

Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2014

Joni Pönkä

# KRYPTOVALUUTAT SIJOITUSKOHTENA

– Lainsäädäntö ja riskienhallinta



TURUN AMMATTIKORKEAKOULU  
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

Marraskuu 2014 | 40 sivua

Pasi Iivonen

Joni Pönkä

# KRYPTOVALUUTAT SIOITUSKOHTENA – LAINSÄÄDÄNTÖ JA RISKIENHALLINTA

Tämän opinnäytetyön aiheena on kryptovaluuttojen turvallisuus sijoituskohtena. Työn on tarkoitus tarjota sijoittajalle tarvittavat taidot mahdollisimman turvalliseen ja riskittömään sijoittamiseen. Työ tehdään omasta kiinnostuksesta sijoittamista kohtaan.

Työn teoriaosuudessa kuvaillaan virtuaalivaluuttojen tekninen toiminta sekä käsitellään kuinka tällaisen valuutan arvo muodostuu. Lukijalle tarjotaan erilaisia tapoja säilyttää kryptovaluuttaa sekä käsitellään eri säilytystapojen turvallisuutta. Lähemmin tutustutaan verottajan suhtautumiseen virtuaalivaluutan käyttämiseen. Työssä keskitytään Suomen verottajan ohjeistukseen. Työssä perehdytään myös lainsäädäntöön sekä valtioiden suunnalta tuleviin riskeihin.

Työssä sekä ostetaan että myydään bitcoin virtuaalivaluuttaa suomalaisen palveluntarjoajan välityksellä. Työssä perehdytään kaupan eri vaiheisiin sekä otetaan kantaa myymisen kannattavuuteen.

Työmenetelminä ovat kirjalliset lähteet sekä empiiriset toimenpiteet virtuaalivaluutan säilyttämisessä, myymisessä sekä ostamisessa. Lähteet ovat enimmäkseen verkkolähteitä, mutta myös verohallinnon tiedoksiäntöä sekä kirjallisuutta käytetään.

Työn tuloksena on kokonaisuus jonka avulla kiinnostunut henkilö kykenee sijoittamaan mahdollisimman turvallisesti näihin korkean riskin kohteisiin. Työn perusteella kryptovaluuttaan sijoitetut summat tulee ymmärtää mahdollisesti menetetyiksi.

ASIASANAT:

Pääomasijoittaminen, riskienhallinta, tietoturva, virtuaalivaluutta

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

November 2014 | 40 pages

Pasi Iivonen

Joni Pönkä

# INVESTING IN CRYPTOCURRENCY – LEGISLATION AND RISK MANAGEMENT

The objective of this bachelor's thesis is safety of cryptocurrencies as an investment target. This thesis aims to give the necessary skills to invest as safely as possible. The thesis was written as a result of the writer's personal interest in investing.

The theoretical part discusses how cryptocurrency works and how the value of these virtual currencies is defined. The thesis offers different ways to store cryptocurrency and examines their safety to the user. A closer look is also taken on how taxation authorities see virtual money usage and investing. The tax examples are mostly from the Finnish tax regulations. It is also discussed how the legislation sees virtual money.

In this work bitcoins are purchased and sold via a Finnish service provider. A closer look is taken on the necessary needed steps as well as a stand when selling is profitable.

Mainly written sources were used in the thesis. Also some empirical methods were used when virtual currency was purchased, stored and sold. The sources are mainly from the Internet but literature and taxation information were also used.

As a result, the reader is provided with good tools to safely invest in cryptocurrency. These currencies are considered to be extremely high risk investment and the investor must be ready to lose everything.

## KEYWORDS:

Cryptocurrency, investing, information security, risk management

# SISÄLTÖ

<b>SANASTO</b>	<b>6</b>
<b>1 JOHDANTO</b>	<b>6</b>
<b>2 KRYPTOVALUUTTA</b>	<b>7</b>
2.1 Historia	7
2.2 Bitcoinin synty	8
2.3 Toiminta	8
<b>3 VALUUTAN ARVON MUODOSTUMINEN</b>	<b>11</b>
<b>4 KRYPTOVALUUTAN HENKILÖKOHTAISET SÄILYTYSTAVAT</b>	<b>12</b>
4.1 Paperilompakko	12
4.2 Lompakko tietokoneella	13
4.3 Lompakko puhelimessa	14
<b>5 VERKKOPANKKI</b>	<b>16</b>
<b>6 VALUUTAN HANKKIMINEN</b>	<b>17</b>
<b>7 KRYPTOVALUUTAN KÄYTTÄMINEN</b>	<b>20</b>
<b>8 TURVALLISUUS SIOITTAJALLE</b>	<b>22</b>
<b>9 KRYPTOVALUUTAN OSTAMINEN</b>	<b>25</b>
<b>10 KRYPTOVALUUTAN REALISOINTI</b>	<b>28</b>
<b>11 VEROSEURAAMUKSET JA LAINSÄÄDÖNTÖ</b>	<b>32</b>
<b>12 YHTEENVETO</b>	<b>35</b>
<b>LÄHTEET</b>	<b>37</b>

## KUVAT

Kuva 1. Bitcoin paperilompakon generointi.	13
Kuva 2. Mycelium: rahan vastaanotto.	15
Kuva 3. Minered litecoin louhinta.	19
Kuva 4. Bitcoin ostotapahtuma. ( <a href="https://bittiraha.fi/bitcoin/buy">https://bittiraha.fi/bitcoin/buy</a> ).	26
Kuva 5. Maksutapahtuma. ( <a href="https://bittiraha.fi/bitcoin/buy">https://bittiraha.fi/bitcoin/buy</a> ).	27
Kuva 6. Bitcoinien myynti. ( <a href="https://bittiraha.fi/myy">https://bittiraha.fi/myy</a> ).	30

# SANASTO

Bitcoin	Tunnetuin laajaan käyttöön levinnyt kryptovaluutta. (Gilson 2013.)
Bitcoin-Qt	Bitcoin louhintaohjelma. (Nakamoto 2014.)
Feathercoin	Vaihtoehtoinen kryptovaluutta. (Comparison of cryptocurrencies.)
Hajautettu laskenta	Tehtävä jota fyysisesti eri paikoissa sijaitsevat koneet suorittavat. (Bittiraha.fi 2014b.)
Kryptovaluutta	Verkossa toimiva virtuaalinen raha. (Smithers 2013.)
Litecoin	Vaihtoehtoinen kryptovaluutta. (Comparison of cryptocurrencies.)
Lohkoketju	Kryptovaluutan tiivistetty siirtohistoria jota ylläpidetään hajautetulla laskennalla. (Bittiraha.fi 2014a.)
Louhinta	Ilmaisu jota käytetään kryptovaluutan siirtohistorian ylläpitämisestä. (Bittiraha.fi 2014a.)
Mt. Gox	Konkurssiin päätnyt bitcoin välittäjä. (Kelleher 2014.)
Namecoin	Vaihtoehtoinen kryptovaluutta. (Comparison of cryptocurrencies.)
Virtuaalivaluutta	Synonyymi kryptovaluutalle. (Bittiraha.fi 2014a.)
Yhteisölouhinta	Louhintaprosessi jossa iso joukko ratkaisee samaa lohkoketjun osaa. Tällä saavutetaan suuri laskentateho. (Pooled mining.)

# 1 JOHDANTO

Kryptovaluutat yleisessä käytössä ovat kohtalaisen tuore ilmiö. Kuitenkin johtuen yleisestä kiinnostuksesta, tietomurroista, häiriöitä sekä vioista ovat ne näkyneet uutisissa. Nämä häiriöt ovat aiheuttaneet huomattavia menetyksiä bitcoin-sijoittajille. Lisäksi valuutan arvostus on kärsinyt näistä vahingoista.

Kuitenkin bitcoinin sekä muiden kryptovaluuttojen, kuten feathercoinin tai litecoinin alkuperäinen ajatus oli luoda turvallinen valuutta. Raha joka on vapaa pankkien sekä valtioiden hallinnasta.

Isoimmat ongelmat kryptovaluutoissa ovat koskeneet valuutan säilyttämistä. Käyttäjät ovat halunneet luovuttaa virtuaalivaluuttansa pankkien hallintaan. Pankkeihin on murtauduttu tai niiden perustajat ovat olleet epärehellisiä. Näin kryptovaluuttojen alkuperäinen idea on kärsinyt juuri yhdestä perustamisen alkuperäisistä syistä: pankeista.

Tämän työn tavoitteena on ohjeistaa kryptovaluutan käyttäjää minimoimaan riskit. Lisäksi sijoittajan on hyvä tuntea valuuttaa koskeva lainsäädäntö sekä verokäytännöt.

