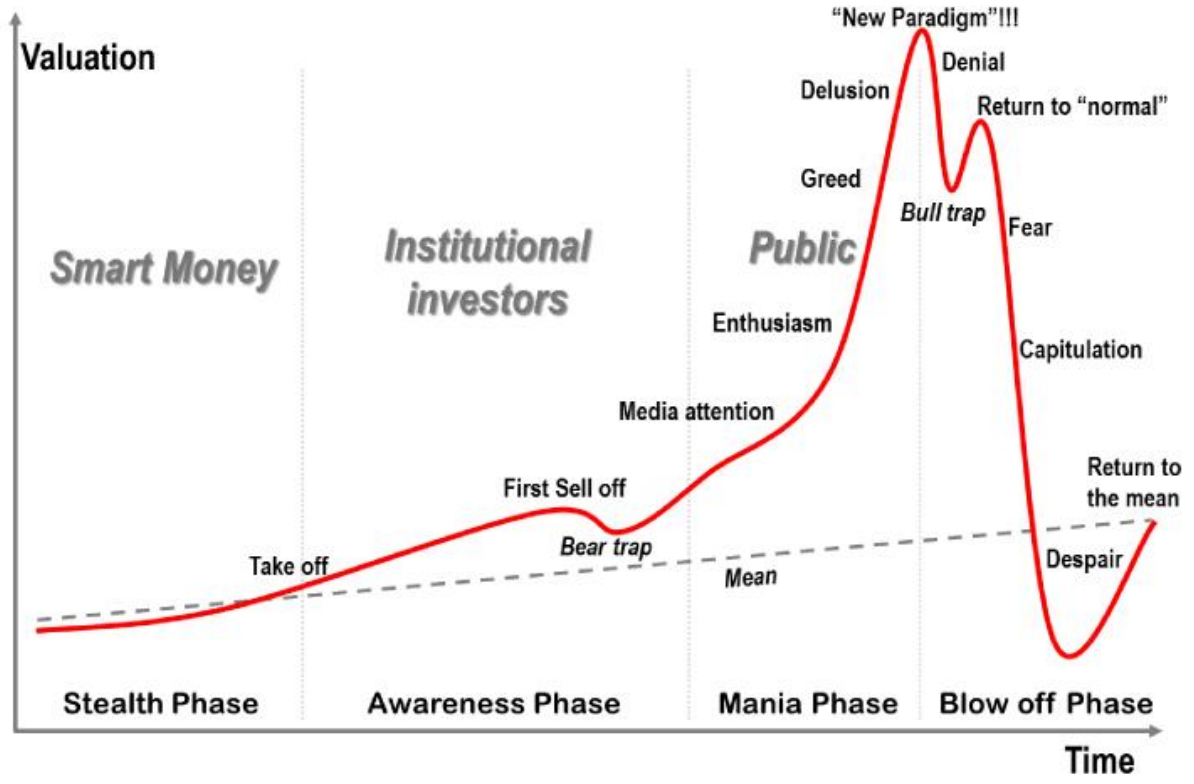
I den andre typen boble øker prisen i en periode frem til den når en topp (Kindleberger og Aliber 2011). Deretter er prisen stabil i dette punktet før den synker igjen, ofte med samme hastighet som i vekstfasen. Det er derfor ingen krasj i vanlig forstand. Denne formen for aktivaboble står i kontrast med andre typer bobler fordi prisen ikke faller raskere enn den steg. I denne typen boble kan mange agenter være utilfreds når prisen synker, men det er ingen generell panikk i markedet. Enkelte argumenterer for at dette egentlig ikke er noen boble, ettersom man forventer at det skal være en dramatisk nedgang i prisen når en boble sprekker. Motargumentet til Kindleberger er at man observerer en pris som er høyere enn fundamental verdi, noe som er et sentralt kjennetegn ved aktivabobler.

Den tredje typen boble er den som oppstår i perioder med generelle økonomiske vanskeligheter, en type først identifisert og merket av Minsky i 1972 (Kindleberger og Aliber 2011). Her øker prisen til en topp som etterfølges av en gradvis nedgang i en periode. Til slutt oppstår det panikk, og boblen sprekker. I følge Kindleberger er det den mest vanlige fasongen en boble inntar, noe som bekreftes av de største og mest berømte boblene i historien. Dette inkluderer Mississippi-boblen i 1719, Sørhav-boblen i 1720 og boblene i det amerikanske aksjemarkedet i 1929 og 1987 (Rosser, Rosser, og Gallegati 2012). Dette er den vanligste formen for aktivaboble, men det er også den som det er produsert minst forskning på. Man

forutsetter heterogen oppførsel blant agentene. Noen av aktørene er insidere som likviderer aktivumet på topp, mens resten holder posisjonen helt frem til perioden med finansiell uro og krasj. Den finansielle uroen kjennetegnes ved at noen aktører ikke klarer å møte sine forpliktelser. Her kan det trekkes linjer mot subprime lånene i USA hvor det oppstod en nedgang i markedet da låntagerne ikke klarte å betale sine forpliktelser til banken.

3.1.4 Rodrigues bobleteori

Denne modellen ble presentert av Jean-Paul Rodrigue ved Hofstra University. Den fikk en del oppmerksomhet under og i etterkant av den siste finansielle krisen i 2008. Dette er ikke hentet fra en publisert økonomisk artikkel, og har dermed ikke den samme akademiske tyngden som enkelte andre teorier. Allikevel har modellen vist seg å være en god forklaringsfaktor i ulike kriser. Her deles en boble opp i fire faser; lite synlig, bevissthet, mani og avblåsing (Rodrigue 2013).



Figur 4: Utviklingen i en aktivaboble (Rodrigue 2013)

Lite synlig

Beskrives som fasen hvor et fåtall aktører investerer i markeder og segmenter som andre enda ikke har oppdaget. Informasjonen er gjerne begrenset til spesielle nettverk.

Bevissthet

Fasen hvor andre investorer merker seg utviklingen, og de foretar derfor investeringer. Dette driver prisene videre oppover. Etter hvert henter noen av de første investorene ut sine gevinster, noe som fører prisene litt nedover igjen.

Mani

Her kommer media inn og gjør allmennheten oppmerksom på saken. Dette bidrar til en rekke investeringer, og som en følge av det drives prisen raskt oppover. I denne situasjonen trekker de første smarte investorene seg sakte tilbake og selger seg ut.

Avblåsning

En utløsende faktor gjør at panikken sakte begynner å spre seg blant investorene. Prisen faller og fornektelsen inntreffer, og man prøver å overbevise investorene om at dette er en forbigående fase. Mange ønsker å selge, og tilbudet blir mye større enn etterspørselen. Dermed begynner prisene å falle dramatisk. De som sitter igjen med aktivumet, er ofte de som kom sist inn.

3.2 Fundamental verdi

Den fundamentale verdien kan beskrives som verdien man tillegger et aktivum. Dette er basert på fundamentale faktorer som kontantstrøm, forventet vekst og risiko (Damodaran 2011b). For kontantstrømgenererende eiendeler kan verdien beregnes som en funksjon av neddiskonterte kontantstrømmer og sannsynligheten for at disse inntreffer. I slike modeller tar man hensyn til risikoen gjennom å justere enten avkastningskravet eller kontantstrømmene.

Eiendeler som ikke har noen kontantstrømgenererende effekt har i følge Damodaran ingen fundamental verdi (Damodaran 2011a). Ved verdsettelse av slike eiendeler er det naturlig å benytte metoder for relativ verdsetting. Dette baserer seg på å finne lignende eller identiske eiendeler i markedet, og benytte dette som utgangspunkt for verdiberegningen. Man forsøker med det å avdekke konsumentenes betalingsvillighet for produktet.

3.3 Elastisitet og tilbud

Elastisitet angir endringen i tilbudsmengde som følge av en gitt prisendring (Varian 2010). Hvis et gode har tilbudselastisitet større enn 1 i absoluttverdi, sier vi at det har et elastisk tilbud. Hvis elastisiteten er mindre enn 1 i absoluttverdi, sier vi at det har et uelastisk tilbud. Og hvis elastisiteten er akkurat 1, har den et nøytralelastisk tilbud. I en elastisk tilbudskurve er mengden følsom til prisendringer. Hvis prisen øker med 1 %, synker tilbudt mengde med mer enn 1%.

$$Tilbudselastisitet = \frac{Relativ\ endring\ i\ tilbudsmengde}{Relativ\ prisendring}$$

3.4 Shillers indikatorliste

Shiller har utarbeidet en sjekkliste for bobler (Ewing 2010). Dersom alle punktene på listen er tilstrekkelig oppfylte for et aktivum, kan det være en indikasjon på at det eksisterer en aktivaboble:

- Rask økning i prisen til eiendelen, som under eiendoms- eller dot com-boblen.
- Stor offentlig begeistring om en slik økning.
- Et medfølgende medievanvidd.
- Historier om personer som tjener masse penger, noe som skaper misunnelse blant dem som ikke gjør det.
- Økende interesse rundt eiendelsklassen hos mannen i gata.
- Teori om en ny æra oppstår for å kunne rettferdiggjøre enestående prisøkninger.
- En nedgang i utlånsstandarder.

4. Metode

I denne delen av oppgaven ønsker vi å fremlegge våre perspektiver og hvilke modeller vi har benyttet for å finne en konklusjon på vår problemstilling.

4.1 Undersøkelsesopplegg

Vi skal her se nærmere på hvordan vi går frem for å svare på problemstillingen. Det er viktig at vår tilnærmingsmåte er riktig og opprettholder de standarder vi er vant til å se i akademisk arbeid. Vi har valgt positivistisk tilnærming med kvantitative undersøkelser.

4.1.1 Forskningsdesign

Et forskningsdesign er en oversikt over hvordan forskningen skal foregå. Det omhandler hvordan data samles inn og hva man skal bruke innsamlet data til. I avhandlingen vår har vi et deduktivt design, noe som vil si at vi går fra teori til empiri. Dette kjennetegnes ved et hypotesetestende opplegg. Formålet er å bekrefte eller avkrefte antagelser på områder det finnes mye forhåndskunnskap om (Jacobsen 2010).

4.1.2 Validitet og reliabilitet

Disse to begrepene sier oss noe om kvaliteten til målingene som er gjennomført. Reliabilitetsbegrepet brukes for å si noe om et måleinstruments eller en målemetodes grad av stabilitet og konsistens i målingene (Jacobsen 2010). Det omhandler hvorvidt man får det samme resultatet hver gang man bruker testen. Høy reliabilitet sier derimot ikke noe om vi måler det vi faktisk ønsker å måle, det gjør derimot validitet. Vi mener denne avhandlingen oppfyller kravene til validitet og reliabilitet.

4.1.3 Kilder

For å kunne gjennomføre analyser som kan hjelpe til med å besvare problemstillingen, må vi samle inn data. Det er ønskelig med data fra forskjellige kilder for å sikre objektivitet, reliabilitet og validitet. Det skilles mellom primær- og sekundærdata i forskning. I denne avhandlingen benytter vi sekundærdata. Dette er data som ikke samles inn av forskeren direkte, men det baseres på informasjon som er samlet inn av andre, ofte til andre formål (Jacobsen 2010).

Fallgruver ved å bruke sekundærdata er i følge Jacobsen at man ofte ikke vet hvordan data har blitt samlet inn, hvilke måleapparater og innsamlingsmetoder som er brukt, og hvem som har registrert informasjonen (Jacobsen 2010). Det finnes også ofte problemer knyttet til tall fra ulike tidsperioder der det er viktig å avdekke om registreringsprinsipper har endret seg. Den kanskje viktigste er hvorvidt kilden er pålitelig eller ikke. Dette har vi forsøkt å ta hensyn til etter beste evne, men vi innser at vi kan ha benyttet noen kilder som vanligvis ikke ville oppfylt de krav vi stiller til en avhandling. Bakgrunnen for det er at det er begrenset med akademisk litteratur på området.

4.2 Modeller

I dette underkapittelet presenterer vi modellene vi har benyttet for å beregne volatilitet og korrelasjon. Disse beregningene skal vi senere benytte til å belyse problemstillingen.

4.2.1 Volatilitet

Volatilitet er definert som standardavviket til et aktivums avkastning, og kan belyse hvor mye variasjon man kan forvente. Det er ulike måter å beregne volatilitet på, og vi har valgt å fokusere på den historiske volatiliteten (McDonald 2013). Her benyttes historiske avkastningstall som utgangspunkt i beregningen. Vi har n kontinuerlig forrentede aksjeavkastninger over en periode t. Ved å forutsette at volatiliteten er konstant, kan vi beregne årlig volatilitet i underliggende aktivum. Dette gjøres gjennom en vanlig beregning av standardavviket σ_H for et utvalg.

Gitt at:

$$\epsilon_{t+h} = \ln(\frac{S_{t+h}}{S_t})$$

så beregnes årlig volatilitet ved:

$$\sigma_H = \sqrt{\frac{1}{h}\left[\frac{1}{(n-1)}\sum_{i=1}^{n}\epsilon_i^2\right]}$$

Daglig volatilitet blir beregnet dersom $\frac{1}{h}$ fjernes fra formelen.

Et alternativ til den klassiske beregningen av volatilitet er modellen for høy-lav historisk volatilitet (Garman og Klass 1980). Her benyttes tall på høyeste, laveste, åpnings- og sluttkurs

i løpet av dagen. Formålet med dette er å oppnå et mer korrekt estimat på volatiliteten ved å inkludere flere parametre.

$$\hat{\sigma} = \sqrt{0{,}511 \times (u-d)^2 - 0{,}019 \times [c \times (u+d) - 2 \times ud] - 0{,}383 \times c^2}$$

der $u = \ln(\frac{Kurs\ høy}{Kurs\ åpning})$, $d = \ln(\frac{Kurs\ lav}{Kurs\ åpning})$, $c = (\frac{Kurs\ stenging}{Kurs\ åpning})$

0,511, 0,019 og 0,383 er konstanter i formelen. I følge Garman og Klass skal disse vektene gi den beste analytiske skala-uavhengige estimatoren (Garman og Klass 1980). Det betyr at estimatoren er variansminimerende og at avviket mellom forventet og sann verdi er 0.
Et problem ved å benytte disse to modellene er at historiske tall ikke nødvendigvis er gode prognoser på perioden fremover. Vi anser ikke dette som noe problem ettersom formålet med beregningene er å sammenligne den historiske volatiliteten til ulike aktiva.