Opinnäytetyön empiirisessä osuudessa esitellään turvallinen tapa säilyttää sekä käyttää kryptovaluuttaa. Esimerkkinä käytetään bitcoinia sen tunnettavuuden vuoksi. Lisäksi tarkastellaan yhtä tapaa sijoittaa sekä realisoida kyseistä valuuttaa ilman että tarvitsee turvautua bitcoin-pankkiin.

Teoriaosuudessa selvitetään kryptovaluutan yleistä toimintatapaa sekä esitellään kryptovaluutan louhintaprosessi. Lisäksi tutkitaan tarkemmin mitä turvallisuustekijöitä tulee ottaa huomioon sekä miten valuutan arvo suhteessa perinteiseen rahaan määräytyy. Lisäksi tarkastellaan kryptovaluuttoja koskevaa verotusta sekä lainsäädäntöä suomessa ja maailmalla. Työssä otetaan myös kantaa valuutan realisointiin.

Suurin osa työn esimerkeistä koskee bitcoin-valuuttaa, mutta nämä asiat ovat yleistettävissä myös muihin kryptovaluutoihin.

## 2 KRYPTOVALUUTTA

Virtuaalivaluutat voidaan jakaa karkeasti kolmeen alaryhmään. Ryhmässä yksi ovat suljetut valuutat, joilla ei ole mitään kontaktia muihin valuuttajärjestelmiin. Ryhmässä kaksi ovat virtuaalivaluutat, joilla on vain yksisuuntainen virtaus. Niitä on siis mahdollista ostaa jollakin toisella valuutalla, mutta niiden realisointi ei ole mahdollista. Kolmas ryhmä ovat virtuaalivaluutat kaksisuuntaisella virtauksella. Näitä valuuttoja voi ostaa muilla valuutoilla ja niiden realisointi on mahdollista kohtalaisen helposti. (Paganini & Amores 2013. 108.)

Ryhmän yksi ja kaksi virtuaalivaluutat ovat yleensä jonkin hyvin suljetun yhteisön, kuten esimerkiksi jonkin pelin käyttämiä järjestelmiä. Sijoittajan kannalta nämä ovat lähes merkityksettömiä. Tässä työssä käsiteltävät valuutat kuuluvat kaikki kolmanteen ryhmään. (Paganini & Amores 2013. 108.)

### 2.1 Historia

Ensimmäisen ajatuksen anonyymistä digitaalisesta vaihdon välineestä esitti David Chaum jo vuonna 1982. Hänen alkuperäinen ajatuksena oli kohtalaisen yksinkertainen, mutta peruseriaatteiltaan hyvin nykyisiä digitaalisia valuuttoja vastaava. Hänen ajatuksessaan valuuttasiirroista vastasi kuitenkin jokin tietty taho, eikä hajautettu laskenta kuten nykyisissä kryptovaluutoissa. (Chaum 1998.)

Chaum vastasi myös ensimmäisistä yrityksistä luoda toimivaa digitaalista valuuttaa. Vuonna 1990 hän perusti sähköistä rahaa kehittälevän ja välittävän DigiCash Inc yrityksen. Kyseinen yritys ajautui konkurssiin vuonna 1998. Joitakin yrityksen toimintoja myytiin eteenpäin ja Chaumin kehittelemää teknologiaa onkin käytössä edelleenkin rahansiirtojen salauksessa. (Grigg 1999.)



## 2.2 Bitcoinin synty

Ensimmäinen nykymuotoinen kryptovaluutta on bitcoin. Sen julkaisi vuonna 2008 Satoshi Nakamoto niminen taho. Edelleenkin ei tiedetä onko julkaisija yksittäinen henkilö vai jokin ryhmittymä. Ensimmäinen bitcoin-louhintaan soveltuva ohjelmisto Bitcoin-Qt julkaistiin vuonna 2009. Bitcoin-valuutan perusajatus oli mahdollistaa anonyymit ilmaiset rahansiirrot ilman tarvetta siirtoja käsitteleville raskaille instituutioille. (Nakamoto 2014.)

Bitcoinin julkaisun jälkeen useat tahot alkoivat kehittää omia versioitaan kryptovaluutalle. Tunnetuimpia näistä lienevät namecoin ja litecoin. Namecoin luotiin tarjoamaan hajautetumpi nimijärjestelmä, jotta valuutansiirtoja ei voitaisi estää valtiollisella taholla. Litecoin puolestaan tarjoaa lähes välittömät siirrot. Bitcoin siirtoon menee tyypillisesti muutamia tunteja. (Gilson 2013.)

## 2.3 Toiminta

Kryptovaluutat perustuvat hajautettuun laskentaan, jota suorittaa vapaaehtoisten yhteisö. Tämä yhteisö sekä käyttää että ylläpitää valuuttajärjestelmää. Käyttäjän antaessa koneensa resursseja siirtoverkon käyttöön hänen koneensa sekä suorittaa siirtoja että varmentaa aikaisemmin tapahtuneet rahansiirrot. Käytännössä kryptovaluutan verkko on hajautettu kirjanpitolietokanta. Tähän tietokantaan on tallennettuna jokainen koskaan tapahtunut rahansiirto. (Bittiraha.fi 2014a; Smithers 2013.)

### **Lohkoketju**

Kryptovaluutan hajautettua tietokantaa kutsutaan lohkoketjuksi. Jokainen tapahtunut siirto kirjataan yhteen lohkoon, joka sisältää tiivisteen edellisten lohkojen otsikoista ja tapahtumista. Siirtojen laskenta eli louhiminen on käyttäjien suorittamaa hajautettua laskentaa. Laskennan tarkoituksena on luoda tarpeeksi vaikeat tiivisteet, jotta väärennetyn siirtohistorian luominen olisi taloudellisesti kannattamatonta. Tullakseen hyväksytyksi osaksi siirtohistoriaa,

tulee uuden lohkon olla tarpeeksi monimutkainen ja täyttää tiettyjä tarkkaan määriteltyjä sääntöjä. Mikäli lohkossa on poikkeamia, se ei pääse osaksi lohkoketjua. (Bittiraha.fi 2014a.)

Koko valuuttaverkon kaikki tapahtumat ovat varmennettuna jokaisessa uudessa lohkossa. Yhdenkin siirron muuttamiseksi täytyisi lohkoketjua purkaa laskennallisesti miljoonia kertoja taaksepäin. Tämä vaatisi valtavan laskentatehon ja olisi taloudellisesti erittäin kallista. Ketjuun voi tulla haaraumia, jotka poikkeavat vaikeusasteeltaan toisistaan. Hajautetun laskennan sääntöjen mukaan vaikeampi näistä ketjuista jää voimaan. Tämä mahdollistaa yksimielisyyden hajautetussa laskennassa. (Bittiraha.fi 2014a.)

### **Valuutan syntyminen**

Kryptovaluuttoja yhdistää tapa jolla uutta valuuttaa syntyy. Valuutan syntymisessä on jäljitely arvometallien louhintaa. Bitcoin-valuutassa uusia coineja syntyy 144 pakettia joka päivä. Nämä arvotaan siirtoverkkoon tehdyn laskentatyön painottamana. Yhden paketin koko 22.3.2014 oli 25 bitcoinia. Paketin koko puolittuu 210000 ratkaistun lohkon välein. Valuutan syntyminen siis hidastuu ajan myötä. Bitcoinien tapauksessa lopullinen määrä tulee olemaan hieman alle 21000000 btc. Tämä määrä saavutetaan arviolta vuonna 2140. Määrät vaihtelevat hieman eri valuuttojen välillä mutta peruseriaate on sama kaikissa. (Bittiraha.fi 2014a.)

### **Lompakko**

Jokainen valuuttaverkon käyttäjä omistaa virtuaalisen lompakon. Tämä lompakko koostuu yksityisestä avaimesta, jolla lompakosta voidaan siirtää rahaa pois, sekä mielivaltaisesta määrästä julkisia avaimia. Julkiset avaimet luodaan yksityisestä avaimesta. Julkisella avaimella voi ainoastaa siirtää rahaa lompakkoon. Julkinen avain on noin 33 merkkiä pitkä jono satunnaisia merkkejä (Willis 2010). Esimerkiksi 1LK6zTA2DjyM7Cehc5Hsu3emQHJ9QoaFLL on erään bitcoin-lompakon julkinen avain.

## **Rahansiirto**

Rahansiirrot tapahtuvat ilmoittamalla laskentaverkolle sisääntulon ja ulostulon komennot. Sisääntulossa on siirtävän tahon yksityinen avain sekä tieto mistä raha on tullut alun perin kyseiseen osoitteeseen. Ulostulo sisältää vastaanottajan julkisen avaimen. Vertaamalla näitä tietoja lohkoketjuun siirto-ohjelma varmentaa, ettei kyseisiä yksiköitä ole aikaisemmin siirretty. Siirto kirjataan lohkoon peruuttamattomasti. Siirrosta tulee välittömästi julkista tietoa, joka kirjataan yleiseen lohkoketjuun ja varmennetaan tuhansia kertoja. (Bitcoin Transaction 2014.)

### 3 VALUUTAN ARVON MUODOSTUMINEN

Kryptovaluutan arvoon pätevät samat säännöt kuin mihin tahansa muuhunkin valuuttaan. Valuutat ovat ennen kaikkea vaihdon välineitä, joiden arvolla ei ole mitään tekemistä niiden itsensä kanssa. Jokaisen valuutan ja objektin arvo liittyy viime kädessä haluttavuuteen. Rahaa ei haluta koska se on arvokasta, vaan se on arvokasta koska sitä halutaan. (Kallinen & Ruckenstein 2009, 60-61.)

Kryptovaluuttaa voi vaihtaa euroihin, palveluihin ja esineisiin. Se on siis vaihdon väline ja täyttää siten taloudellisesti arvokkaan asian määritelmän. Vaihdossa yhtä asiaa tarjotaan toista asiaa vastaan. Vaihdon molemmat osapuolet hyötyvät tästä, molemmat saavat asian mitä he haluavat. Todellinen arvo syntyy tarpeeksi usean halusta omistaa kryptovaluutta. (Kallinen & Ruckenstein 2009, 62.)

Määritelmän mukaan raha tarjoaa arvostuksille mittatikun. Rahan voi jakaa lähes loputtoman pieniin yksiköihin ja siten se antaa helpon tavan tasapainottaa suorite ja vastike. Koska rahaa voi käyttää lähes mihin tahansa, molemmat osapuolet saavat täsmälleen mitä he haluavat. Raha on siis vaihdettavuuden puhdas muoto. Kryptovaluuttojen ainoa kompastuskivi toistaiseksi on luottamuksen puute. Osapuolten tulee luottaa että vaihdossa käytetty symbolinen arvo säilyttää vaihdettavuutensa ja arvonsa myös tulevaisuudessa. (Kallinen & Ruckenstein 2009, 62-63)

Niin kauan kuin esimerkiksi bitcoineja halutaan, tulee niillä myös olemaan arvoa. Tällä hetkellä arvostus on korkealla mikä näkyy valuutan korkeana arvona. Kryptovaluutat tarjoavat joitakin etuja perinteisiin valuutoihin nähden. Mielestäni tämä antaa tiettyä varmuutta valuutan arvon säilymiseen tulevaisuudessa.

## 4 KRYPTOVALUUTAN HENKILÖKOHTAISET SÄILYTYSTAVAT

Kuten aikaisemmin on kerrottu, kryptovaluuttaa säilytetään virtuaalisessa lompakossa, joka koostuu yksityisestä ja julkisista avaimista. Mikäli aikoo sijoittaa kryptovaluuttaan, ensimmäinen tehtävä on hankkia säilytyspaikka ja luoda turvallinen varmuuskopio yksityisavaimesta. Virtuaalilompakoista on olemassa erilaisia versioita, jotka toimivat hieman eri tavoin. (Bittiraha.fi 2014b.)

### 4.1 Paperilompakko

Paperilompakko on tietoturvasta huolestuneelle varmin vaihtoehto. Kun yksityinen avain on olemassa ainoastaan paperiversiona, on sen varastaminen mahdotonta verkon kautta. Helpoin tapa luoda bitcoin-paperilompakko on generoida sellainen selainpohjaisella ohjelmalla osoitteessa: <https://www.bitaddress.org>. Generointi tapahtuu liikuttelemalla hiirtä satunnaisesti (kuva1). Hiiren tuottama satunnainen data parantaa lompakon turvallisuutta. Sivusto kannattaa ladata koneelle ja suorittaa generointi verkosta irroitettuna. Luotu paperilompakko on helppo tulostaa tai kirjata paperille. (Bittiraha.fi 2014c.)



Kuva 1. Bitcoin paperilompakon generointi.

Muilla valuutoilla on löydettävissä vastaavia selain tai työpöytäpohjaisia ohjelmistoja yksityisen ja julkisten avainten generointiin. Teoreettisesti on mahdollista että ohjelma generoi jo käytössä olevan yksityisavaimen, mutta tämän todennäköisyys on äärettömän pieni. (Bittiraha.fi 2014c.)

## 4.2 Lompakko tietokoneella

Kryptovaluutan säilyttämiseen voi luoda myös lompakon tietokoneen kovalevylle. Näitä lompakoita on kahdenlaisia. Salasanalla suojattu ja kryptattu lompakko tarjoaa helpon käytettävyyden kohtalaisella turvallisuudella. Koska tällainen lompakko on yleensä käytössä olevalla tietokoneella, tulee koneen tietoturvan olla kunnossa. Koneelle luotavan lompakon voi tehdä usealla bitcoin-ohjelmistolla. Esimerkiksi ensimmäinen koskaan julkaistu bitcoin-ohjelmisto Bitcoin-Qt on hyvä vaihtoehto. (Bittiraha.fi 2014b.)

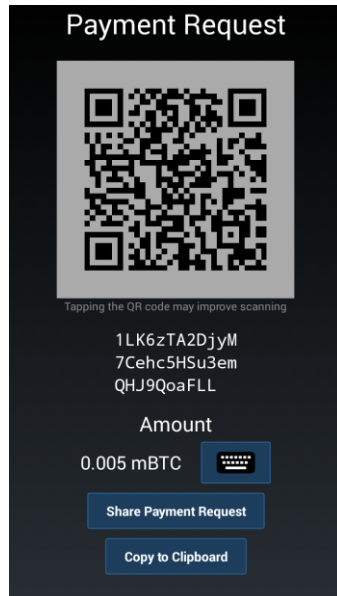
Varmempi ratkaisu on luoda kyseinen lompakko koneelle, joka ei koskaan ole verkossa. Hyvä vaihtoehto tähän on Armory-ohjelmisto. Ohjelmisto tarjoaa yksityiskohtaiset ohjeet verkosta irroitettun lompakon luontiin ja rahansiirtoihin muistitikun avulla. (Bittiraha.fi 2014b.)

Ohjelmisto ladataan verkosta, minkä jälkeen se asennetaan haluttuun kohteeseen. Kun tämän kohteen pitää erillään verkosta, voi rahoja pitää lähes yhtä turvattuina kuin paperilompakossa. (Bitcoinarmory 2014.)

### 4.3 Lompakko puhelimessa

Bitcoin valuuttaa voi myös säilyttää älypuhelimella. Mobiililompakko toimii kryptattuna puhelimen muistissa ja useimmat ohjelmat osaavat luoda paperisen varmuuskopion. Sovellus kannattaa myös suojata salasanalla luvattoman käytön estämiseksi. Tähän sopii esimerkiksi Mycelium Bitcoin Wallet, jonka saa Android-järjestelmälle. Mobiililompakon etuina ovat helppous ja nopeus. (CoinDesk 2014a.)

Lompakko on yleensä mukana ja maksaminen onnistuu NFC yhteydellä tai QR-koodin avulla suoraan toiseen mobiililompakkoon. Vastaanottaja tarjoaa julkista avaintaan, jonka valuutan lähettäjä lukee puhelimensa kameralla (kuva 2). QR-koodin ansiosta kirjoitusvirheen mahdollisuus vastaanottajan osoitteessa poistuu. Mikäli puhelin hajoaa tai se varastetaan, voi lompakon palauttaa paperisesta varmuuskopiosta. Mobiililompakon turvallisuus onkin kiinni pitkälti salasanan turvallisuudesta sekä käyttäjän tekemän varmuuskopion varastoinnista. Käytetyt salaukset ovat poikkeuksetta erittäin vaikeita murtaa. (Blockchain 2014)



Kuva 2. Mycelium: rahan vastaanotto.



## 5 VERKKOPANKKI

Kryptovaluuttaa voi myös säilyttää verkkopankissa tai selainpohjaisessa lompakossa. Tällöin lompakon yksityisavain annetaan ulkopuolisen tahon säilytettäväksi. Peruskäyttäjälle verkkolompakko on helpoin vaihtoehto. Esimerkiksi [easywallet.org](http://easywallet.org) luo automaattisesti sivustolle mentäessä bitcoin-lompakon. Tähän lompakkoon pääsee käsiksi ainoastaan ensi kertaa sivuston luomalla url-osoitteella. Mikäli tämän osoitteen hukkaa on kyseiseen osoitteeseen säilöttyjen bitcoinien käyttäminen mahdotonta. Verkkolompakon etuna on hyvä saavutettavuus ja käytön aloittamisen helppous. Monet isommat palveluntarjoajat myös mahdollistavat kaupankäynnin eri kryptovaluuttojen ja perinteisten valuuttojen välillä. (Bittiraha.fi 2014d.)