4.2.2 Korrelasjon

Når vi snakker om korrelasjon, snakker vi om samvariasjon mellom to eller flere variabler i et utvalg (Studenmund 2011). Vi skiller mellom positiv og negativ korrelasjon. Positiv korrelasjon vil si at en økning i den ene variabelen samsvarer med en økning i den andre. Negativ korrelasjon vil si at en økning i den ene variabelen samsvarer med en nedgang i den andre.

$$r_{12} = \frac{\sum[(X_{1i} - \overline{X_1})(X_{2i} - \overline{X_2})]}{\sqrt{\sum(X_{1i} - \overline{X_1})^2} \times \sum(X_{2i} - \overline{X_2})^2} = \frac{CoV(X_1, X_2)}{Var(X_1) \times Var(X_2)}$$

5. Data

I dette kapittelet ønsker vi å redegjøre for dataen som er innhentet for å kunne gjennomføre de kvantitative analysene.

Som nevnt tidligere benytter vi sekundærkilder i oppgaven. Vi har innhentet ulike data knyttet til bitcoin fra Bitcoincharts, Quandl og Blockchain. Her har vi benyttet ferdige datasett, men i enkelte tilfeller har vi foretatt logaritmiske transformasjoner. Data for bitcoinkursen gjelder for børsen Bitstamp, som er den største aktøren i markedet etter at MtGox ble nedlagt.

Videre har vi hentet data fra Google Trends. Vi mener at utviklingen i antall søk på Google vil være en god indikasjon på hvor mye oppmerksomhet bitcoin har fått i media. Datasettet bygger på en realjustering av antall oppslag i søkemotoren Google. Det høyeste punktet i perioden velges som basispunkt, gis verdien 100, og resten av målingene settes opp mot dette punktet. Dette gjør det mulig å vise sammenhengen mellom utviklingen i bitcoin og Google Trends.

Fra Datastream har vi hentet aksjekurser og indekser fra tidligere aktivabobler. Aksjekursene og software-indeksene vi har benyttet, gjelder for perioden rundt dotcom-boblen ved årtusenskiftet. I tillegg har vi sett på verdier for Dow Jones Industrial Indeks fra børskrakket i 1987. Til sist er valutakursen EUR/USD tatt med for å sammenligne volatiliteten opp mot bitcoin. Disse dataene bidrar i diskusjonen om hva man skal karakterisere bitcoin som. Mange sammenligner bitcoin med dotcom-boblen fordi det tilsynelatende er et stort sprik mellom markedspris og hva de fundamentale faktorene tilsier.

Grunnet bitcoin sin korte levetid erkjenner vi at datagrunnlaget kan være litt for lite. Allikevel mener vi at det kan gi oss gode indikasjoner på hvorvidt bitcoin er en boble eller ikke.

6. Analyse

I dette kapittelet presenterer vi våre funn og ser de opp mot relevant fremlagt teori. Første del er en strategisk analyse mens i andre del analyserer vi våre funn i lys av bobleteori.

6.1 Strategisk analyse

Videre ser vi på særegne karakteristikker ved bitcoin i form av styrker og svakheter. I tillegg går vi i dybden på hvordan det eksterne rammeverket kan påvirke den videre utviklingen.

6.1.1 Styrker ved bitcoin

Lave transaksjonskostnader

Den mest synlige fordelen ved å benytte bitcoin som betalingsmetode er reduserte transaksjonskostnader. Dette er mulig ettersom det ikke er noen finansiell institusjon som står bak. Aktører kan dermed unngå de tradisjonelle avgiftene knyttet til elektronisk betaling og verifisering. Det er i praksis tilnærmet kostnadsfri handel, og kan være spesielt interessant for mindre bedrifter å tilby kunder og betale i bitcoin. Fordelen med bitcoin er at alle aktører i markedet vil ha samme betingelser uavhengig av omsetningsvolum. Det finnes ingen stordriftsfordeler som påvirker transaksjonskostnader i bitcoin.

Et problem ved dette er at transaksjonskostnadene i fremtiden skal utgjøre incentivet for å være tilkoblet nettverket. I dag er det som kjent nyutvinningen av mynter som har denne funksjonen. Dermed må transaksjonskostnadene på et tidspunkt øke, og fordelen ved lave transaksjonskostnader vil på det tidspunktet reduseres.

Selskaper tilbyr sikring mot volatilitet

Høy volatilitet kan være en årsak til at mange bedrifter ikke ønsker å tilby handel av varer og tjenester med bitcoin som betalingsmiddel. Selskaper som Bitpay og Coinbase tilbyr bedrifter å unngå denne risikoen, og som regel gjøres dette mot en transaksjonsavgift. Avgiften ligger typisk på 1 % (Bitpay 2014; Coinbase 2014). Aktører kan dermed i praksis oppnå en total transaksjonskostnad på cirka 1 %. Muligheten til å benytte slike mellomledd kan redusere inngangsbarrierene for nye aktører i markedet.

Overføre penger på tvers av landegrenser

En annen stor fordel med bitcoin er muligheten arbeidsinnvandrere har til å sende penger tilbake til hjemlandet. I første kvartal 2014 var gjennomsnittlig kostnad for pengeoverføringer fra arbeidsinnvandrere til hjemlandet på 8,36 % (World Bank 2014). Dette er et marked som er estimert til å utgjøre over 410 milliarder dollar i 2013 (World Bank 2013). I tillegg til å være kostbart kan det også ta flere dager å gjennomføre slike transaksjoner (Western Union 2013).

Vanskelig kontrollerbart for myndigheter

Det er umulig for myndighetsorganer å stanse overføringer av bitcoin. I land med strenge bestemmelser knyttet til overføring av kapital kan bitcoin være nyttig. Muligheten til å unngå slike reguleringer kan være interessant for mange. Dette så vi eksempelvis i 2013 da myndighetene på Kypros begynte å diskutere hvorvidt de skulle benytte innbyggernes sparepenger i bailouten av EU og IMF (Farrell 2013). Som en følge av dette steg prisen på bitcoin med 87 % på mindre enn to uker. Det bør nevnes at regulerende myndigheter kan identifisere aktører i ettertid, men de har ingen mulighet til å stanse transaksjoner. Med tradisjonelle betalingsløsninger som Visa og Mastercard vil myndighetene kunne legge press på nevnte aktører slik at transaksjoner blir stoppet i forkant.

Mikrotransaksjoner

På grunn av lave transaksjonskostnader er det mulig å benytte betalingsløsninger som bygger på mikrotransaksjoner. Dette gjelder blant annet tjenester hvor man betaler etter bruk, som for eksempel ved at internettleverandører måler og tar betalt etter forbruk fremfor faste satser (Brito 2013a).

Sikkerhet

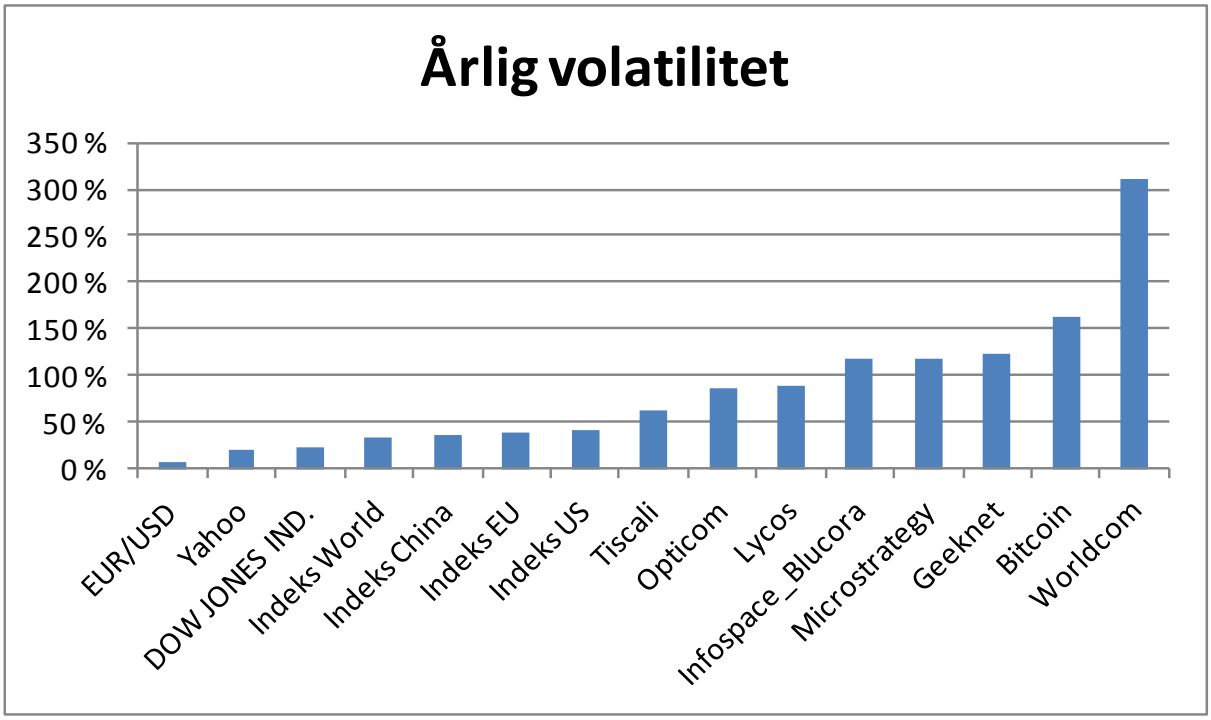
I henhold til kalkulasjonene til Satoshi Nakamoto er det nå under 0,1% sannsynlighet for at en uærlig bruker kan ta over hele kjeden hvis han har 45% sannsynlighet for å finne neste blokk. Dette vil si at selve kjernen til bitcoin er meget vanskelig å gjøre noe med sikkerhetsmessig.

6.1.2 Svakheter ved bitcoin

Høy volatilitet

Som vist i vedlegg 2 har bitcoin hatt en årlig volatilitet på drøyt 162 %. Dette vil ha en avskrekkende effekt hos mange når alternativet er å benytte tradisjonelle valutaer. Her viste vi at EUR/USD har en årlig volatilitet på cirka 8 %. Da er det rimelig å anta at svært få vil benytte bitcoin som lagringsplass for verdi fremfor andre valutaer i nåværende tilstand. Volatiliteten vil i mange tilfeller ha mindre betydning i situasjoner der bitcoin benyttes som betalingsmiddel (Brito 2013b). Dette fordi de fleste selskapene oppgir sine priser i dollar, for deretter å konvertere til bitcoin i salgsøyeblikket.

Figur 5 viser beregnet historisk volatilitet til en rekke aktiva. Vi har valgt ut valutakursen EUR/USD for å vise hvilken volatilitet etablerte valutaer har. Videre har vi sett på ulike aksjer som både overlevde og gikk konkurs under dotcom-boblen. Til sist har vi beregnet volatiliteten til Dow Jones Industrial Indeks i tilknytning til Black Monday i 1987 og ulike softwareindekser fra dotcom-boblen.



Figur 5: Årlig volatilitet hos utvalgte aktiva (Quandl 2014; Datastream 2014)

Sikkerhetsbrister hos ulike markedsaktører

Det er viktig å ha på plass gode sikkerhetsrutiner for selskaper som benytter bitcoin. Dersom man mister sine personlige nøkler, er det ingen måte å få dem tilbake på (Bitcoin.org 2014). Det har vært flere eksempler på at store aktører i markedet har vært gjenstand for datainnbrudd (Hern 2014). Det største tilfellet var nedleggelsen av børsen MtGox. Her ble det avdekket at omtrent 850 000 mynter var borte. Det tilsvarte om lag 7 % av den totale pengemengden i markedet. Av disse er 200 000 funnet i ettertid (BBC 2014b).

Det essensielle er at det aldri har blitt funnet sikkerhetshull i kildekoden. Flere av verdens beste hackere har forsøkt å finne svakheter i systemet. Ingen av dem klarte å få til dette (Cutler 2013). Problemet omhandler derfor hvordan tredjepartsleverandører løser utfordringene knyttet til sikkerhet. Det har spesielt vært problemer i forhold til varme lommebøker.

Godt egnet for kriminelle forhold

Mange anser bitcoin for å være de kriminelles valuta (Mihm 2013). En grunn til dette kan være at man har muligheten til å gjennomføre transaksjoner som ikke er sporbare direkte tilbake til person. I prinsippet er det dermed tilnærmet å finne ut hvem det er som har overført bitcoin til hverandre. Dette har amerikanske myndigheter tatt hensyn til ved å innlemme børsene i det nasjonale lovverket for anti-hvitvasking (Lee 2013).

6.1.3 Porters fem krefter

Porters fem bransjekrefter benyttes til å vurdere hvor attraktivt et marked er ved å se på kjøpernes, distributørenes og leverandørenes forhandlingsstyrke, trusselen knyttet til nyetableringer og substitutter, samt konkurranseintensiteten i markedet (Johnson, Whittington, og Scholes 2011). Vi har valgt å se på bitcoin i markedet for kryptografisk valuta.

Trussel knyttet til nyetableringer

Kryptografisk valuta er en forholdsvis ny oppfinnelse, og bitcoin ble laget som en kritikk til sentrale styringsmakter etter krisen i 2008 (Feuer 2013). Den 1. april 2014 var det 222 ulike varianter fordelt på 680 markeder (Coinmarketcap 2014). Man kan med trygghet si at det eksisterer en trussel knyttet til nyetableringer. Ingen av aktørene i markedet kan måle seg med

bitcoin i så stor grad at de utgjør en trussel. Oppmerksomheten er i all hovedsak rettet mot bitcoin, spesielt i det offentlige mediebildet. Vi mener det er lite trolig at det vil være noen stor trussel knyttet til nyetableringer i nær fremtid på grunn av bitcoin sitt sterke omdømme.

Forbrukerens forhandlingsstyrke

Bitcoin vil ikke opphøre selv om forbrukerne slutter å bruke dem, fordi det ikke er noen kostnad ved at programvaren eksisterer. For at den skal holde seg i verdi, er man avhengig av at det utføres handel med den. Ettersom det er handel direkte mellom brukerne, er det ikke noen som har kontroll over hva én bitcoin skal koste. Prisen er derfor i stor grad markedsstyrt.

Leverandørenes forhandlingsstyrke

Leverandørene er utvinnerne som tilfører nye mynter til markedet. Som vi har sett tidligere i bakgrunnskapittelet, er de fleste utvinnerne organisert i større grupper. De tre største aktørene står for over 50% av utvinningen, se figur 3. Samlet sett vil disse ha høy grad av forhandlingsmakt siden de sitter på den største delen av ressursene som trengs for utvinne. Det er grunnlag for å anta at aktørene er profittmaksimerende og vil derfor ta markedsandelene til den som eventuelt trekker seg. Isolert sett er den individuelle forhandlingsstyrken blant leverandørene derfor lav.

Distributørenes forhandlingsstyrke

Distributørene i markedet er de forskjellige børsene som tilbyr handel i bitcoin på internett. De forenkler prosessen mellom kjøper og selger ved å la disse komme i kontakt med hverandre mot en kommisjon. Børsene vil derfor kunne sees på som en driver for høyere pris. Prisen ville ikke blitt opprettholdt på samme nivå uten børsene ettersom antall transaksjoner ville blitt redusert.