Selainpohjainen lompakko on kaikkein herkin ulkoisille uhkatekijöille. Kun käyttäjällä ei ole käytössään oman lompakkonsa yksityisavainta, lompakon turvallisuus riippuu lähes täysin palveluntarjoajan luotettavuudesta. Mikäli palveluntarjoaja kohtaa tekninen vika tai hakkerointi voivat säilötyt rahat olla menetetty. Moni palveluntarjoaja ottaa myös pientä maksua tehdyistä bitcoin siirroista. (Browser-based wallet 2014.)

Esimerkkinä pahasta ongelmasta verkkopankin kohdalla on käytetty salaus. Useimmat verkkosivut käyttävät OpenSSL salaustekniikkaa. Keväällä 2014 ilmennyt heartbleed-haavoittuvuus kyseisessä salaustekniikassa koski useimpia tunnetuista kryptovaluutta-palveluntarjoajia. Tiedossa ei ole menetettyjä lompakkoja kyseisen haavoittuvuuden takia, mutta riski kyseisessä tapauksessa oli todellinen. (Bualang 2014.)

## 6 VALUUTAN HANKKIMINEN

Kaikki kryptovaluutat syntyvät louhintaprosessista. Uuden valuutan synnyn määrää kaava, joka on jokaisella kryptovaluutalla uniikki.

Yksi tapa hankkia kryptovaluuttaa onkin siis valjastaa koneensa osaksi valuuttaverkkoa suorittamaan siirtojen laskentaa. Tämä vaatii kuitenkin jonkin verran osaamista sekä selvitystyötä. Valuutan hankkiminen louhimalla on hidas prosessi. Lisäksi laskennan kuluttaman sähkönsä vuoksi louhinta voi olla jopa tappiollista. (Startbitcoin 2014a). Louhimisen kannattavuutta voi laskea, mikäli tietää paikallisen sähkönsä hinnan sekä tuntee oman tietokoneensa kokoonpanon (Startbitcoin 2014b).

Paljon helpompi tapa valuutan hankkimiseen onkin ostaa sitä suoraan joko siirtoja välittävältä taholta tai suoraan toiselta henkilöltä. Suosittu tapa bitcoinien hankkimiseen on tavaroiden myyminen. Valitettavasti usein myydyt tavarat ovat laittomia, kuten huumeita, johtuen kryptovaluutan anonymistisestä luonteesta. Kuitenkin yhä useampi tunnettu yksityisille tarkoitettu kauppapaikka sallii myös bitcoin-maksujen vastaanottamisen. (Startbitcoin 2014c; BBC 2013.)

Bitcoinien ostamiseen tutustutaan paremmin erillisessä empiirisessä osiossa myöhemmässä vaiheessa.

### **Kryptovaluutan louhiminen**

Louhiminen voi tapahtua joko täysin itsenäisesti omalla koneella tai yhteisössä. Yhteisössä hyöty jaetaan lohkon ratkaisemiseen annetun työn mukaisesti. Itsenäisesti louhiessa hyöty jää täysin itselle eikä kukaan ota siirtopalkkioita välistä. Tämä vaatii kuitenkin paljon osaamista ja on erittäin hidasta. (Cryptocurrencies 2014.)

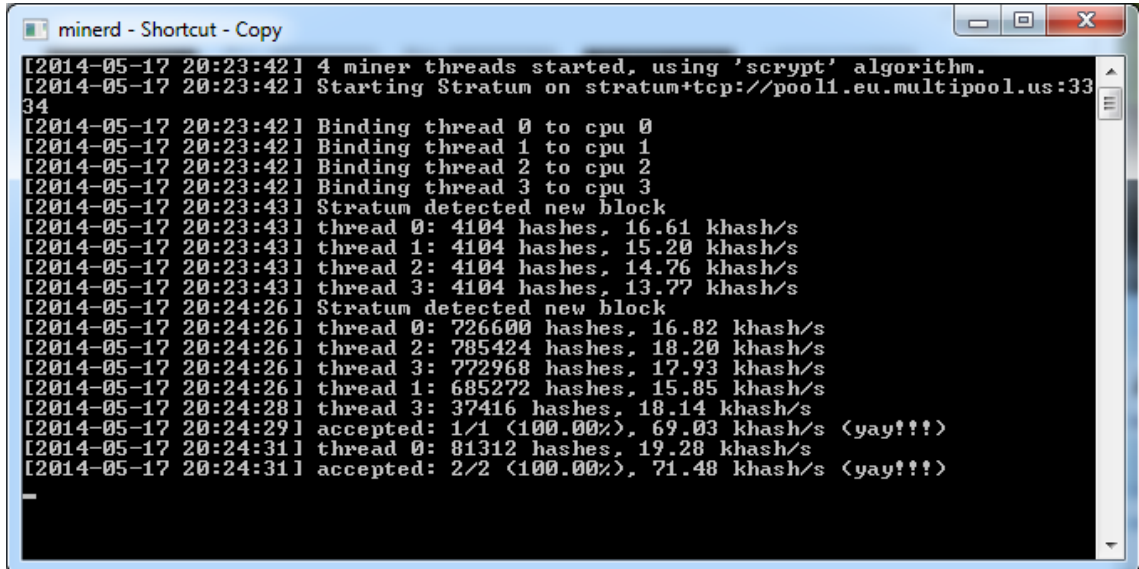
Yhteisölouhinnassa suoritetaan yksittäisten siirtojen laskentaa kunnes yhteisö saa ratkaistua koko lohkon. Louhinta on kohtalaisen helppoa aloittaa. Myös

tulosta saa myös huomattavasti nopeammin, johtuen yhteisön suuremmasta laskentatehosta. Louhinta lähtee rekisteröitymisestä johonkin yhteisöön eli pooliin. Esimerkissä käytetään sivustoa [www.multipool.us](http://www.multipool.us). (Pooled mining; Multipool 2014a.)

Kun lähdetään louhimaan kryptovaluuttaa, hankitaan ensiksi siihen suunniteltu ohjelma. Laskentaa voi suorittaa prosessorilla, näytönohjaimella sekä joissakin tapauksessa tarkoitusta varten suunnitelluilla laskentayksiköillä. Jokaiselle tekniikalle löytyvät omat ohjelmat. Lisäksi joillakin ohjelmilla on mahdollista suorittaa laskentaa useita eri tekniikoita käyttäen. Yksi helpoimmista vaihtoehdoista on Guiminer, jolla pystyy käyttämään laskennassa sekä prosessoria että näytönohjainta (GUIMiner 2014). Myös yhteisölouhinta sekä yksittäin suoritettu ovat molemmat mahdollisia Guiminerin avulla. (Startbitcoin 2014a.)

Kun louhintaohjelma on hankittu, tulee päättää mihin yhteisöön haluaa liittyä. Eri yhteisöillä on hieman erilaiset palkitsemismenetelmän. Käyttäjän kannattaakin tutustua mikä sopii omaan käyttöön parhaiten. Liittyminen tapahtuu kirjautumalla yhteisön verkkosivuilla. Liittymisen jälkeen käyttäjä saa tunnukset joiden avulla pääsee mukaan louhintaprosessiin. (Pooled mining 2014.)

Useimmat yhteisöt tarjoavat selkeät ohjeet asetuksille, jotka tulee syöttää louhintaohjelmistoon. Esimerkiksi Multipool ohjeistaa kirjaamaan seuraavat tiedot litecoin louhintaohjelmaan; `stratum+tcp://pool1.eu.multipool.us:3334` username.n password. Komento koostuu käytetystä protokollasta, yhteisön osoitteesta sekä kyseisen valuutan sivustolla käyttämästä portista. Lopuksi tulee kirjatuksi vielä käyttäjätunnus, käytetyn louhijan numero, joka on kirjattu n:llä sekä salasana. Louhintaohjelma antaa käydessään tietoa toteutuvasta edistyksestä (kuva 3). (Pooled mining; Multipool 2014b.)



```
[2014-05-17 20:23:42] 4 miner threads started, using 'scrypt' algorithm.
[2014-05-17 20:23:42] Starting Stratum on stratum+tcp://pool1.eu.multipool.us:3334
[2014-05-17 20:23:42] Binding thread 0 to cpu 0
[2014-05-17 20:23:42] Binding thread 1 to cpu 1
[2014-05-17 20:23:42] Binding thread 2 to cpu 2
[2014-05-17 20:23:42] Binding thread 3 to cpu 3
[2014-05-17 20:23:43] Stratum detected new block
[2014-05-17 20:23:43] thread 0: 4104 hashes, 16.61 khash/s
[2014-05-17 20:23:43] thread 1: 4104 hashes, 15.20 khash/s
[2014-05-17 20:23:43] thread 2: 4104 hashes, 14.76 khash/s
[2014-05-17 20:23:43] thread 3: 4104 hashes, 13.77 khash/s
[2014-05-17 20:24:26] Stratum detected new block
[2014-05-17 20:24:26] thread 0: 726600 hashes, 16.82 khash/s
[2014-05-17 20:24:26] thread 2: 785424 hashes, 18.20 khash/s
[2014-05-17 20:24:26] thread 3: 772968 hashes, 17.93 khash/s
[2014-05-17 20:24:26] thread 1: 685272 hashes, 15.85 khash/s
[2014-05-17 20:24:28] thread 3: 37416 hashes, 18.14 khash/s
[2014-05-17 20:24:29] accepted: 1/1 (100.00%), 69.03 khash/s <yay!!!>
[2014-05-17 20:24:31] thread 0: 81312 hashes, 19.28 khash/s
[2014-05-17 20:24:31] accepted: 2/2 (100.00%), 71.48 khash/s <yay!!!>
```

Kuva 3. MinerD litecoin louhinta.