Trusler knyttet til substitutter

Et av formålene ved kryptografisk valuta er å være et substitutt til monetær valuta. Hvis man tar utgangspunkt i dette, vil monetær valuta også være substitutt til bitcoin. Som vi har nevnt tidligere, kan alt være penger. Det som tilegner en gjenstand verdi, er hva man er villig til å bytte for det, og penger trenger derfor ikke å gjenspeile sin fundamentale verdi (Friedman 1992). Det at aktører er villige til å holde penger som tegn på en ufullstendig byttehandel, gjør det til en lagringsplass for verdi.

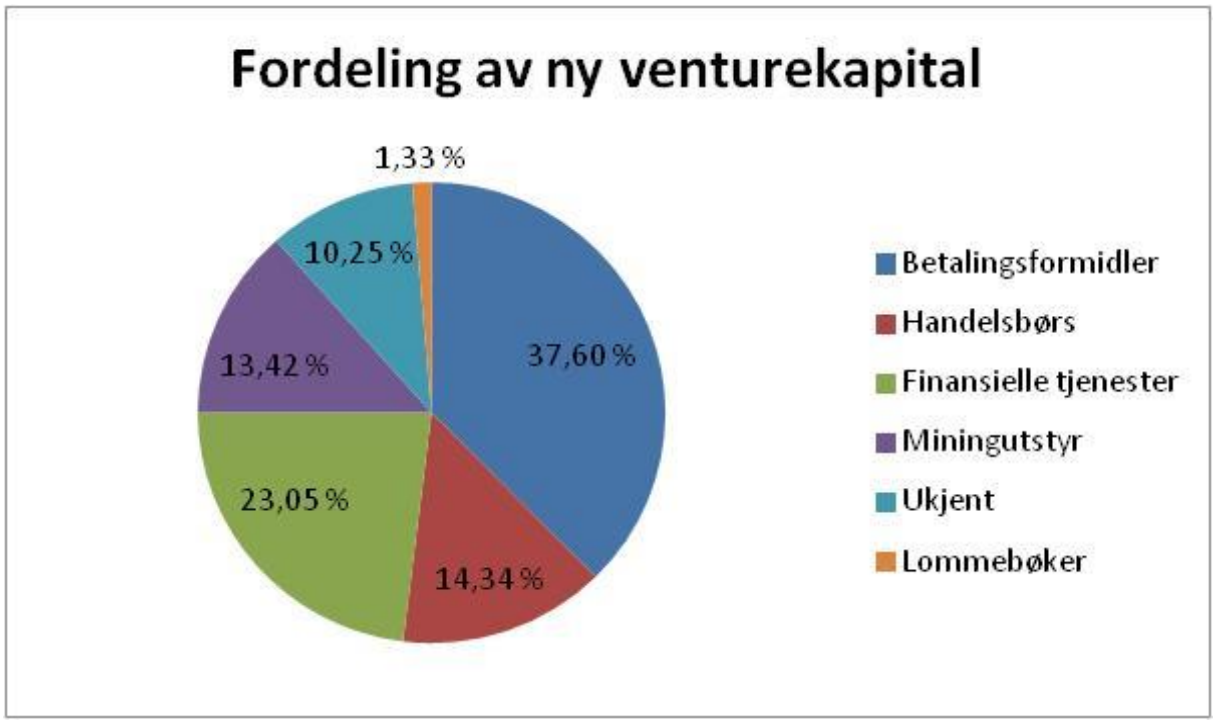
Bitcoin oppfyller så langt de forholdsvis løse kravene til Friedman om hva som må til for at det skal kunne kalles penger. Så lenge noen ser på det som en verdi og er villig til å utføre byttehandler med det, er det penger. Dette gjelder i økende grad for bitcoin ettersom det er stadig flere som er villige til å akseptere det i byttehandler. Dermed kan man si at det har en lagringsplass for verdi.

Skatteetaten i USA definerer en virtuell valuta som en representasjon av verdi som fungerer som et byttemiddel, en unit of account, og/eller lagringsplass for verdi (Internal Revenue Service 2014a). Bitcoin oppfyller kravene til Friedman ved at det fungerer som et byttemiddel og lagringsplass for verdi. Problemet under definisjonen til skatteetaten i USA er hvorvidt bitcoin kan kategoriseres som unit of account. Tanken er her at eksempelvis den norske kronen er et måltall for mer enn selve myntene og sedlene. Tall i regnskap og tall på kontoer er norske kroner og har verdi selv om det ikke er fysiske mynter og sedler. Bitcoin kan dermed ikke sies å være en unit of account. Enheten måles som regel i dollar, og har ikke opparbeidet seg den status eller sikkerhet til eksempelvis å kunne sammenlignes med norsk krone eller annen valuta. Den sammenlignes derfor med norske kroner gjennom amerikanske dollar.

Som det fremgår av norsk lov er kronen en lovfestet valuta og et tvungent betalingsmiddel. Det er kun Norges Bank som kan utstede mynter og sedler. Bitcoin er ikke en lovfestet valuta eller tvungent betalingsmiddel. Dette vil si at man på ingen måte må akseptere en betaling i bitcoin for et produkt. Dermed faller det utenfor definisjonen til Skatteetaten som gyldig og allmenn akseptert betalingsmiddel. Truslene knyttet til substitutter er derfor meget sterke.

Komplementører

Dette er andre produsenter som tilbyr varer som kan benyttes sammen med bitcoin og dermed gi økt totalverdi for kundene. Hvis man skal handle med bitcoin, er man avhengig av å ha en lommebok. Det finnes flere forskjellige tilbydere av lommebøker. Andre eksempler på komplementører er Coinbase som samarbeider med Overstock, og tar seg av alle transaksjoner som gjennomføres med bitcoin (Love 2014). Dette gjør det lettere for bedrifter å ta imot bitcoin som betaling. Figur 6 viser fordelingen av venturekapital i markedet.



Figur 6: Fordelingen av ny venturekapital (Coindesk 2014b)

I følge undersøkelser gjort av Coindesk tilsvarer de totale investeringene gjennom ventureselskaper i bitcoinmarkedet cirka $97,5 millioner (Coindesk 2014b). Vi ser fra figuren at store deler av investeringene går direkte til utvikling av komplementører.

Konkurranseintensitet i markedet

Som nevnt finnes det 222 registrerte kryptografiske valutaer, og bitcoin er den desidert største aktøren (Coinmarketcap 2014). For bitcoin er ikke intensiteten særlig sterk, men blant de andre aktørene er konkurranseintensiteten mye sterkere. Markedet har 1.april 2014 en total verdi på cirka 7 milliarder amerikanske dollar (Coinmarketcap 2014). Etter opprettelsen av bitcoin har det kommet flere forskjellige varianter av kryptografisk valuta; ripple, litecoin, peercoin og dogecoin. Felles for dem alle er at de har andre egenskaper enn bitcoin, men ingen av dem har allikevel blitt foretrukket fremfor bitcoin av massene.

Aktivum	Markedsverdi per 1. april 2014 (Tall i USD)
Bitcoin	5 729 473 990
Ripple	802 241 644
Litecoin	311 776 767
Peercoin	39 434 714
Dogecoin	31 080 567

Tabell 2: Markedsverdi for kryptografiske valutaer (Coinmarketcap 2014)

6.1.4 PESTEL

Vi velger å bruke et analyseverktøy som heter PESTEL-analyse. Her analyseres de eksterne faktorene som bedriften har lite kontroll på, men samtidig må forholde seg til (Johnson, Whittington, og Scholes 2011). Dette blir litt spesielt for bitcoin siden den ikke har tilhørighet til et bestemt land, men må forholde seg til alle land i verden.

Politiske og lovmessige

Dette omhandler lover, regler og retningslinjer som utformes og reguleres av myndighetene. Bitcoin er internettbasert, og er dermed tilgjengelig i de fleste land. Ingen land kan derfor kontrollere bitcoin som helhet, men de kan legge føringer for hvordan produktet skal behandles i sine respektive land. I løpet av våren 2014 har de fleste land tatt stilling til hvordan bitcoin skal behandles som produkt. Vi tar for oss de største aktørene; USA, Kina, Japan, Tyskland og Frankrike. I tillegg har vi sett på hva det norske skattedirektoratet har uttalt.

Den amerikanske skatteetaten har kommet med sin uttalelse angående bitcoin. Etaten sier at kryptografisk valuta skal behandles som eiendom i skatteøyemed (Internal Revenue Service 2014b). Kinesiske myndigheter har gitt beskjed til bankene om at de ikke har lov til å handle i eller tilby bitcoin til kundene (Deng 2014). I Japan behandles ikke bitcoin som en valuta, men transaksjoner med bruk av kryptografisk valuta skal beskattes. Heller ikke japanske banker har lov til å tilby bitcoin til sine kunder (BBC 2014a). Det tyske finanstilsynet uttaler at bitcoin blir ansett som en unit of account, og at den derfor kan benyttes til skatte- og handelsformål. Den blir ansett for å være et finansielt instrument, og dersom den skal benyttes av bedrifter, må man innhente godkjennelse fra finanstilsynet (Clinch 2013). Den franske sentralbanken har kritisert bitcoin for å være et spekulativt objekt, men har ikke innført spesifikk lovgivning eller reguleringer mot det (Hill 2014).

I Norge legges det til grunn at bitcoin er et formuesobjekt, og i følge skatteloven er gevinst ved salg av formuesobjekter skattepliktig inntekt. Omsetning av bitcoin klassifiseres som ordinær avgiftspliktig omsetning av elektroniske tjenester. Skattedirektoratets vurdering er at bitcoin ikke kan anses som «gyldige betalingsmidler» (merverdiavgiftsloven § 3-6 d) og derfor heller ikke kan anses som en unntatt «finansiell tjeneste». Bitcoin klassifiseres som «tjeneste» (§ 1-3 bokstav c), nærmere bestemt «elektronisk tjeneste» (§ 1-3 bokstav j). Dermed skal næringsdrivende legge 25% merverdiavgift på sin omsetning av bitcoin

(Skatteetaten 2013). Finanstilsynet i Norge gått ut og advart norske forbrukere mot at man ikke er sikret på noen måte ved eventuelle tap (Finanstilsynet 2013).

De politiske og lovmessige forholdene rundt bitcoin varierer fra land til land. Brukerne har ulike skattemessige og lovmessige reguleringer å forholde seg til, noe som kan gjøre bruken av det mer komplisert.

Økonomiske

Økonomiske eksterne forhold som påvirker bitcoin er makroøkonomiske forhold som rentenivå, valutakurs og hvordan den generelle økonomiske veksten er. Det er ingen reguleringsmyndighet som kan styre bitcoin, men verdens makroøkonomiske utvikling vil påvirke bitcoin. Hvis eksempelvis USD styrker seg, vil forholdet BTC/USD svekke seg, og man får altså mindre BTC per USD. Samtidig vil rentenivået i de forskjellige landene kunne påvirke bitcoin indirekte ettersom en heving av renten vil redusere kjøpekraften til forbrukeren.

Sosiale

Dette omhandler demografiske og kulturelle endringer. Trender spiller en stor rolle for hvordan vi mennesker forbruker. Bitcoin er således i dag trendy. Det ligger en utfordring i å sørge for at produktet følger trendene og samfunnets kulturelle utvikling. På grunn av sin teknologiske tilnærming er det grunnlag for å anta at bitcoin som produkt hovedsakelig retter seg mot yngre folk.

Teknologiske

Dette punktet omhandler teknologiske utviklinger i det eksterne miljøet som kan påvirke markedet. Bitcoin er et helteknologisk produkt som kan tilpasse seg nye utviklinger raskt. Det kan påvirkes av at teknologiske nyvinninger gjør miningen mer kostnadseffektiv og mindre ressurskrevende.

Miljømessige

Punktet omhandler forurensing og energibruk. Som nevnt tidligere har miningen av bitcoin et stort strømforbruk som vokser etter hvert som miningen blir vanskeligere og krever mer av maskinene som skal utføre den. Dette har vært gjenstand for kritikk på grunn av at mange mener det er bortkastet energi (Gimein 2013). I tillegg sies det at veksten i markedet vil gjøre

problemet enda større. Energibruken er høy, men ikke på nivå med annen industri. Den vil heller ikke øke nevneverdig ettersom en nokså stor andel allerede er utvunnet. På samme tid er lønnsomheten på vei nedover (Anderson 2013).

6.2 Elastisitet

Vi har beregnet tilbudselastisiteten basert på prisutviklingen til bitcoin og produsert mengde i markedet. Vi fant en elastisitet på 0,07 (vedlegg 6), noe som tyder på et svært uelastisk tilbud. Dette tilsier at en økning i pris på 1 % medfører en økning i tilbudet på 0,07%. Med andre ord vil både solgt mengde og pris øke samtidig.

6.3 Fundamental verdi

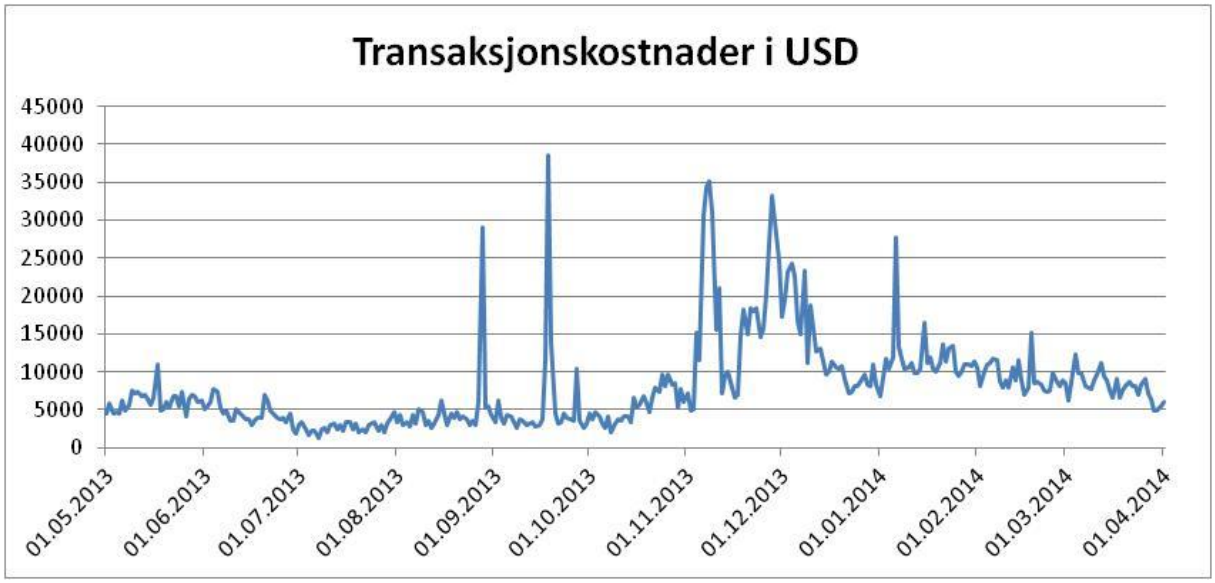
Her ønsker vi å gi et anslag på hva som kan være bitcoin sin fundamentale verdi. Det er hovedsaklig to markeder som det er rimelig å anta at bitcoin kan øke sin tilstedeværelse i. Dette dreier seg om markedene for elektronisk handel og elektroniske pengeforsendelser til hjemlandet fra arbeidsinnvandrere. Vi ser derfor på hvor stor økning det er realistisk at bitcoin kan oppnå på sikt i disse to markedene, og beregner en verdi basert på dette.

Nettverk	Gjennomsnittlig transaksjonsvolum per dag målt i millioner USD
Visa Incorporated	16518
Mastercard Incorporated	9863
China Unionpay	7562
American Express Company	2434
Discover (Pulse Network)	438
Paypal	397
Discover (Discover Network)	299
Bitcoin	257
Western Union Company	216
Xoom Corporation	15

Tabell 3: Gjennomsnittlig transaksjonsvolum for ulike betalingssystemer (Wile 2013)

Tabellen over inneholder data fra 5.desember 2013 (Wile 2013). Dette var like etter toppunktet på bitcoinkursen. Tilsvarende data for 1.april 2014 er et gjennomsnittlig transaksjonsvolum på cirka 60 millioner USD (Coinometrics 2014).

En av fordelene med bitcoin er reduserte transaksjonskostnader. Hos tilbyderne av tradisjonelle betalingsmetoder kreves ofte avgifter på flere prosent. Visa opererer med avgifter opp til 1,60 % (Visa 2014). Transaksjonskostnaden ved overføring av bitcoin er foreløpig tilnærmet eller lik null i de fleste tilfeller. Man har imidlertid muligheten til å legge til en frivillig transaksjonskostnad for å fremskynde gjennomføringen. Det vil dermed kunne være gunstig for bedrifter å tilby betaling i bitcoin ettersom man da slipper unna dyre mellomledd.



Figur 7: Estimerte transaksjonskostnader for bitcoin per dag (Blockchain 2014d)

Som figuren viser er de totale transaksjonskostnadene for bitcoin relativt små sett i sammenheng med den totale markedsverdien på over 5 milliarder dollar.

6.3.1 Avgifter i dagens system for kredittbetaling

Dagens system for kredittbetaling bygger på at bedrifter må betale en transaksjonsavgift hver gang det foretas et salg (Cohen 2008). Denne avgiften kalles merchant discount rate. I følge en rapport fra Goldman Sachs om det amerikanske markedet utgjør gjennomsnittlig merchant discount rate 3 % for kjøp over internett og 2,5 % for vanlige kjøp i butikk (Paymentlawadvisor 2014).

6.3.3 Beregning av fundamental verdi

For å kunne gjennomføre en relativ verdsettelse må vi først lokalisere markedene der bitcoin som betalingsmiddel kan ta markedsandeler. En av de viktigste styrkene til bitcoin er de lave transaksjonskostnadene. Samtidig er det en stor fordel for bedrifter at transaksjonene er

irreversible, noe som reduserer mulighetene for svindel. Dette gir gode forutsetninger for å bli en betydelig aktør i markedet for elektroniske transaksjoner.

Større utbredelse som elektronisk betalingssystem

Som vi har nevnt tidligere, er Overstock en av de største aktørene innen e-handel som tilbyr betaling med bitcoin. Administrerende direktør i selskapet har uttalt at daglig omsetning i bitcoin utgjør mellom 20 og 30 tusen amerikanske dollar (Love 2014). Vi anslår derfor en salgsmengde for Overstock per dag i bitcoin til å utgjøre 25 tusen dollar. Videre vet vi at Overstock i begynnelsen av mars 2014 passerte en million dollar i solgte varer som ble betalt med bitcoin. Basert på disse beregningene og salgstall fra Overstock første kvartal 2014 har vi kommet frem til at bitcoin utgjør 0,52% av den totale salgsmengden til Overstock (vedlegg 8).

Vi overfører andelen på 0,52% til å gjelde hele e-handelsmarkedet i USA. Vi bruker salgstall for hele salgsåret 2013. Omsetningen for elektronisk handel i USA i 2013 var cirka $262,5 milliarder dollar (Thomas, Davie, og Weidenhamer 2014). Dette betyr at total verdi for bitcoin vil være om lag 1,37 milliarder dollar. Denne verdien fordelt på 21 millioner BTC gir oss en verdi per enhet på $65,03 (vedlegg 8).

Pengeoverføring fra arbeidsinnvandrere

Dette er det andre markedet hvor bitcoin kan overta markedsandeler basert på sine lave transaksjonskostnader. Som nevnt tidligere anslås det at dette markedet har en verdi på $410 milliarder (World Bank 2013). Western Union er den mest kjente pengeoverføringstilbyderen. Årsrapporten fra 2013 viser at Western Union hadde en omsetning knyttet til elektroniske overføringer på $3 942 000 000 (Western Union 2014). Gitt at bitcoin klarer å skaffe seg en lik markedsandel, vil dette fordelt på 21 millioner mynter gi en enhetsverdi på $187,71 (vedlegg 8).

Potensiell verdi E-commerce (i USD)	1 365 641 926
Potensiell verdi pengeoverføringer (i USD)	3 942 000 000
Total verdi bitcoin (i USD)	5 307 641 926
Antall bitcoin	21 000 000
Fundamental verdi per enhet (i USD)	252,74

Tabell 4: Beregning av fundamental verdi i USD

Minste fundamentale verdi er dermed etter våre beregninger $252,74. Dette gir en total markedsverdi for bitcoin på $5,3 milliarder.

6.5 Irrasjonelle bobler

I denne delen trekker vi linjer mellom bobleteori og våre funn, noe som skal gi grunnlag for videre drøfting i neste kapittel.

6.5.1 Shillers sjekkliste

Formålet er å se hvorvidt disse momentene gjelder i markedet for bitcoin. Som vi nevnte i innledningen, har Shiller uttalt at bitcoin ser ut som en klassisk spekulativ boble (Weisenthal 2014). Bitcoin som fenomen er sannsynligvis for lite til at utlånsstandardene blir påvirket, og vi har følgelig sett bort fra dette punktet.

Rask økning i prisen slik som under eiendoms- og dotcombobler

Verdien på bitcoin økte med nesten 5500 % i løpet av 2013. Dette er svært høyt i forhold til vanlige aktiva som omsettes i markedet. Til sammenligning hadde aksjer som Infospace_Blucora og Opticom henholdsvis 1200% og 2300% kursøkning året i forkant av at dotcom-boblen sprakk (Vedlegg 7). Slike endringer kan være en indikasjon på at prisøkningen ikke oppstår som følge av fundamentale endringer, men at det er spekulering som ligger til grunn for investeringen.

Stor offentlig begeistring om en slik økning

Bitcoin er fremdeles ikke blitt et aktiva som vanlige investorer i stor grad er tilbøyelige til å sette penger i. Aktivumet har tidligere vært forbeholdt spesielt interesserte ettersom det krever ekstra innsats å forstå hvordan det fungerer. Dette skillet er blitt hvisket ut den senere tid. Et eksempel på dette er veksten i antall brukere av den elektroniske lommeboka My Wallet. I perioden fra mai 2013 til april 2014 har antall kontoer økt fra cirka 250 000 til over 1 500 000 (Blockchain 2014c).

Et medfølgende medievanvidd

Fra januar til november 2013 økte antall medieartikler i USA som omhandlet bitcoin fra 187 til 14 179 (Barford 2013). Dette samsvarer godt med kursutviklingen.

Historier om folk som tjener masse penger

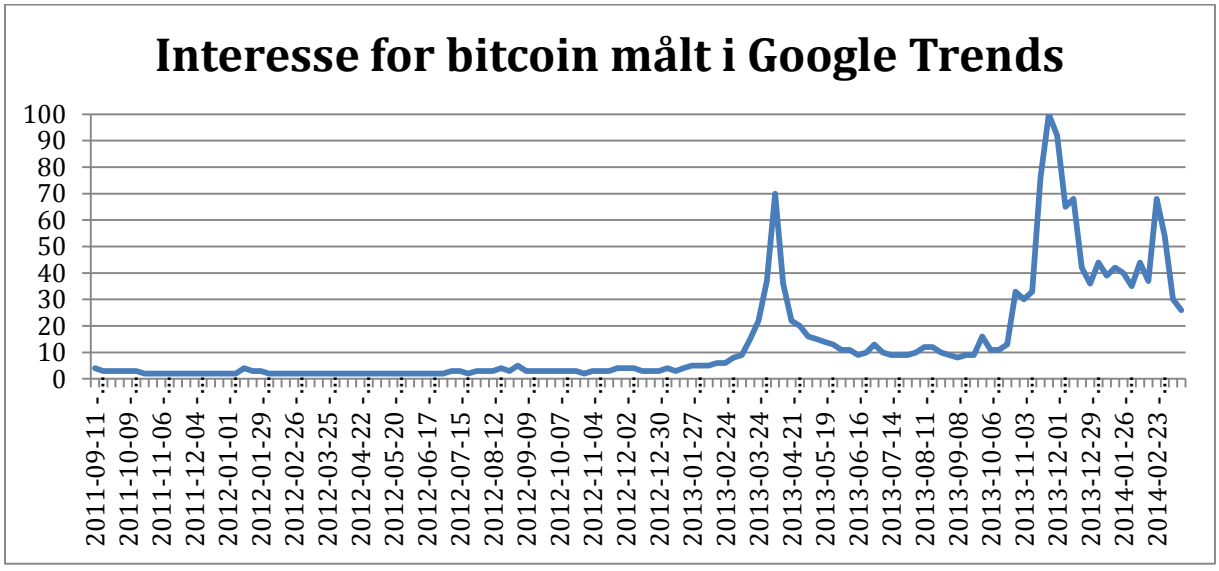
Det har dukket opp flere historier om folk som har tjent millioner på bitcoin. I 2009 investerte en norsk student 150 kroner i kryptovalutaen, noe han ikke erindret før høsten 2013. Da var verdien steget til om lag fem millioner kroner (Lauritzen 2013).

Et viktig moment her er at det også dukker opp historier om folk som har mistet harddisker som inneholdte koder til kontoer med mange mynter. Eksempelvis gjelder dette en person i England som mistet 7 500 bitcoin da han kastet datamaskinen på søppeldyngen (Harrison 2013). Det dukker opp både historier om folk som har tapt og tjent penger, men fokuset i media knytter seg til at har vært en eventyrlig prisstigning.

Mange mennesker blir trigget av å høre om hvordan andre mesker seg i lettjente penger, noe tidlige investorer i bitcoin kunne gjøre. I tillegg var det mulig å oppnå store gevinster gjennom mining. Dette er blitt vanskeligere etter hvert som flere har kommet til nettverket. Når folk har tjent store summer på å la datamaskinen stå og jobbe for seg selv, kan dette virke appellerende for andre.

Økende interesse rundt eiendelsklassen hos mannen i gaten

Det faktum at det er mulig å benytte bitcoin som betalingsmiddel i mye større grad enn tidligere, tyder på at produktet er blitt mer interessant blant vanlige folk. Vi har målt publikumsinteressen basert på data hentet fra Google Trends. Tanken er at dette skal gi et representativt bilde på interessen hos massene.



Figur 8: Søketrend for bitcoin (Google Trends 2014)

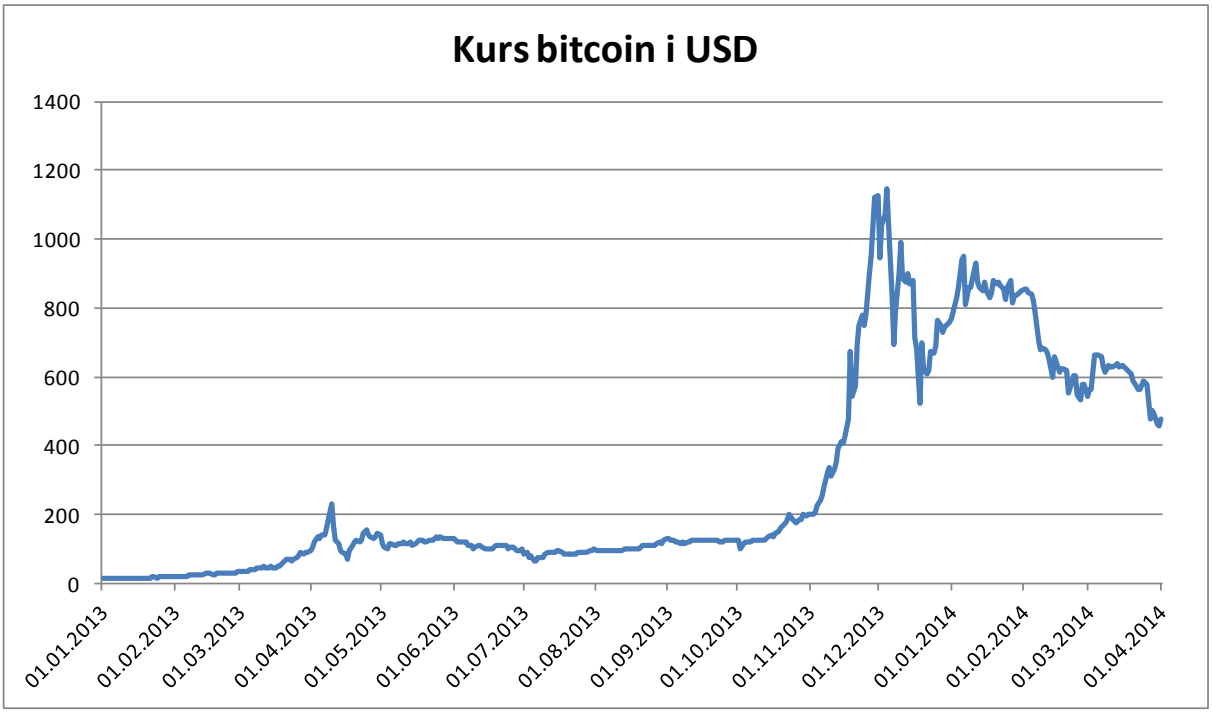
Utviklingen i søketrenden er påfallende lik kursutviklingen til bitcoin. Vi beregnet korrelasjonen mellom de logaritmiske verdiene fra Google Trends og bitcoinkursen (vedlegg 3). Her fant vi en svært sterk korrelasjon på 0,96. Dette kan være en klar indikasjon på at interessen blant mannen i gata er det som har drevet prisen oppover.