Yhteisölouhinta kartuttaa kryptovaluuttaa lähes poikkeuksetta yhteisön sivustolle. Tähän kertyvä arvo kannattaakin siirtää mahdollisimman nopeasti omaan lompakkoon. Näin varmistetaan valuutan säilyminen yhteisön kaatuessa. (Bitcoinmining.com 2014)

## 7 KRYPTOVALUUTAN KÄYTTÄMINEN

Kryptovaluuttoja käytetään paitsi sijoitustuotteina myös vaihdon välineinä kuten perinteisempiäkin valuuttoja. Käyttäminen tapahtuu siirtämällä valuuttaa omasta virtuaalilompakosta toiseen lompakkoon. Käytännössä vastaanottaja tarjoaa oman julkisen osoitteensa, johon maksaja suorittaa pyydetyn suuruisen siirron. (Smithers 2013.)

Bitcoin eniten käytettynä kryptovaluuttana on myös hyväksytty useimmissa paikoissa. Pääosa bitcoin-kaupasta tapahtuu verkossa. Tänä päivänä on mahdollista ostaa lähes mitä tahansa sijoituspalveluista taiteeseen. (Trade). Myös normaalien laskujen maksaminen onnistuu suomalaisessa Bittiraha.fi palvelussa (Bittiraha.fi 2014g).

Kuten aikaisemminkin on kerrottu, ovat mobiililompakot erittäin käytännöllisiä virtuaalivaluutan käyttämisessä. Mukana kannettava rakaisu tarjoaa vapauksia käytön suhteen. (Mycelium.com 2014.)

Verkosta löytyy useita listoja paikoista missä käyttää bitcoineja. Bitcoin-käyttäjän kannattaakin aika ajoin tarkistaa tilanne. Suoran käytön etuna on välikäsiä poistuminen ketjusta. Tämä laskee mahdollisia kustannuksia. (Smithers 2013.)

Bitcoin käyttäjän kannattaa myös seurata valuutan arvon muutoksia ja varmistaa, että maksettu hinta vastaa senhetkistä valuutan arvoa. Mikäli myyjä ei päivitä hintaansa valuutan arvon muuttuessa, voi ostaja päätyä maksamaan rajua ylihintaa. Myös skenaario jossa tuotteen saa tavallista halvemmalla on mahdollinen. (Smithers 2013.)

### **Käyttöriskit**

Kryptovaluutan käyttäminen on pääosin jopa turvallisempaa kuin perinteisen paperirahan. Perinteisen lompakon voi varastaa kuka tahansa eikä sisältöä, eli fyysisiä rahoja voi suojata mitenkään. Tästä syystä perinteistä rahaa kannetaankin harvoin isoja summia mukana. (Bitcoin.org 2014.)

Myöskään eniten käytetyn kryptovaluutta-lompakon sisältö kannattaa pitää kohtalaisen pienenä. Näin haavoittuvin säilytyspaikka ei tee isoa vahinkoa talouteen sisällön päätyessä vääriin käsiin. (Bitcoin.org 2014.)

Isommat määrät suositellaan säilytettäväksi lompakossa, jonka julkinen avain on joko ainoastaan paperilla tai vähintään kiintolevyllä, joka ei ole verkkoon yhteydessä. (Bitcoin.org 2014.)

Mobiililompakot ovat mahdollisia kohteita varkaudelle kuten perinteiset lompakot. Etuna perinteiseen lompakkoon on kuitenkin mahdollisuus kryptata eli suojata lompakko vahvalla salasanalla. Näin mahdollinen varas ei voi hyödyntää saalistaan mitenkään. Lisäksi oikein tehty yksityisavaimen varmuuskopio mahdollistaa sisällön palauttamisen oikealle haltijalle. Perinteisellä valuutalla tämä ei ole mahdollista. (Bitcoin.org 2014)

Isoimmat riskit käytössä ovatkin varkaus, väärä osoite valuutansiirrossa sekä mahdollinen ylihinnan maksaminen tuotteesta. Käyttäjän ottaessa nämä huomioon kryptovaluutan käyttäminen on hyvin turvallista.

## 8 TURVALLISUUS SIOITTAJALLE

Virtuaalivaluutan turvallisuudessa on useita eri puolia. Amores & Paganini jakavat riskit seuraaviin: käyttöriskit eli mahdollinen varkaus tai toimintahäiriö, lailliset riskit, valuutan arvostukseen liittyvät riskit ja palveluntarjoajan luotettavuusriski (Paganini & Amores 2013. 110.)

Teknisiä riskejä ei tässä työssä tarkemmin kuvailla. Kryptovaluutat perustuvat hajautettuun laskentaan. Niiden toiminnallinen varmuus on todella hyvä, niin kauan kuin valuutalla on käyttäjiä sekä ylläpitäjiä. (Paganini & Amores 2013. 240.) Tässä työssä keskitytään tarkemmin valuutan turvalliseen käyttöön sekä sijoittajaa koskeviin riskeihin.

### **Sijoittajan riskit**

Kryptovaluuttaan sijoittaminen on äärimmäisen korkean riskin sijoittamista. Kryptovaluutan arvo heilahtelee käytännössä hallitsemattomasti ja niiden laillisuuskin on hieman harmaalla alueella. Anonyymiytensä vuoksi valuuttaa käytetään huomattavissa määrin myös laittomaan toimintaan. Sijoittajan kannattaakin pitää jokaista kryptovaluuttaan sijoittamaansa euroa menetettynä. Näin mahdolliset tappiot eivät tuhoa taloutta. (Hahtela 2014.)

Kryptovaluutan suuret kurssiheilahtelut tarjoavat toki myös mahdollisuuden nopeaan rikastumiseen ostajan ollessa oikeaan aikaan liikkeellä. Tämä vaatii kuitenkin sekä onnea että kiinnostusta seurata kryptovaluuttamarkkinoita ahkerasti. (Hahtela 2014.)

Kuten aikaisemmin on kerrottu, valuutan arvoon vaikuttaa eniten kyseisen valuutan haluttavuus. Iso riski minkä tahansa valuutan kohdalla onkin arvostuksen menetys. (Paganini & Amores 2013. 110.)

Pahin vahinko, mikä on kryptovaluutoille tapahtunut, on tunnetun Mt.Gox.in kaatuminen keväällä 2014. Mt.Gox oli kryptovaluuttoihin keskittynyt pankki sekä välittäjä, jonka kautta tapahtui parhaimmillaan jopa 70% bitcoin-kaupankäynnistä. Virallisten tietojen mukaan Mt.Gox joutui verkkohyökkäyksen

kohteeksi, minkä seurauksena pankilta hävisi yli 400 miljoonan dollarin edestä bitcoineja. (Kelleher 2014.)

Kyseinen katastrofi vahingoitti pahasti bitcoinin uskottavuutta ja syöksi valuutan arvon syöksykierteeseen. Varkauden mahdollistanut haavoittuvuus on sittemmin korjattu, mutta menetetty uskottavuus palautuu todella hitaasti. Riski omien talletusten menettämiseen tällaisessa tapauksessa voidaan poistaa säilyttämällä itse tilin yksityisavainta. (Sag 2014.)

### **Deflaatio**

Yksi isoista riskeistä sekä mahdollisuuksissa esimerkkivaluutta bitcoinin kohdalla on deflaatio. Deflaatio tarkoittaa valuutan arvon hallitsematonta nousua. Bitcoinien syntyminen hidastuu ajan myötä, kunnes lopullinen määrä tulee olemaan noin 21 miljoonaa. Tämä tulee lähestulkoon varmasti aiheuttamaan todella kovan deflaation valuutalle. (Paganini & Amores 2013. 112.)

Kova deflaatio aiheuttaa valuutan käytön hiipumista. Mikäli arvo nousee, eivät valuuttaa omistavat tahot halua kuluttaa sitä arvonnousun takia. Mikäli käyttö kuitenkin hiipuu liikaa deflaation vuoksi, romahtavat valuutan markkinat lopullisesti. Bitcoinien kohdalla käytettävyyttä deflaatiotilanteessa pyritään varmistamaan jaettavuudella alaspäin. (Paganini & Amores 2013. 113-114.)