Teori om en ny æra oppstår for å rettferdiggjøre prisøkningen
Mange som ikke har tiltro til ulike styresmakters kontroll over pengeflyten i samfunnet, ser på bitcoin som en mulig løsning på dette problemet. En form for valuta uten sentralstyring fremstår som attraktivt for personer som ikke ønsker å benytte seg av offentlige tilbud. I tillegg fjernes skillet mellom ulike nasjoner, noe som gjør det enklere for aktørene i markedet å foreta transaksjoner over landegrensene.

Bitcoin kan enkelt deles opp i mindre bestanddeler, helt ned til 1 Satoshi. Satoshien tilsvarer en åttendedels bitcoin. Dette anses av mange som en stor fordel i forhold til å benytte kontanter, som i fysisk form ikke kan deles opp i mindre bestanddeler.

6.5.2 Kindleberger om bobler

I sine teorier om bobler skiller Kindleberger mellom tre typer bobler (Kindleberger og Aliber 2011). Den første kjennetegnes ved følgende; prisene øker raskt, vanligvis med en akselererende rate, for å synke veldig raskt tilbake til antatt fundamentalt nivå etter å nådd sine høyder. Agentenes forventninger om prisvekst er det som driver prisene videre oppover. Hvis prisen slutter å stige på grunn av et eksogent sjokk, vil forventningene bremses. Dette fører til at den spekulative etterspørselen forsvinner, noe som sender prisen tilbake til det fundamentale nivået. Her vil det ikke være noen forventninger om prisstigning.



Figur 9: Kursutvikling (Quandl 2014)

Som vi ser av grafen over, økte prisen på bitcoin veldig raskt mot slutten av 2013. Den voldsomme prisstigningen begynte rett etter at den ulovlige salgskanalen Silk Road ble stengt av amerikanske myndigheter. Det ble skrevet mye om bitcoin, og det er grunnlag for å anta at det var på denne tiden at bitcoin ble allmenn kjent. Man kjøpte bitcoin i forventning om å gjøre en fortjeneste på dette nye fenomenet. Det som fikk prisen til å synke igjen, var dalende etterspørsel grunnet politiske og juridiske lovgivninger angående reguleringen av bitcoin. Prisen har derimot ikke falt med samme rate som stigningen.

Den andre typen boble Kindleberger omtaler, handler om en topp hvor den holder seg en stund før den gradvis synker ned igjen mot det som antas å være fundamental verdi. Denne type boble skiller seg fra andre ved at det ikke er en utbredt panikk. Bitcoin hadde en fenomenal topp på oppunder $1200 før den halverte seg for så å stabilisere seg en kort periode på mellom $900 - $1000. Prisen har så gradvis sunket ned til å ligge mellom $400 - $500. Bitcoin kan sies å ha hatt innslag av panikk med enkelte dramatiske fall, men den nedgangen har vært gradvis hvis man ser på den historiske kursen.

Den tredje type boble utviser en periode av økonomiske vanskeligheter. Prisen øker til en topp som er etterfulgt av gradvis nedgang en periode, men så kommer panikken og krasjet.

Boblen kjennetegnes ved heterogen oppførsel blant agenter, noen insidere kommer seg ut på toppen mens andre holder fast under perioden med finansiell uro inntil panikken og krasjet inntreffer. Bitcoin ble laget som et motsvar til finanskrisen i 2008 hvor mange mente at bankene hadde skylden (Feuer 2013). Man ønsket derfor å kutte ut det unødvendige mellomleddet. Basert på den grafiske fremstillingen av bitcoinprisen økte prisen til en topp før den sank dramatisk, gikk litt opp igjen før den gradvis har sunket igjen. Bitcoin er ikke noe man finner i den vanlige husholdningen, dermed vil det sannsynligvis være det første man kutter hvis det oppstår finansiell uro. Det har ikke forekommet verken panikk eller krasj, med mindre bitcoin nå er på sitt fundamentale nivå.

6.5.3 Rodrigues bobleteori

Lite synlig

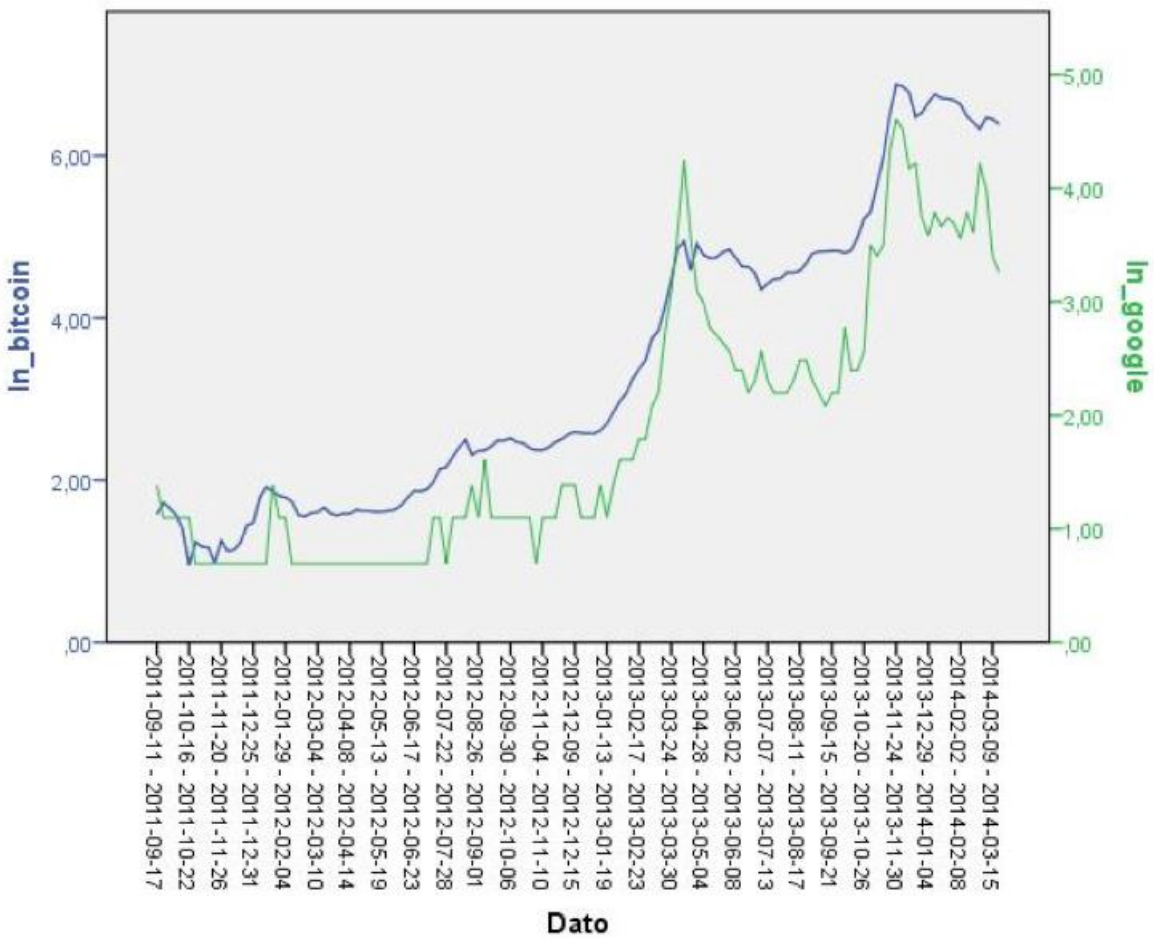
I den første perioden var bitcoin lite kjent blant vanlige borgere, og man måtte være del av spesielle nettverk for å bli opplyst om fenomenet. Det spredde seg via forum på nettet og var dermed lite synlig for allmennheten.

Bevissthet

Her begynner andre investorer å interessere seg for produktet, noe som kan samsvare med prisoppgangen i april 2013. Samtidig kan den samme nedgangen i prisen like etter skyldes, som Rodrigue nevner, at de første investorene begynner å ta ut gevinster.

Mani

Manifasen er når media griper tak i fenomenet, og allmennheten får opp øynene for produktet. Dette kan settes i sammenheng med den enorme oppgangen i november 2013. Våre funn viser også at det var i denne perioden bitcoin hadde flest søk i Google som en følge av økt eksponering. Figur 10 viser prosentvis ukentlig endring i bitcoin sin kurs og Google-søk.



Figur 10: Logaritmisk sammenheng mellom Google Trends og bitcoin (Google Trends 2014; Quandl 2014)

Avblåsning

Beskrives som en fase hvor panikken brer seg, prisen faller, man prøver å overbevise om at dette er en forbigående fase. Tilbudet blir større enn etterspørsel, og prisene faller dramatisk. Det kan virke som at det oppsto panikk i perioden da bitcoinprisen halverte seg. Oppgangen i etterkant kan skyldes at investorene prøvde å overbevise markedet om at det var en forbigående fase. Prisen har derimot per 1. april 2014 ikke falt dramatisk igjen. Dette kan tyde på at kursen nå ligger rundt en falsk topp.

7. Diskusjon

I dette kapittelet diskuterer vi i henhold til fremlagt teori, funn og analyse hvorvidt bitcoin er en boble. Første del blir brukt til å definere hva bitcoin er.

Vi har i analysedelen gjort flere funn som vi ønsker å kommentere. Volatilitetsberegningene våre er basert på historiske målinger. Det finnes metoder som gir en mer korrekt verdi på volatiliteten i dag, eksempelvis impliserte volatilitetsberegninger. Dette ville derimot involvert en mer krevende beregningsprosess enn den vi har valgt å bruke. Allikevel mener vi at våre volatilitetsberegninger gir gode nok anslag til å kunne brukes i konkluderingen av problemstillingen. Vi har også beregnet korrelasjon mellom bitcoin sin kursutvikling og antall søk i Google trends. Korrelasjonsberegningen er gjort i det statistiske analyseverktøyet SPSS. Denne korrelasjonen sier ikke direkte om bitcoin er en boble eller ikke, men vi mener den er med å implisere tilstander som beskrives i fremlagt teori.

Våre analyser av fundamental verdi inneholder en del antagelser, noe som er nødvendig når man skal prøve og predikere fremtiden. Dette kombinert med at bitcoin er et nytt fenomen med lite tilgjengelig data, har gjort vurderingen vanskelig. Vi erkjenner at denne verdien ikke er eksakt, men mener den kan gi et omtrentlig bilde. Vi mener at det er mulig for bitcoin å overta 0,5% av e-handelsmarkedet i USA basert på at enheten utgjør 0,5% av inntektene til en av de store netthandlerne. Dette er basert på dagens tall, altså vil ikke nødvendigvis bitcoin stå 0,5% av all netthandel i fremtiden. Vi mener summen, $252,74, er bitcoin sin minste fundamentale verdi, og er det tallet vi kommer til å bruke i videre diskusjon.

7.1 Hva er bitcoin?

Før vi kan begynne å diskutere hvorvidt bitcoin er en aktivaboble, må vi først se på hva vi mener bitcoin kan fungere som i det økonomiske markedet.

I analysedelen av avhandlingen har vi prøvd å se bitcoin i sammenheng med det teoretiske rammeverket som foreligger. Vi har også vurdert hvordan reguleringer og uttalelser fra ulike land kan legge føringer for den videre veien. Det er tydelig at de fleste nasjoner ikke anerkjenner bitcoin som en valuta, og det er det flere grunner til. Våre beregninger viser at bitcoin har en daglig volatilitet på rundt 8,5 %, til sammenligning har eksempelvis EUR/USD en daglig volatilitet på 0,5 %. Dette medfører stor usikkerhet for den som eier bitcoin siden

man opplever så store svingninger. Denne usikkerheten gjør det vanskelig for bitcoin å oppnå en status som unit of account, en av forutsetningene for at det skal kunne kategoriseres som en offisiell valuta. Bitcoin opplever også tydelige problemer med å løsrive seg fra den amerikanske dollaren, og er heller ikke lovmessig innlemmet som et tvungent betalingsmiddel. Dette er derimot faktorer som kan endre seg over tid, og usikkerheten kan forsvinne hvis man velger å tro på produktet og aksepterer det som unit of account.

Vi vet at pengemengden økes hver dag basert på miningen som skjer. Selv om tilbudsmengden er minkende, fordi det blir vanskeligere å utvinne, er det grunnlag for å anta at det er inflasjon i bitcoin. Det sitter derimot ikke en sentralstyringsmakt som kan påvirke denne inflasjon etter hvilket nivå man ønsker å ligge på. Eksempelvis er det ingen som kan heve eller senke renter for henholdsvis å redusere eller øke investeringer. Foreløpig er ikke dette et problem for bitcoin. Problemet ligger frem i tid når man nærmer seg taket på antall bitcoin. Siden man da vet at det ikke vil bli produsert flere mynter, er det grunnlag for å anta at eierne vil sitte på det man har i håp om fremtidig verdiøkning. Dette ligner situasjonen som Krugman beskrev i sin forklaring av deflasjon. En naturlig konsekvens er at det oppstår en nedgang i sirkulasjonen av bitcoin. Som Krugman påpeker, fører dette til at bitcoin havner i resesjon. Hadde man ikke hatt et tak, ville den enkle løsningen vært å utstede flere mynter. Samtidig er det grunnlag for å tro at mynter gradvis vil fortsette å forsvinne i uendelig fremtid, og dermed vil pengemengden reduseres. Dette fører til en deflasjonsspiral som det kan gjøres lite med. På den andre siden argumenteres det for at hvis en økonomi baserer seg kun på bitcoin som betalingsmiddel, vil det være en naturlig sirkulasjon siden alt man kan betale med er bitcoin. Et av problemene med dette argumentet er at det er for få mynter totalt til å kunne fungere som en verdensøkonomi siden det finnes en nedre grense på en åttendedels bitcoin. Dersom markedet blir stort nok, vil ikke pengemengden være av tilfredsstillende størrelse.

Vi kan med bakgrunn i analysen og diskusjonen trekke slutninger om at bitcoin ikke vil fungere som en valuta. Videre vil den heller ikke fungere som råvare på bakgrunn av at bitcoin ikke har noen alternativ anvendelse, den innehar ikke de fysiske egenskapene som kreves. og møter derfor ikke egenskapen som input i produksjon. Det tyder heller ikke på at bitcoin er en svindel, da aktivumet er svært risikofylt og med inkonsistent avkastning. Vi velger derfor å utelukke den som råvare og ren svindel.

Det kan se ut som bitcoin så langt kun har fungert som et spekuleringsobjekt, hvor man kjøper i dag med håp om prisøkning i fremtiden. Man kan handle med myntene på nettsteder, men mye tyder på at de som handler er de som allerede sitter på mynter. Det er grunn til å anta at de som handler eksempelvis på Overstock med bitcoin allerede hadde mynter da denne tjenesten ble lansert. Hvis man skal kjøpe en gjenstand på Overstock, vil man ikke først kjøpe bitcoin for så å handle eiendelen, med mindre man er ute etter å spekulere i kursgevinst. Som nevnt priser bedriftene varene i dollar, før de konverteres til bitcoin i transaksjonsøyeblikket. Dette viser hvor liten tillit bitcoin har i markedet. Vi fant i våre analyser at bitcoin sin pris har en sterk negativ korrelasjonskoeffisient med gull på -0,7. Gull kan sies å være motsyklisk, noe som vil si at man investerer i gull når resten av markedet er dårlig, som en slags sikker havn. Dette kan tyde på at man nå er i gode tider, og at man derfor har større mulighet til å spekulere og ta risiko. Hvis vi nå skulle havnet i en ny resesjon, er det lite gunstig å ha verdiene sine bundet opp i en nettvaluta som har begrenset anvendelsesmulighet. Eksempelvis vil man ikke kunne betale husleie eller lån med bitcoin. Dette kan i utgangspunktet ikke gjøres med gull heller. Allikevel er gull så utbredt i markedet at det er lett omsettelig uansett hvor i verden man er. Dette er fordi gull har en sterk posisjon historisk sett. I tillegg innehar det et annet anvendelsesområde enn som lagringsplass for verdi, det er også en råvare.

Som vi viste i analysedelen, er den største styrken til bitcoin de lave transaksjonskostnadene som blant annet gjør det mulig å gjennomføre mikrotransaksjoner. Dette er sjeldent lønnsomt å gjennomføre med dagens betalingssystemer ettersom transaksjonskostnaden kan utgjøre en for stor del av summen. Denne egenskapen skaper grobunn for innovative betalingsløsninger i forhold til pay-per-use, hvor man kan betale for eksakt forbruk av en tjeneste. Mange arbeidsinnvandrere bruker Western Union til å sende penger hjem til familie, og for dem vil det være lukrativt å minimere transaksjonskostnadene, da vi kan anta at summene de sender ikke er store. Ved å benytte bitcoin vil det åpne seg muligheter for hyppigere transaksjoner med mindre summer. Ulempen for bitcoin i forhold til Western Union er at man er avhengig av nett-tilgang for å motta den, samt problematikken rundt veksling til lokal valuta. Det er nødvendig å utvikle en infrastruktur som ikke øker transaksjonskostnadene for mye. Et annet argument er stabilisering av verdien på bitcoin. Hvis faktorer vi har påpekt tidligere stabiliserer seg og markedet går den rette veien, kan vi se for oss at bitcoin frem tid kan fungere som et elektronisk betalingssystem.

7.2 Er bitcoin en boble?

Vi har tidligere beregnet bitcoin sin tilbudselastisitet til å være 0,07. Med andre ord er tilbudet nesten uavhengig av prisendringer. En uelastisk tilbudskurve kan vise seg å bli et problem, spesielt med tanke på at antall bitcoins stadig kommer nærmere taket på 21 millioner. Dette fordi det ikke finnes virkemidler som kan benyttes til å tilpasse seg etterspørsel og generelle sykliske hensyn i økonomien. I tradisjonelle nasjonaløkonomier kan sentralbanken påvirke markedssykliske endringer gjennom å trykke penger eller endre renten.

Vi har tidligere sammenlignet bitcoin med gull, som også har et uelastisk tilbud. Problemet med et uelastisk tilbud er at prisen kan bli svært ustabil. Dette kan være et resultat av at mange benytter bitcoin som et spekuleringsinstrument. En stor fordel ved gull er at tilbudt mengde har fulgt verdensøkonomien i stor nok grad til at man ikke har opplevd nevneverdig prisinflasjon. Problemet til bitcoin er at etterspørselen er langt større enn tilbudet, selv om den ikke finnes i et verdensdekkende marked. Dersom det oppstår større vekst enn tidligere, vil dette problemet bli enda mer utbredt. Det finnes ingen måte å regulere dette på, og problemet vil derfor vedvare. Man kan derfor si at det uelastiske tilbudet er en faktor som driver prisen oppover. Senere i diskusjonen kommer vi tilbake til hvordan markedsprisen til bitcoin har utviklet seg i forhold til de fundamentale verdiene.

En rasjonell boble beholder klassisk finansteori sine forutsetninger om rasjonalitet, og kan oppstå dersom investorer er villige til å betale mer enn den observerbare fundamentale verdien tilsier. Det er vidt forskjellige oppfatninger om hva den fundamentale verdien til bitcoin er. Slikt sett holder ikke tankegangen om den observerbare fundamentale verdien i praksis. Allikevel er det grunnlag for å mene at bitcoin tildels kan se ut som en rasjonell boble. Dette kan blant annet forklares ut fra vår beregning av fundamental verdi. Beregningen bygger på at bruken av bitcoin vil være langt mer utbredt enn tilfellet er i dag. Allikevel er markedsprisen per dags dato høyere enn vår estimerte verdi.

I analysen av Shiller sin sjekkliste for bobler så vi at de fleste punktene var gjeldende for bitcoin. Til å begynne med viste vi at veksten til bitcoin overgikk kursoppgangen til flere av teknologiaksjene i perioden før dotcom-boblen sprakk. Dette var en periode hvor mange spekulerte i it-aksjer som tilsynelatende hadde liten fundamental verdi. På mange måter kan man sammenligne denne villigheten til å ta risiko med en investering i bitcoin. Her er det også tilsynelatende ingen fundamental verdi dersom man ser isolert på produktet bitcoin. Vår

vurdering er at den fundamentale verdien til bitcoin må vurderes ut fra hvilke bruksområder bitcoin kan ha. Derfor mener vi det er rimelig å si at bitcoin og dotcom-aksjene i stor grad kan sammenlignes med hverandre. Differansen mellom markedsverdi og hva de fundamentale faktorene tilsier, er så stor at det er grunnlag til å tro det er en aktivaboble.

Alle som investerer i bitcoin kan ha så mange brukerkontoer som man selv ønsker. Dette gjør det umulig å beregne nøyaktig hvor mange unike brukere det finnes. På bakgrunn av den sterke utviklingen i antall brukere av e-lommebøker, er det likevel rimelig å anta at det har vært en relativt stor vekst i antall brukere. Dette kan relateres til seksdoblingen i antall brukere hos My Wallet i løpet av det siste året. Brukerveksten kan sannsynligvis i stor grad tilskrives den økte eksponeringen i media. Som vi nevnte i analysen, var det en sterk korrelasjon mellom kursen på bitcoin og søkehistorikken i Google. Dette kan tyde på at bitcoin ikke er stabil nok i seg selv, og at medieoppmerksomhet bidrar for sterkt til prisutviklingen. Eksempelvis omtrent halverte prisen på bitcoin seg da kinesiske myndigheter gikk ut og antydet at bitcoin kunne forbys i landet i desember 2013. Det samme ville naturlig nok skjedd med aksjen til et børsnotert selskap hvis deres produkt ble strengt regulert, men til gjengjeld har et selskap en kontantstrøm-genererende virksomhet som er med å påvirke verdien. Derfor ville ikke kursen sunket lengre ned enn det som er den grunnleggende verdien til selskapet. Problemet til bitcoin er at markedsverdien er så liten at det får en stor utslagsgivende effekt med slike negative nyheter. Hvis bitcoin opplever flere slike negative nyheter på rekke og rad, kan det i verste fall sørge for at de massene som skulle stå for stabiliseringen trekker seg unna og sørger for bitcoin sin krasj.

Forkjemperne for bitcoin snakker varmt om hvordan den desentraliserte styringsmekanismen skal gjøre systemet mer pålitelig og troverdig. På kort sikt kan dette virke appellerende hos mange som ikke har tillit til dagens finanssystemer. De mener at de frie markedskreftene vil føre til stabilitet i markedet. Problemet er at man på lengre sikt ikke har noen virkemidler som kan kneble den uunngåelige deflasjonsproblematikken. Dette fører til en situasjon hvor ingen vil benytte sine bitcoins. Det vil være mer rasjonelt å holde på dem ettersom de vil stige i verdi. Et annet moment er det faktum at bitcoin noteres i forhold til andre valutaer, og stort sett er det amerikanske dollar som benyttes. Dette gjør at verdien på bitcoin vil påvirkes av den amerikanske valutastyringen.

Det har vært flere datainnbrudd hos aktører som tilbyr ulike tjenester tilknyttet kryptografisk valuta. Slike brister vil svekke tilliten til bitcoin som helhet. Med tanke på den utbredte mediedekningen er det også svært trolig at dette vil påvirke rekrutteringen av nye brukere negativt. I sentralstyrte valutaer finnes det et bankvesen som både garanterer for innskuddene og som gir en ekstra trygghet. Dette finnes ikke i markedet for bitcoin, noe som gjør innskudd svært risikabelt dersom aktørene ikke har tilstrekkelig god sikkerhet. Eksempelvis så vi ved nedleggelsen av MtGox at bitcoinprisen sank drastisk i løpet av kort tid. Det har vært flere lignende hendelser i mindre skala. Bitcoin vil aldri kunne bli akseptert som et globalt betalingsmiddel dersom sikkerhetsløsningene ikke forbedres. Skaperen av bitcoin er ukjent, og samtidig er det usikkerhet knyttet til om protokollen er fri for feil. Slike momenter vil gjøre det vanskelig å oppnå bred aksept i samfunnet, og spesielt blant de som ikke er teknologisk kyndige.

Basert på vår drøfting mener vi det er rimelig å si at bitcoin ut fra Shiller sin beskrivelse er en aktivaboble. Den ekstreme veksten kan etter vår mening ikke forklares ut fra fundamentale forhold, og det synes å være spekulativ atferd som driver prisen. Likheten til dotcom-boblen er slående, spesielt når det gjelder den raske veksten. Prisstigningen bygger på stor entusiasme og forventninger om videresalg til høyere kurs fremfor hva de fundamentale faktorer tilsier. Vårt eget estimat på fundamental verdi underbygger påstanden om at bitcoin er en boble.

Det er viktig å annonsere spørsmålet om hvorvidt bitcoin kommer til å overleve som produkt frem til taket er nådd. Som vi har nevnt tidligere vil tilnærmet alle myntene være utvunnet i 2030. Klarer man å opprettholde incentivet for minerne før man når taket? Vi vet at gevinsten reduseres samtidig som kravet til datakraft økes, noe som igjen fører til økte kostnader for minerne. Volatiliteten til bitcoin gjør det også vanskelig å forutsi hvor mye penger man vil tjene på mining i fremtiden. Gitt at prisen ikke øker i takt med kostnaden for å utvinne, vil dette si at transaksjonskostnadene må utgjøre en større del av gevinsten minerne får for arbeidet. Avhengig av pris på bitcoin, strømprisen, teknologiske nyvinninger samt andre variabler er det vanskelig å anslå hvor mye disse transaksjonskostnadene må ligge på. For å sikre fortsatt bruk er man avhengig av den lave transaksjonskostnaden som er bitcoin-nettverkets fremste konkurransefortrinn.

Det kan oppstå store problemer knyttet til incentivet for minerne. Økte transaksjonskostnader er ødeleggende for bitcoin som produkt, mens på den andre siden er lave transaksjonskostnader ødeleggende for utvinnerne på sikt. Basert på vår fundamentale analyse viser dette at prisen skal ned, noe som betyr at man ikke kan forvente at prisen kommer til å øke jevnt med vanskelighetsgraden på miningen. Hvis man da ikke øker transaksjonskostnaden, vil det etter hvert bli vanskelig å profittere på utvinning, og da mister bitcoin sin attraktivitet for utvinnerne. Dette kunne vært løst ved et system hvor utvinneren var et ikke-profitterende styringsorgan som justerte transaksjonskostnaden basert på antall transaksjoner, strømpris og vanskelighetsgraden med mål om et null-resultat. Problemet med dette er at man da må innføre en styringsmekanisme, som jo er det bitcoin er en kritikk mot. Med økende behov for datakraft og synkende utbytte i form av mynter frem mot taket, er man som nevnt veldig avhengig av prisen på bitcoin.

Hvis taket blir nådd, vil incentivsystemet måtte basere seg utelukkende på transaksjonskostnader, og utvinnerne vil ha enda større interesse av å øke denne. En løsning på dette kan være at brukermengden øker mye i forkant av at taket nås. Da vil det være mulig å opprettholde en lav prosentmessig transaksjonsavgift ettersom det totale volumet vil være mye høyere. Utvinnerne vil dermed få stor nok profitt til at de holdes fornøyde. Man kan også argumentere for at demokratiet vil seire. Brukerne og minerne kan gjennom én-datamaskin-én-stemme systemet bli enige om en transaksjonskostnad begge parter kan akseptere, noe som selvfølgelig vil være optimalt. Fremtiden til bitcoin ligger i retning av et betalingssystem, og er avhengig av å kunne opprettholde den lave transaksjonskostnaden. Vår fundamentale verdi vil ikke gi utvinnerne nok utbytte til at det vil være av interesse for disse å bruke all datakraften som kreves. Dette kan føre til at de forskjellige interessentene omsider vil ødelegge for hverandre da den enes brød er den andres død.

En løsning på problemene kan være store investeringer i kostnadsreduserende tiltak for minerne. Som vi har sett i analysen går kun 13% av nyinvesteringer til miningen mens resten hovedsakelig går til infrastruktur rundt bitcoin (figur 6). Disse investeringene vil være kostbare da det trengs ny teknologi for å effektivisere utvinningen.

Utfordringene diskutert over er så store at vi mener veien videre for bitcoin vil være enten den andre eller tredje typen bobler som vi har analysert basert på Kindleberger sine teorier. Enten synker bitcoin i fremtiden gradvis ned til fundamental verdi, eller så krasjer den. Vi tror ikke

incentivutfordringene kan løses på måten de er planlagt, og at et gradvis frafall av enten brukere eller minere sørger for at prisen synker. Det andre scenarioet vi kan se for oss, er at minerne slutter å utvinne idet profitten uteblir, eller at brukerne slutter å handle idet transaksjonskostnaden blir for stor. Man opplever da et krasj i markedet og kapitulasjonsfasen i Rodrigue sin beskrivelse av bobler er et faktum.

Et siste moment er at bitcoin på veldig lang sikt vil dø ut uansett. Tilslutt vil alle myntene være mistet, forsvunnet eller glemt på samme måte som det forsvinner norske kroner. Men i motsetning til kronen, kan man ikke trykke flere.

8. Konklusjon

Formålet med avhandlingen er å belyse teamet rundt kryptografiske valutaer, samt analysere hvorvidt det er belegg i påstanden til Robert J. Shiller om at bitcoin er en perfekt aktivaboble. Våre analyser viser at bitcoin er en boble, da prisen ligger over det som er fundamentalt nivå nå og i fremtiden. Den fungerer i dag kun som spekuleringsobjekt, og kjøpes i håp om fremtidig gevinst. Samtidig inneholder bitcoins økonomiske modell signifikante svakheter blant annet i form av et for lavt tilbudstak. Det er for mange usikkerhetsmomenter til at bitcoin kan bestå over tid.