### **Laiton käyttö**

Anonyymejä kryptovaluuttoja käytetään huomattavia määriä myös laittomaan kaupankäyntiin. Esimerkiksi Silk Road sivustolla myytiin huumeita, aseita sekä muuta laitonta materiaalia bitcoineja vastaan. Kyseisen sivuston kohtaloksi muodostui Yhdysvaltojen hallinnon sitä vastaan suorittamat vastatoimet. Tässä tapauksessa vastatoimet kohdistuivat sivustoon itseensä, mutta olemassa oleva riski on myös itse valuutan kimppuun käymisestä. (Paganini & Amores 2013. 164-166.)

Mahdolliset valtaapitävien hyökkäykset kryptovaluuttoja vastaan voivat vahingoittaa valuutan arvoa todella vakavasti. Tällainen hyökkäys ei kuitenkaan



todennäköisesti kykene kaatamaan valuuttaa koska virtuaalivaluuttoja ei ole sidottu yhteenkään laitokseen tai valtioon. Laajamittainen hyökkäys olisi täten helppo ennakoida laajuutensa vuoksi. Valuutan realisointia kannattaakin harkita ennen toimenpiteitä. (Paganini & Amores 2013. 165-166.)

## 9 KRYPTOVALUUTAN OSTAMINEN

Eurojen vaihtaminen kryptovaluuttaan on ylivoimaisesti helpoin tapa sijoittaa niihin. Esimerkiksi bitcoin-taloudesta löytyy kymmeniä vaihtopörsssejä jotka tarjoavat mahdollisuuksia ostaa bitcoineja. Eri pörssien välityspalkkiot ja vaihtokurssit vaihtelevat jonkin verran. Käyttäjän kannattaakin vertailla, mikä on edullisin luotettava vaihtoehto. (Bittiraha.fi 2014e.)

Suomalaisille luonteva paikka ostaa bitcoineja on kotimainen Bittiraha.fi bitcoin-pörssi. Kyseinen sivusto ei ole edullisin mahdollinen paikka, mutta kotimaisuutensa asiasta mahdollisessa ongelmatapauksessa reklamaatiot onnistuvat huomattavasti helpommin. (Bittiraha.fi 2014e.)

Ostotapahtumassa Bittiraha.fi sivustolla käyttäjä antaa ostosumman euroissa. Sivusto antaa arvion kertyvälle bitcoin-määrälle senhetkisen kurssin mukaan. Koska osto tapahtuu sopivan lähteen löydyttyä, voi todellinen määrä poiketa arviosta kurssin ehtiessä muuttua. Esimerkissä ostetaan 20 euron edestä bitcoineja arviokurssilla joka oli voimassa 4.6.2014 kello 10.50 (kuva 4). Tärkeää on varmistaa julkisen bitcoin-osoitteen olevan oikein. Toteutuneiden siirtojen peruuttaminen ei ole mahdollista. Yleisen turvallisuuden vuoksi käyttäjän on myös hyvä varmistaa salattu yhteys. Salatun yhteyden näkee parhaiten url-osoitteen alussa olevasta https-protokollatiedosta. (Bittiraha.fi 2014e; Bittiraha.fi 2014f)



Kuva 4. Bitcoin ostotapahtuma. (<https://bittiraha.fi/bitcoin/buy>).

Bittiraha-sivusto tiedustelee ostajan henkilöllisyydestä. Mikäli käyttäjä ostaa kyseisestä pörssistä ja haluaa säilyttää anonyymiteetin, kannattaa ostetut rahat siirtää mahdollisimman pian eteenpäin toiseen lompakkoon. Henkilötietojen kyselyllä on hyvänä puolena helppo yhteydenpito ongelmatapauksissa. Lopuksi tilaus vahvistetaan. Maksu onnistuu kaikkien yleisimpien Suomessa toimivien pankkien verkkopalveluiden kautta sivuston antamien maksutietojen avulla (kuva 5). (Bittiraha.fi 2014f)

https://bittiraha.fi/bitcoin/buy

Etusivu Bittipörssi Laskupalvelu BTC Store Yrityksille Forum UKK Tiedotteet

**Bittiraha**

Bitcoin Is Having One Of Its Strongest Periods Ever (via @BusinsiderAU) <http://t.co/Qjv2EGBbt0> @Bittirahafi about 21 hours ago

Kurssitiedot  
4.6.2014  
1 BTC = ...  
Os...

### Maksutiedot

Etusivu

Kiitos tilauksesta! Tässä maksutiedot. Tilausvahvistus lähetetään sähköpostiisi.

Saaja: *Prasos Oy*  
Tili: *FI14 3636 3010 2113 57*  
Summa: *20,00* EUR  
Viite: *9008538070*

Virtuaaliviivakoodi: *41436363010211357000020000000000000000900853807014060400*

BIC/SWIFT -koodi: TAPIFI22 (tämä tarvitaan, jos maksat ulkomaisesta pankista)

Verkkopankkien pikalinkit  
*Nordeasta, Osuuspankista ja Tapiolasta tehdyt maksut ohjautuvat meille samantien*

**Mikä on Bitcoin**

- Aloita tästä!
- Mitä bitcoineilla voi tehdä?
- Miten Bitcoinia käyttää?
- Miten voin hankkia Bitcoinia?
- Karttapalvelu
- Bitcoinin tekninen ku...
- Bitcoin ja verotus
- Usein kysytyt kysymykset

**Forumilla nyt**

- Vs: Worldcoin
- Vs: Blockchain wallet
- Vs: Lucrativa.biz
- Vs: Lucrativa.biz

Kuva 5. Maksutapahtuma. (<https://bittiraha.fi/bitcoin/buy>).

## 10 KRYPTOVALUUTAN REALISOINTI

Sijoittajan on hyvä tietää koska myydä sijoituksensa. Hyvän sijoittajan kannattaa seurata säännöllisesti markkinoiden kehittymistä ja myydä omistuksensa kun saatavilla on vähintään itselle asetetut tuotto-odotukset. Tämä pätee kaikkiin sijoituksiin aina osakkeista keräilyesineisiin. (Coleman 2014.)

Sijoittajan on hyvä myös muistaa mahdolliset veroseuraamukset, jotka syövät tuottoja. Myös hintojen laskiessa rajusti kannattaa harkita pikaista myymistä tappion minimoimiseksi. Pahimmassa tapauksessa sijoittaja voi menettää koko sijoituksensa. Kryptovaluutta korkean riskin sijoituksena on kuitenkin hieman poikkeava tässä kohdassa. Kryptovaluutan kurssi voi heilahdella todella rajustikin ja sijoituksia kannattaa alusta alkaen pitää menetettyinä. Tästä syystä myymistä kannattaa miettiä tarkkaan myös kurssin romahtaessa. (Coleman 2014.)

Bitcoinien kohdalla myymistä kannattaa harkita myöskin todennäköisen deflaation vuoksi. Valuutan syntyminen hidastuu ajan myötä, mikä todennäköisesti johtaa arvon nousemiseen. Lisäksi yhä useampi taho ottaa vastaan maksuna bitcoineja. Tämä saattaa tulevaisuudessa mahdollistaa valuutan käyttämisen jokapäiväisenä maksuvälineenä. Onkin siis mahdollista, ettei virtuaalivaluuttaa tarvitse koskaan realisoida perinteiseen valuuttaan. Tämä on sikäli järkevää, että käyttäjän myydessä omistustaan välittäjä ottaa aina oman osuutensa tuotosta. (Bitcoinrati 2014.)

### **Tavat realisoida**

Kryptovaluutan realisointi tapahtuu myymällä valuuttaa ostajalle jotakin toista hyödykettä vastaan. Yleensä kaupankäynti tapahtuu käyttövaluutasta, kuten euroista tai dollareista, mutta myöskin vaihto tavaraan tai muihin sijoituskohteisiin on mahdollista. Karkeasti ottaen realisointi tapahtuu joko verkossa tai henkilökohtaisesti tapaamalla ostaja. Näissä molemmissa on omat etunsa sekä huonot puolensa. (Coindesk 2014b.)

## **Henkilökohtainen myynti**

Henkilökohtainen myyminen suoraan ostajalle on varmin tapa kaupankäyntiin. Kun maksun saa heti käteisellä voi olla huoletta sen suhteen. Henkilökohtaisessa myynnissä oikean hinnan sopiminen on myyjän ja ostajan välinen asia. Ongelmana on kuitenkin ostajan löytäminen sekä luotettavuus. Myyjälle on olemassa joitakin verkkoyhteisöjä joissa voi mainostaa olevansa halukas myymään suoraan ostajalle. Etuna suorassa myynnissä on välittäjän palkkion poistuminen. (Coindesk 2014b.)

## **Verkossa myynti**

Verkossa myyminen on huomattavasti yleisempää kuin kasvotusten käyty kaupankäynti. Verkossa myyjän täytyy yleensä rekisteröityä myyjäksi sivustolle, joka välittää tai ostaa suoraan kryptovaluuttaa. Myyminen kryptovaluuttaa ostavalle verkkosivulle on nopein tapa saada kauppa suoritettua. Suora myyminen välittäjälle ei kuitenkaan välttämättä kannata, mikäli hakee parasta mahdollista hintaa. (Coindesk 2014b.)

Suomalaisella Bittiraha.fi-sivustolla on myös mahdollista asettaa minimihinta ja odotusaika. Kauppa ei toteudu, mikäli myyjä ei saa asettamaansa minimihintaa odotusajan sisällä. Tällöin sivusto palauttaa lähetetyt bitcoinit myyjän antamaan osoitteeseen. Esimerkissä palveluun on syötetty muut tiedot paitsi myyjän tilinumero (kuva 6). Tämän vaiheen jälkeen sivusto kysyy myyjän tiedot ja lopuksi sivusto lähettää maksuohjeet sekä sähköpostiin että tekstiviestillä (Bittiraha.fi 2014h.)



**Bittiraha** 

Uusi #kurssiraportti julkaistu! 400 dollaria edelleen haasteena. <https://t.co/bQF...>  
 #bitcoin #bittiraha  
 @Bittirahafi 4 days ago

## Bitcoinien myynti: Vaihe 1

Tervetuloa *Bittipörssiin!* Tämän yksinkertaisen lomakkeen avulla voit myydä bitcoineja. Vaihdamme bitcoineja euroiksi joko muiden asiakkaidemme tai Bitstamp-pörssin kautta, riippuen siitä miten saamme kaupalle parhaan hinnan.

Bitcoin-siirron suorittamiselle annamme viikon aikaa. Vastaanotettuamme maksun, käsittelemme tilauksesi mahdollisimman nopeasti. Palvelun ehdot voit lukea [Bittipörssin pääsivulta](#).

*Mikäli lähettämäsi summa hieman eroaa ilmoittamastasi summasta, tämä ei haittaa. Käsittelemme tilauksesi lähetetyn summan mukaan.*

Summa (bitcoineina) \*  Myyntisumma 0.02 BTC. Kulu 0 BTC.

Euromäärä (arvio)  Arvioitu kurssilla 277.71 EUR/BTC 

IBAN-tilinumero \*  

Haluan asettaa tilaukselleni minimihinnan

Tilausasetukset

Minimihinta (EUR/BTC) \*  Toteutuessa saat vähintään 4.66 EUR 

Odotusaika \*  

Bitcoin-osoitteesi \*  

Kuva 6. Bitcoinien myynti. (<https://bittiraha.fi/myy>).

Verkossa tapahtuu myös suoraan ostajalta myyjälle tapahtuvaa kaupankäyntiä, joka vastaa hieman kasvokkain käytyä kauppaa. Tällaisessa kaupankäynnissä ostaja ja myyjä kohtaavat kaupankäyntiin tarkoitettussa verkkoympäristössä. Esimerkiksi Amazon-verkkokauppa tarjoaa mahdollisuutta myydä bitcoineja. Etuna on ostamisen helppous kansainvälisen pankkikortin avulla. Sivustojen keräämät maksut saattavat kuitenkin olla kohtuuttoman isoja. (Coindesk 2014b.)

## **Rekisteröitynä myyminen**

Suoraa myymistä kannattavampi vaihtoehto onkin rekisteröityä myyjäksi kauppasivustolle. Tässä tapauksessa myyjä menettää toki osan yksityisyydestään. Useimmat sivustot ovat kuitenkin erittäin luotettavia. (Coindesk 2014b.)

Etuna on mahdollisuus asettaa automaattinen tavoitehintaa. Kun ostaja tarjoaa tavoitehinnan mukaista maksua, kauppa toteutuu automaattisesti. Myös kauppasivustot vievät oman osuutensa kaupasta. Mahdollisesti korkeamman kauppahinnan takia summa onkin usein suhteessa pienempi. (Coindesk 2014b.)



## 11 VEROSEURAAMUKSET JA LAINSÄÄDÖNTÖ

Virtuaalivaluutat eivät ole Suomessa virallista valuuttaa. Täten kirjanpitovelvolliset eivät ole velvollisia hyväksymään virtuaalivaluuttaa. Virtuaalivaluutan käyttäminen on kuitenkin laillista mikäli sekä ostaja että myyjä ovat valmiita hyväksymään kaupan. (Verohallinto 2013.)

Käytettäessä kryptovaluuttaa kaupankäynnin välineenä, ne ovat verottajalle erikseen määrittelemättömän käyttäjien välisen sopimus. Tällaisessa sopimuksessa menetykset eivät ole vähennyskelpoisia. Sijoittajan on hyvä tiedostaa tämä miettiessään riskejä virtuaalivaluutaan sijoittamisessa. (Verohallinto 2013)

Virallisesti hyväksytyt ja virtuaalivaluutan vaihdossa verottaja suhtautuu omaisuuden tuottoon pääomatulona. Myös muut tulot ja myyntivoitto ovat pääomatuloa. Virtuaalivaluutan sopimusluonteen takia tuloverolaki koskien luotusvoittoja. (Verohallinto 2013.)

Louhimisessa syntynyt valuutta ei ole varallisuuden kerryttämistä vaan muuta kuin pääomatuloa. Louhinnalla hankittu virtuaalivaluutta on siten ansiotuloa. Louhinnasta saatu tulo siirtyy verotettavaksi valuutan siirtyessä käyttäjän hallintaan. Verotusarvona käytetään senhetkistä yleisesti hyväksyttyä kurssia. (Verohallinto 2013.)

Elinkeinoharjoittajan vastaanottama maksu käsitellään myös senhetkisen vaihtokurssin mukaan verotettavana elinkeinotoiminnan tulona. Erona elinkeinoharjoittajan ja yksityishenkilön välillä on virtuaalivaluutan myynnistä aiheutuneen tappion vähennyskelpoisuus. (Verohallinto 2013.)

Virtuaalivaluutan käyttäminen on hetki, jolloin arvonnousu realisoituu verotettavaksi tuloksi. Suomessa verovelvollinen on henkilö kenelle myyntivoitto realisoituu. Ilmoitusvelvollisuus verohallinnolle kuuluu kyseiselle henkilölle. Tulo realisoituu riippumatta siitä tapahtuuko myynti Suomeen vai ei. Veroilmoitus

tulee tehdä sen vuoden veroilmoituslomakkeella, jolloin myyntivoiton saaminen on tapahtunut. (Verohallinto 2013.)

Virtuaalivaluutat ovat luonteeltaan anonyymejä. Niiden valvominen on siis erittäin vaikeaa. Lisäksi on yksinomaan verovelvollisen vastuulla pitää kirjaa ostetuista ja louhimalla hankituista yksiköistä. (Verohallinto 2013.)

Maailmalla verottajan suhtautuminen virtuaalivaluuttaan vaihtelee suuresti maittain. Monella taholla ei ole tarpeeksi tietotaitoa ottaa kantaa näiden vaihtoehtotalouksien verottamiseen. Myös rajojen ylitse käytävä kauppa on ongelmallista. Lähtokohtana on toimiminen sen maan lainsäädännön mukaan, missä kaupankäyjät asuvat. (Paganini & Amores 2013. 150.)

Esimerkiksi Yhdysvaltojen lainsäädäntö virtuaalivaluuttojen kohdalla on jopa Suomen vastaavaa monimutkaisempi. Lähtökohtaisesti virtuaalivaluutta on omistusta eikä valuuttaa. Kuitenkin myyntivoittoa kohdellaan verotettava tulona. Poikkeuksia on kuitenkin useita. Tippinä tai lahjana saatu virtuaalivaluutta on tiettyyn pisteeseen asti verovapaata. (Selkis 2014.)

Virtuaalivaluutat eivät täytä kaikkia lain asettamia maksuvälineen tai valuutan tunnusmerkkejä. Suomessa kyseisten vaihdon välineiden käyttö on kuitenkin täysin laillista. Käyttäjää on ilmoitusvelvollinen verottajalle, mikäli tämä hyötyy taloudellisesti. (Suomen pankki: Bitcoin ei ole oikea valuutta 2014.)

Maailmalla käytännöt vaihtelevat maasta toiseen. Esimerkiksi pohjoismaista Norjassa bitcoin ei kelpaa viralliseksi valuutaksi, joskin yksityinen käyttö on laillista. Tanska puolestaan harkitsee kuinka näitä valuuttoja tulisi kohdella. (Suomen pankki: Bitcoin ei ole oikea valuutta 2014.)