Vi konkluderer med at bitcoin er en boble. Det vil ikke ha en fremtid som elektronisk betalingssystem, valuta eller noe annet av økonomisk funksjon. Vi mener at bitcoin som produkt er borte før 2030. Den store prisveksten har vært et resultat av spekulativ atferd blant investorer. Vi avfeier derimot ikke kryptografiske valutaer i sin helhet, og våre analyser viser tydelig at det kan være rom for et slikt betalingssystem innen netthandel. Dette kan være begynnelsen for et slikt betalingssystem, men bitcoin sin modell er feil måte å løse et slikt behov på.

Forslag til videre forskning

På bakgrunn av våre funn ligger det et godt grunnlag for videre forskning på området. Dette vil omfatte en analyse av hvilke faktorer som kan endres for å skape en mer robust økonomisk modell. Samtidig må modellen opprettholde de grunnleggende egenskapene som pseudonymitet og lave transaksjonskostnader, uten å innføre sentralisert styring. Dette kunne vært knyttet til en analyse av hvordan incentivsystemet til utvinnerne kan optimaliseres for alle involverte aktører.

Det vil være interessant med en dyptgående analyse basert på de samme punktene som vi har gjennomført. Med tilgang til store mediedatabaser kunne man med større sikkerhet sjekket om prisen styres av medieoppslag og medfølgende oppmerksomhet blant publikum. Til sist kunne en sammenlignende analyse av ulike kryptografiske valutaer vært nyttig. Dette kunne belyst hvorvidt det finnes en type kryptografisk valuta som løser problemene vi tar opp på en tilfredsstillende måte.

9. Referanser

Alden, William. 2013. "The Bitcoin Mines of Iceland." *The New York Times*, 23. desember. Hentet 5. februar 2014. http://dealbook.nytimes.com/2013/12/23/morning-agenda-the-Bitcoin-mines-of-iceland/

Anderson, Nate. 2013. "Mining bitcoins takes power, but it isn't an 'environmental disaster." Hentet 19. april 2014. http://www.wired.co.uk/news/archive/2013-04/15/bitcoin-environmental-disaster

Barford, Vanessa. 2013. "Bitcoin: Price v hype." *BBC News*, 13.Desember. Hentet 8. mars 2014. http://www.bbc.com/news/magazine-25332746

BBC. 2012. "Rewards set to halve for digital money miners." Hentet 28. april 2014. http://www.bbc.com/news/technology-20510447

BBC. 2014a. "Bitcoin not a currency says Japan government." Hentet 16. april 2014. http://www.bbc.com/news/business-26478059

BBC. 2014b. "MtGox finds 200,000 missing bitcoins in old wallet. Hentet 25. mars 2014. http://www.bbc.com/news/technology-26677291

Bitcoin.org. 2014. "Frequently Asked Questions." Hentet 3. april 2014. https://bitcoin.org/en/faq#what-happens-when-bitcoins-are-lost

Bitpay. 2014. "Questions & Answers." Hentet 1. april 2014. https://bitpay.com/pricing

Blanchard, Olivier J., og Mark W. Watson. 1982. "Bubbles, Rational Expectations and Financial Markets." Hentet 13. februar 2014. http://www.nber.org/papers/w0945.pdf?new_window=1

Blockchain. 2014a. "Difficulty." Hentet 27. april 2014. https://blockchain.info/charts/difficulty

Blockchain. 2014b. "Hashrate Distribution." Hentet 10. februar 2014. https://blockchain.info/pools

Blockchain. 2014c. "My Wallet Number Of Users." Hentet 16. april 2014. https://blockchain.info/charts/my-wallet-n-users

Blockchain. 2014d. "Transaction Fees in USD." Hentet 21. april 2014. http://blockchain.info/charts/transaction-fees-usd

Boehler, Patrick. 2013. "Chinese yuan dominates global bitcoin trade." *South China Morning Post*, 3. desember. Hentet 20. februar 2014. http://www.scmp.com/business/banking-finance/article/1371767/chinese-renminbi-dominates-global-bitcoin-trade-researchers

Brito, Jerry. 2013a. "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies. Senate Committee on Homeland Security and Governmental Affairs." Hentet 2. april 2014. http://www.hsgac.senate.gov/download/?id=0dcd748d-035a-4c0f-b695-7680adc2425d

Brito, Jerry. 2013b. "Why bitcoin's valuation doesn't really matter." Hentet 2. april 2014. http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/

Brunner, Grant. 2013. "The Bitcoin network outperforms the top 500 supercomputers combined." Hentet 10. februar 2014. http://www.extremetech.com/extreme/155636-the-bitcoin-network-outperforms-the-top-500-supercomputers-combined

Cassidy, John. 2010. "Interview with Eugene Fama." *The New Yorker*, 13. januar. Hentet 14. mars 2014. http://www.newyorker.com/online/blogs/johncassidy/2010/01/interview-with-eugene-fama.html

Clinch, Matt. 2013. "Bitcoin recognized by Germany as 'private money'." *CNBC,* 19.August. Hentet 16. april 2014. http://www.cnbc.com/id/100971898

Cohen, Greg. 2008. "Where does the money go?" Hentet 24. april 2014. http://www.transactionworld.net/articles/2008/February/commonGround1.asp

Coinbase. 2014. "What fees does Coinbase charge for merchant processing?" Hentet 1. april 2014. http://support.coinbase.com/customer/portal/articles/1277919-what-fees-does-coinbase-charge-for-merchant-processing-

Coindesk. 2014a. "Bitcoin Network Data." Hentet 28. april 2014. http://www.coindesk.com/data/bitcoin/

Coindesk. 2014b. "Exclusive: State of Bitcoin 2014 Report Analyses Emerging Trends." Hentet 24. april 2014. http://www.coindesk.com/bitcoin-2014-report/

Coindesk. 2014c. "How to Store Your Bitcoins." Hentet 17. mars 2014. http://www.coindesk.com/information/how-to-store-your-bitcoins/

Coindesk. 2014d. "What Can You Buy with Bitcoins?" Hentet 17. mars 2014. http://www.coindesk.com/information/what-can-you-buy-with-Bitcoins/

Coinmarketcap. 2014. "Crypto-Currency Market Capitalizations." Hentet 9. april 2014. http://coinmarketcap.com/all.html

Coinometrics. 2014. "Daily Transaction Volume." Hentet 1. april 2014. http://www.coinometrics.com/bitcoin/btix

Cutler, Kim-Mai. 2013. "Unfazed By Bitcoin's Wild Swings And Mysterious Origins, Silicon Valley VCs Place Their Bets." Hentet 3. april 2014. http://techcrunch.com/2013/04/11/bitcoin/

Dai, Wei. 1998. "B-money." Hentet 20. januar 2014. http://www.weidai.com/bmoney.txt

Damodaran, Aswath. 2011a. "Dark Side of Valuation." Hentet 20. april 2014. http://people.stern.nyu.edu/adamodar/pdfiles/country/darkside2012extended.pdf

Damodaran, Aswath. 2011b. "Thoughts on Intrinsic Value." Hentet 20. april 2014. http://www.stern.nyu.edu/experience-stern/faculty-research/UAT_025578

De Bondt, Werner. 2002. "Bubble Psychology." Hentet 14. februar 2014. http://driehaus.depaul.edu/about/centers-and-institutes/driehaus-center-for-behavioral-finance/publications-and-resources/Documents/206.pdf

Deng, Chao. 2014. ”China cracks down on bitcoin” *The Wall Street Journal*, 1. april. Hentet 16. april 2014. http://online.wsj.com/news/articles/SB10001424052702304157204579475233879506454

Doepke, Matthias og Martin Schneider. 2013. "Money as a Unit of Account." Hentet 3. mars 2014. http://economics.mit.edu/files/9633

Ewing, Jack. 2010. "Shiller's List: How to Diagnose the Next Bubble." *The New York Times*, 27. januar. Hentet 22. mars 2014. http://dealbook.nytimes.com/2010/01/27/schillers-list-how-to-diagnose-the-next-bubble/?_php=true&_type=blogs&_r=0

Farrell, Maureen. 2013. "Bitcoin prices surge post-Cyprus bailout." *CNN*, 28. mars. Hentet 2. april 2014. http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/

Feuer, Alan. 2013. "The Bitcoin Ideology." *The New York Times*, 14. desember. Hentet 25. januar 2014. http://www.nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html?_r=0

Finanstilsynet. 2013. "Advarsel til forbrukere - informasjon om virtuelle valutaer." Hentet 17. april 2014. http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2013/4_kvartal/Advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/

Friedman, Milton. 1992. *Money mischief: episodes in monetary history*. New York: Harcourt Brace Jovanovich.

Foodler. 2014. "Deposit Bitcoin." Hentet 5. april 2014. https://www.foodler.com/user/Bitcoin.do

Garman, Mark B., Klass, Michael J. 1980. On the Estimation of Security Price Volatilities from Historical Data. *The Journal of Business* 53(1)*:* 67-78. http://www.jstor.org/stable/2352358?seq=8

Gimein, Mark. 2013. "Virtual Bitcoin Mining Is a Real-World Environmental Disaster." *Bloomberg*, 12. april. Hentet 19. april 2014. http://www.bloomberg.com/news/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster.html

Gobry, Pascal-Emmanuel. 2013. "This 1998 Paul Krogman Column Perfectly Explains The Design Flaw At The Heart Of Bitcoin." *Forbes*, 5.april. Hentet 13. mars 2014. http://www.forbes.com/sites/pascalemmanuelgobry/2013/04/05/krugman-baby-sitting-co-op-bitcoin/

Google Trends. 2014. "Trends." Hentet 4. april 2014. http://www.google.no/trends/explore#q=bitcoin

Harrison, Virginia. 2013. "Bitcoin worth $9M buried in garbage dump." *CNN*, 29.November. Hentet 28. april 2014. http://money.cnn.com/2013/11/29/news/bitcoin-haul-landfill/

Heggstad, André. 2014. "Virtuelle valutaer - case Bitcoin." Hentet 3. mars 2014. http://beta.skatteetaten.no/virtuelle-valutaer-case-bitcoin/

Herbert, Simon A. 1978. "Rational Decision-Making in Business Organizations." Hentet 4. mars 2014. http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1978/simon-lecture.pdf

Hern, Alex. 2014. "A history of Bitcoin hacks." *The Guardian*, 18. mars. Hentet 3. april 2014. http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

Hill, Kashmir. 2014. "Bitcoin's Legality Around The World." Forbes, 31. januar. Hentet 16. april 2014. http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/

Internal Revenue Service. 2014a. "Virtual Currency." Hentet 3. mars 2014. http://www.irs.gov/pub/irs-drop/n-14-21.pdf

Internal Revenue Service. 2014b. "IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply." Hentet 16. april 2014. http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance

Jacobsen, Dag I. 2010. *Hvordan gjennomføre undersøkelser*. 2. utgave. Kristiansand: Høyskoleforlaget

Johnson, Gerry, Richard Whittington og Kevan Scholes. 2011. *Exploring Strategy*. Niende utgave. Harlow: Pearson Education.

Justcoin. 2014. "Kjøp og selg Bitcoin." Hentet 25. mars 2014. https://justcoin.no/

Kindleberger, Charles P., og Robert Z. Aliber. 2011. *Maniacs, Panics and Crashes*. Sjette utgave. Basingstoke: Palgrave Macmillan.

Lansing, Kevin J. 2007. "Asset Price Bubbles." Hentet 4. mars 2014. http://www.frbsf.org/economic-research/publications/economic-letter/2007/october/asset-price-bubbles/#subhead2

Lauritzen, Fredrik. 2013. "Kjøpte leilighet for internettpenger." *NRK,* 25. oktober. Hentet 28. mars 2014. http://www.nrk.no/okonomi/kjopte-bolig-for-internettpenger-1.11314773

Lee, Timothy B. 2013. "New Money Laundering Guidelines Are A Positive Sign For Bitcoin." *Forbes,* 19. mars. Hentet 3. april 2014. http://www.forbes.com/sites/timothylee/2013/03/19/new-money-laundering-guidelines-are-a-positive-sign-for-bitcoin/

London, J. P., Melbourne, G. T. 2011. "Bits and bob." *The Economist,* 13. juni. Hentet 15. februar 2014. http://www.economist.com/blogs/babbage/2011/06/virtual-currency

Lovdata. 2011. "Lov om Norges Bank og pengevesenet mv." Hentet 3. mars 2014. http://lovdata.no/dokument/NL/lov/1985-05-24-28/KAPITTEL_3#KAPITTEL_3

Love, Dylan. 2014. "Overstock CEO: We're Doing $20k - $30k In Bitcoin Transactions Per Day. *Business Insider,* 12.Mars." Hentet 4. mai 2014. http://www.businessinsider.com/bitcoin-and-overstock-2014-3#!JlSwY

McDonald, Robert L. 2013. *Derivatives Markets*. Boston: Pearson Education.

Mihm, Stephen. 2013. "Are Bitcoins the Criminal's Best Friend?" *Bloomberg,* 18.November. Hentet 3. april 2014. http://www.bloombergview.com/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-

Nakamoto, Satoshi. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System." Hentet 20. januar 2014. https://bitcoin.org/bitcoin.pdf

Opstad, Leiv. 2012. *Innføring i makroøkonomi for økonomisk-administrative studier*. Oslo: Cappelen Damn.

Organisation for Economic Co-operation and Development. 2006. "Online Payment Systems For E-Commerce." Hentet 6. mars 2014. http://www.oecd.org/internet/ieconomy/36736056.pdf

Overstock. 2014. "Overstock.com Reports FY and Q4 2013 Results." Hentet 20. mars 2014. http://investors.overstock.com/phoenix.zhtml?c=131091&p=irol-newsArticle&ID=1895315&highlight=

Paymentlawadvisor. 2014. "Goldman Sachs: All about Bitcoin." Hentet 24. april 2014. http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf

Quandl. 2014. "Bitcoin Exchange Rate (BTC vs. USD) on Bitstamp." Hentet 2. april 2014. http://www.quandl.com/BITCOIN/BITSTAMPUSD-Bitcoin-Markets-bitstampUSD

Rodrigue, Jean-Paul. 2013. *The Geography of Transport Systems*. Tredje utgave. New York: Routledge.

Rosser, J. Barkley, Rosser, Marina V., og Gallegati, Mauro. 2012. A Minsky-Kindleberger Perspective on the Financial Crisis. *Journal of Economic Issues* 46(2): 449-458.

Rouse, Margaret. 2005. "Peer-to-peer." Hentet 27. januar 2014. http://searchnetworking.techtarget.com/definition/peer-to-peer

Rouse, Margaret. 2006a. "Hashing." Hentet 27. januar 2014. http://searchsqlserver.techtarget.com/definition/hashing

Rouse, Margaret. 2006b. "Node." Hentet 27. januar 2014. http://searchnetworking.techtarget.com/definition/node

Rouse, Margaret. 2008. "Nonce." Hentet 28. januar 2014. http://searchsecurity.techtarget.com/definition/nonce

Secher, Kristian. 2013. "Fornuften forsvinner i informasjonsfellene på nettet." Hentet 11. mars 2014. http://www.forskning.no/artikler/2013/juni/360373

Shapiro, Bruce. 2000. "Bits and Bytes". Hentet 28. januar 2014. http://taomc.com/bits2bots/bitbyte1.htm

Shiller, Robert J. 2005. *Irrational Exuberance*. Andre utgave. Princeton, N.J: Princeton University Press.

Skatteetaten. 2013. "Bruk av Bitcoins - skatte- og avgiftsmessige konsekvenser." Hentet 17. april 2014. http://www.skatteetaten.no/no/Radgiver/Rettskilder/Uttalelser/Prinsipputtalelser/Bruk-av-bitcoins--skatte--og-avgiftsmessige-konsekvenser/

Spendbitcoin. 2014. "Places that accept bitcoin." Hentet 5. april 2014. https://spendbitcoins.com/places/

Steigum, Erling. 2006. "Aktivabobler - kan og bør myndighetene gjøre noe?" *Magma,* 9(1): 57-67. http://www.magma.no/aktivabobler-kan-og-boer-myndighetene-gjoere-noe

Stiglitz, Joseph E. 1990. "Symposium on Bubbles." *Journal of Economic Perspectives* 4(2): 13-18.

Studenmund, A. H. 2011. *Using Econometrics: A Practical Guide*. 6th edition. Boston: Pearson Education, Inc.

Szabos, Nick. 2005. "Bit Gold". Hentet 22. januar 2014. http://unenumerated.blogspot.no/2005/12/bit-gold.html

Szydlo, Michael. 2004. "Recent improvements in the efficient use of merkle trees: additional options for the long term." Hentet 29. januar 2014. http://www.emc.com/emc-plus/rsa-labs/historical/recent-improvements-efficient-use-merkle-trees.htm

The World Bank. 2013. "Developing Countries to Recieve Over $410 Billion in Remittances in 2013, Says World Bank." Hentet 1. april 2014. http://www.worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank

The World Bank. 2014. "An Analysis of Trends in the Average Total Cost of Migrant Remittance Services." Hentet 1. april 2014. https://remittanceprices.worldbank.org/sites/default/files/RPW_Report_Mar2014.pdf

Thomas, Ian, William Davie, og Deanna Weidenhamer. 2014. "Quarterly Retail E-Commerce Sales 4th Quarter 2013." Hentet 6. mai 2014. http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

U.S. Securities and Exchange Commission. 2014. "Ponzi Schemes." Hentet 6. mars 2014. http://www.sec.gov/answers/ponzi.htm

Varian, Hal R. 2010. *Intermediate Microeconomics: A Modern Approach*. New York: W. W . Norton & Company, Inc.

Visa. 2014. "Visa Domestic Interchange Reimbursement Fees 2014." Hentet 21. april 2014. http://www.visaeurope.com/en/about_us/our_business/fees_and_interchange.aspx

Weisenthal, Joe. 2014. ”Robert Shiller: Bitcoin is an amazing example of a bubble.” *Business Insider,* 24.Januar. Hentet 6. mars 2014. http://www.businessinsider.com/robert-shiller-bitcoin-2014-1

Western Union. 2013. "Frequently Asked Questions." Hentet 1. april 2014. http://onlinefx.westernunion.com/faq/

Western Union. 2014. "Western Union Reports First Quarter Results." Hentet 3. mai 2014. http://ir.westernunion.com/files/doc_news/Financial%20News/WU%20FINAL%20Q1%202014%20ER%20043014.pdf

Wile, Rob. 2013. "The Daily Value Of Bitcoin Transactions Has Passed Western Union's And It's Catching Up To Paypal's." *Business Insider,* 5.Desember. Hentet 20. mars 2014. http://www.businessinsider.com/bitcoin-versus-paypal-comparison-2013-12#!JsLrr

Wilhelm, Alex. 2014. "Overstock's Bitcoin Purchases Account For Less Than 1% Of Revenue, But It's Growing." Hentet 17. mars 2014. http://techcrunch.com/2014/03/12/overstocks-Bitcoin-purchases-account-for-less-than-1-of-revenue-but-its-growing/

10. Vedlegg

Vedlegg 1: Satoshi Nakamoto sin manual

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

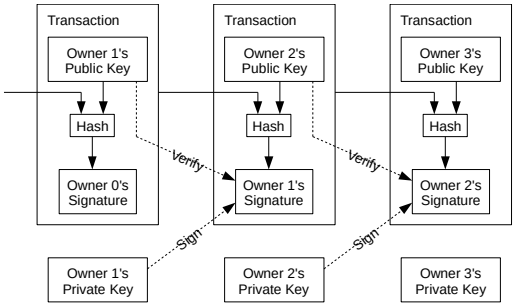
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

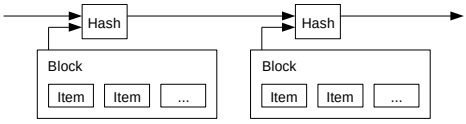


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

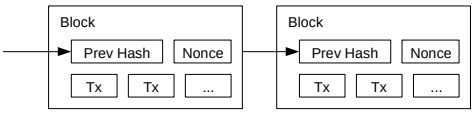
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

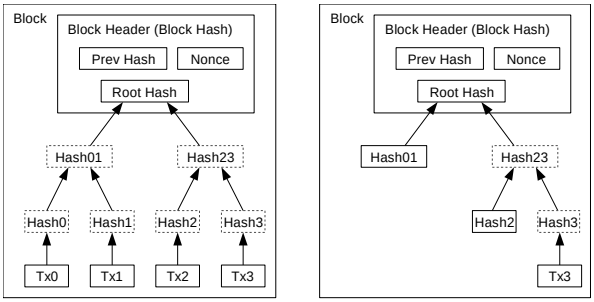
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



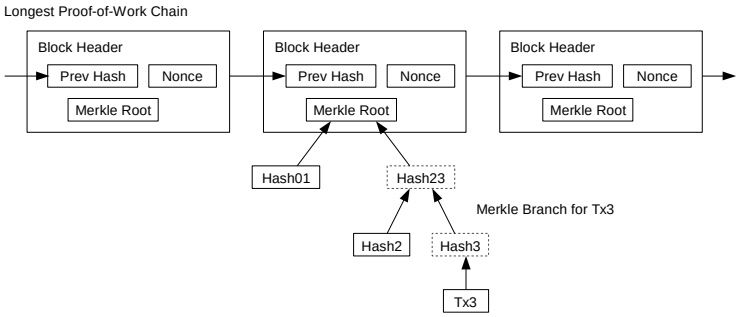
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

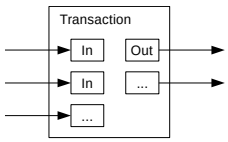
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

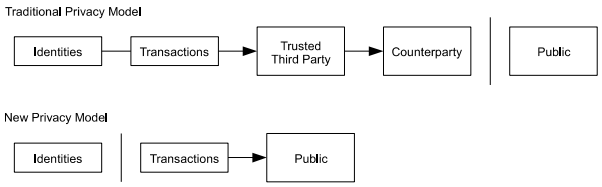
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012

q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Vedlegg 2: Daglige og årlige volatilitetsberegninger

Aktiva	Daglig volatilitet	Årlig volatilitet
EUR/USD	0,52%	8,20%
Yahoo	1,22%	19,42%
Dow Jones Industrial Indeks	1,50%	23,78%
Software Indeks Verden	2,15%	34,19%
Software Indeks Kina	2,19%	34,76%
Software Indeks Europa	2,41%	38,19%
Software Indeks USA	2,56%	40,60%
Tiscali	3,86%	61,23%
Opticom	5,49%	87,18%
Lycos	5,61%	89,12%
Infospace_Blucora	7,37%	116,94%
Microstrategy	7,43%	118,02%
Geeknet	7,73%	122,75%
Bitcoin	8,52%	162,74%
Worldcom	19,50%	309,53%

Tabell 5: Daglig og årlig volatilitet. Data hentet fra Datastream og Quandl

Vedlegg 3: Korrelasjonsberegninger

Correlations

		Googletrends	Bitcoin
Googletrends	Pearson Correlation	1	,872
	Sig. (2-tailed)		,000
	N	132	132
Bitcoin	Pearson Correlation	,872	1
	Sig. (2-tailed)	,000	
	N	132	133

Correlations

		ln_googletrends	ln_bitcoin
ln_googletrends	Pearson Correlation	1	,960
	Sig. (2-tailed)		,000
	N	132	132
ln_bitcoin	Pearson Correlation	,960	1
	Sig. (2-tailed)	,000	
	N	132	133

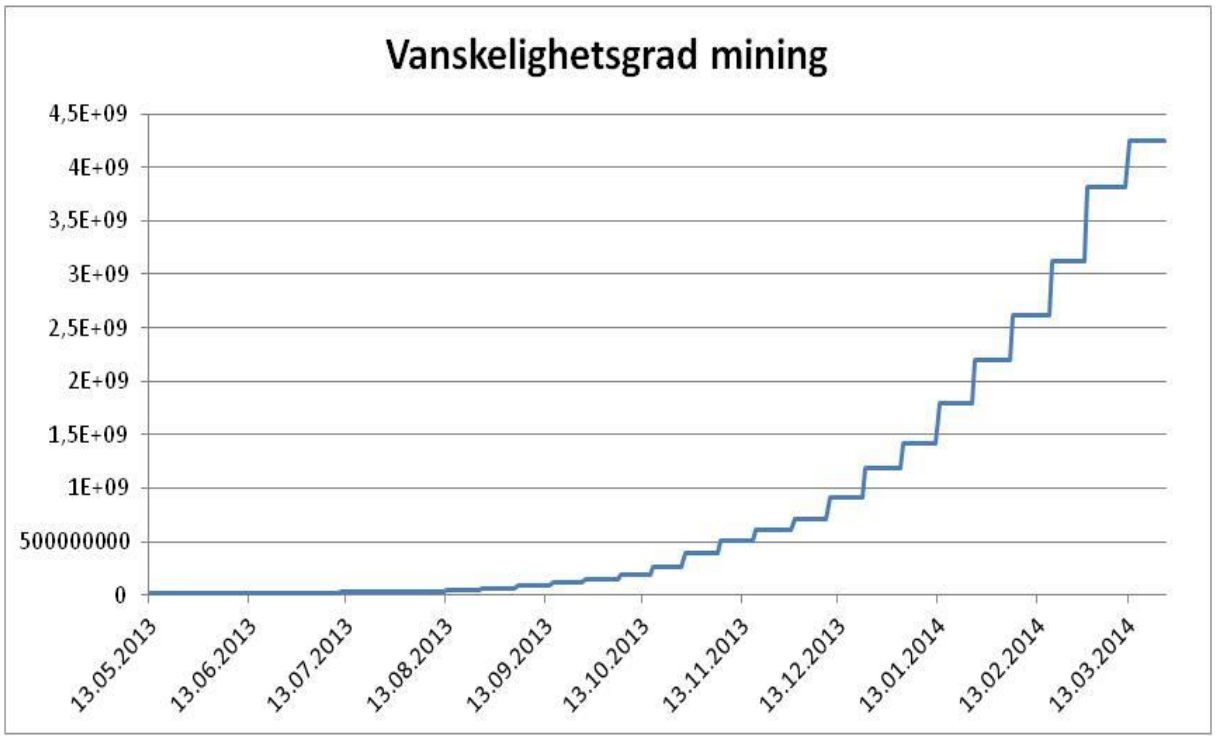
Correlations

		ln_googletrends_2013-2014	ln_bitcoin_2013-2014
ln_google_2013-2014	Pearson Correlation	1	,899**
	Sig. (2-tailed)		,000
	N	65	65
ln_bitcoin_2013-2014	Pearson Correlation	,899**	1
	Sig. (2-tailed)	,000	
	N	65	65

**. Correlation is significant at the 0.01 level (2-tailed).

Korrelasjon gullpris/bitcoin 1.1-2012 - 1.4-2014	-0,7062

Vedlegg 4: Vanskelighetsgrad mining (Blockchain 2014a)



Vedlegg 5: Fordeling av ny venturekapital (Coindesk 2014b)

Sektor	Verdi (millioner USD)	Prosentvis andel	Antall bedrifter
Betalingsformidler	36,7	37,60%	6
Handelsbørs	14	14,34%	9
Finansielle tjenester	22,5	23,05%	7
Miningutstyr	13,1	13,42%	3
Ukjent	10	10,25%	2
Lommebøker	1,3	1,33%	3
Sum	97,6	100,00%	30

Vedlegg 6: Beregning av tilbudselastisitet

Akkumulert prosentvis endring i tilbudt mengde			0,45
Akkumulert prosentvis endring i pris			6,56
Tilbudselastisitet			0,07

Vedlegg 7: Årlige avkastninger

	Måleperiode	Årlig avkastning
Bitcoin	2013	5461 %
Opticom	1999	2329 %
Infospace_Blucora	1999	1187 %

Vedlegg 8: Beregning av fundamental verdi

Salgsinntekter i BTC hos Overstock Q1 2014	1775000
Totale salgsinntekter Overstock Q1 2014	341 200 000
Inntekt bitcoin i % av totale salgsinntekter	0,520 %
Overstock markedsandel E-commerce i USA	0,497 %
Salgsinntekter E-commerce i USA 2013	262 511 000 000
Potensielt marked for BTC innen E-commerce	1 365 641 926
Verdi per bitcoin	65,03
Total remittance (estimat for 2013)	410 000 000 000
Western Union omsetning 2013	78 840 000 000
Markedsandel Western Union	19,23 %
Elektronisk omsetning WU	5,00 %
Potensielt marked for bitcoin	3 942 000 000
Verdi per bitcoin	187,71
Sum fundamental verdi per bitcoin	252,74

Sektor	Verdi (millioner USD)	Prosentvis andel	Antall bedrifter
Betalingsformidler	36,7	37,60 %	6
Handelsbørs	14	14,34 %	9
Finansielle tjenester	22,5	23,05 %	7
Miningutstyr	13,1	13,42 %	3
Ukjent	10	10,25 %	2
Lommebøker	1,3	1,33 %	3
Sum	97,6	100,00 %	30

http://www.slideshare.net/fullscreen/CoinDesk/coindesk-state-of-bitcoin-2014/55