Virtuaalivaluutat ovat olleet koko olemassaolonsa ajan poliittisen keskustelun kohteena. Useat maat harkitsevat niiden käytön kieltämistä, rajoittamista tai valvomista. Tähän mennessä harvat ovat kuitenkaan ryhtyneet toimenpiteisiin. Yleinen ilmapiiri on myönteinen näyden valuuttojen käytölle, niin kauan kuin ne eivät uhkaa vakaita olemassaolevia talousjärjestelmiä. (Paganini & Amores 2013. 151-161.)

## Lainsäädäntö

Useat maat ovat huolissaan virtuaalivaluutoista. Eniten valioiden toimenpiteitä aiheuttavat virtuaalivaluutan käyttötavat. Rahanpesu sekä ase- ja huumekauppa ovat saaneet jotkin valtiot toimiin virtuaalivaluuttoja vastaan. Esimerkiksi Kiina suhtautuu hyvin kriittisesti kryptovaluuttaan. (Pyburn 2014.) Bangladesh puolestaan kieltää bitcoinin rahanpesuun vedoten ja uhkaa käyttäjää välittömällä vankeustuomiolla. (Asiaone Business 2014.)

Lähinnä lainsäätäjät ovat huolissaan kryptovaluuttojen anonyymiyteen liittyvistä ongelmista. Todennäköisesti valuuttoja ei tulla kokonaan kieltämään, mutta tiukempi kontrolli kryptovaluutan käyttöön saattaa olla näköpiirissä. Lainsäätäjät eivät toistaiseksi koe pienen volyymin vaihtoehtotalouksien olevan vakavasti otettava uhka valtioiden ja keskuspankkien kontrolloimille valuutoille. (Coindesk 2014c)

## 12 YHTEENVETO

Tähän työhön kerättyjen tietojen perusteella voidaan päätellä kryptovaluuttojen olevan pääsääntöisesti turvallisia käyttää. Isoimmat riskit koostuvat käyttäjän itsensä tekemistä virheistä sekä luotettavuudesta käytettäessä ulkoista palveluntarjoajaa.

Mikäli varmistetaan, että virtuaalivaluutan säilytykseen tarkoitetun lompakon yksityisavain on hyvässä tallessa, siten ettei ulkopuolisella taholla ole siihen pääsyä, ovat kyseisessä lompakossa olevat varat erittäin varmassa tallessa. Tällaisen lompakon murtaminen on lähestulkoon mahdotonta.

Myöskin valuutan jakaminen pienempään käyttölompakkoon sekä isompiin säilytyslompakoihin lisää turvallisuutta. Varmuuskopioiden tekeminen mahdollistaa menetetyn lompakon palauttamisen.

Sijoittajan puolesta virtuaalivaluutat ovat houkuttelevia erittäin korkean riskin kohteita. Suuret kurssiheilahtelut voivat antaa isonkin tuoton tai vastaavasti tuottaa valtavat tappiot. Niin kauan kuin sijoittaja tiedostaa tämän ja riskeeraa ainoastaan summan, jonka hän on valmis myös menettämään pysyvät tappiot kuitenkin hallittuna.

Sijoittaminen virtuaalivaluuttaan vaatii aktiivista seuraamista. Kurssi saattaa käydä hetkellisesti tavoitehinnassa, jolloin kannattaisi myydä, mutta hidas sijoittaja saattaa menettää mahdollisuutensa

Palveluntarjoajia on sekä luotettavia että arveluttavia. Käyttämällä maalaisjärkeä ja selvittämällä muiden käyttäjien kokemuksia voi kauppaa kuitenkin käydä turvallisesti mielin.

Käyttäjän kannattaa myös seurata lainsäädäntöä ja tiedostaa mahdollisesti muuttuvat ohjeet. Virtuaalivaluutoiden tuotot ovat veronalaista tuloa. Tämä voi tulla yllätyksenä perehtymättömälle käyttäjälle.

Myöskin maakohtaiset erot lainsäädännössä voivat olla isoja. Käyttäjän kannattaakin varmistaa kohdemaansa lainsäädäntö, mikäli aikoo ostaa jotakin virtuaalivaluutalla. Pahimmassa tapauksessa ostetut tuotteet voi menettää valtiolle, mikäli kyseisen valuutan käyttö onkin laitonta kohdemaassa.

Kaikenkaikkiaan virtuaalivaluutat ovat erittäin marginaalisia sekä erittäin epävarmoja kohteita vakavalle sijoittajalle. Mahdollinen deflaatio kuitenkin puhuu sen puolesta, että ainakin pieni summa kannattaa pitää odottamassa kasvua eikä koskaan myydä aivan kaikkea omistamaansa kryptovaluuttaa. Mikäli hyvin käy, tuotto voi olla jopa odotuksia isompi.

## LÄHTEET

Asiaone Business 2014. Bangladesh warns of jail for Bitcoin traders. Viitattu 25.10.2014. <http://business.asiaone.com/news/bangladesh-warns-jail-bitcoin-traders>.

BBC 2013. FBI arrests Silk Road drugs site suspect. Viitattu 15.5.2014. <http://www.bbc.com/news/technology-24373759>.

Bitcoin Transaction. 2014. Bitcoin wiki. Viitattu 22.3.2014. <https://en.bitcoin.it/wiki/Transactions>.

Bitcoin.org 2014. Securing your wallet. Viitattu 1.10.2014. <https://bitcoin.org/en/secure-your-wallet>.

Bitcoinarmory 2014. About Armory. Viitattu 20.4.2014. <https://bitcoinarmory.com/about/about-armory/>.

Bitcoinmining.com 2014. Bitcoin mining pools. Viitattu 1.6.2014. <http://www.bitcoinmining.com/bitcoin-mining-pools/>.

Bitcoinrati 2014. The Bitcoin conversion neccessity – why you may never need to sell Bitcoins. Viitattu 26.10.2014. <http://bitcorati.com/2013/10/24/conversion-necessity-why-you-may-never-need-to-sell-bitcoins/>.

Bittiraha.fi 2014a. Bitcoinin tekninen kuvaus. Viitattu 22.3.2014. <https://bittiraha.fi/content/bitcoinin-tekninen-kuvaus>.

Bittiraha.fi 2014b. Mitä tapoja on säilyttää bitcoineja turvallisesti? Viitattu 19.4.2014, 20.4.2014. <https://bittiraha.fi/content/usein-kysytyt-kysymykset#b15>.

Bittiraha.fi 2014c. Ohjeet paperilompakon luontiin. Viitattu 19.4.2014. <https://bittiraha.fi/content/ohjeet-paperilompakon-luontiin>.

Bittiraha.fi 2014d. Hanki Bitcoin-lompakko. Viitattu 14.5.2014. <https://bittiraha.fi/content/miten-bitcoinia-k%C3%A4ytet%C3%A4%C3%A4n>.

Bittiraha.fi 2014e. Miten voin hankkia Bitcoineja? Viitattu 1.6.2014, 4.6.2014. <https://bittiraha.fi/content/miten-voin-hankkia-bitcoineja>.

Bittiraha.fi 2014f. Bitcoinien osto. Viitattu 4.6.2014. <https://bittiraha.fi/bitcoin/buy>.

Bittiraha.fi 2014g. Maksa laskusi bitcoineilla. Viitattu 27.8.2014. <https://bittiraha.fi/laskupalvelu>.

Bittiraha.fi 2014h. Bitcoinien myynti. Viitattu 26.10.2014. <https://bittiraha.fi/myy>.

Blockchain 2014. Wallet. Viitattu 20.4.2014, 1.10.2014. <https://blockchain.info/wallet>.

Browser-based wallet. 2014. Bitcoin wiki. Browser-based wallet. Viitattu 14.5.2014 . [https://en.bitcoin.it/wiki/Browser-based\\_wallet](https://en.bitcoin.it/wiki/Browser-based_wallet).

Bualang, N. 2014. Cryptocurrency safety concerns in the wake of heartbleed. Crypto Coins Insider. Viitattu 22.10.2014. <http://www.cryptocoinsinsider.com/safety-of-cryptocurrency-amid-heartbleed/>.

Chaum, D. 1998. Blind signatures for untraceable payments. Viitattu 22.3.2014. <http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>.

- CoinDesk 2014a. How to store your Bitcoins. Viitattu 20.4.2014. <http://www.coindesk.com/information/how-to-store-your-bitcoins>.
- Coindesk 2014b. How to sell Bitcoin. Viitattu 26.10.2014. <http://www.coindesk.com/information/sell-bitcoin/>.
- Coindesk 2014c. Is Bitcoin legal? Viitattu 26.10.2014. <http://www.coindesk.com/information/is-bitcoin-legal/>.
- Coleman, H. 2014. When to sell stocks - 6 questions to ask before selling your shares. Money crashers. Viitattu 26.10.2014. <http://www.moneycrashers.com/when-to-sell-stocks-questions-checklist/>.
- Comparison of cryptocurrencies. 2014. Bitcoin wiki. Viitattu 21.11.2014. [https://en.bitcoin.it/wiki/Comparison\\_of\\_cryptocurrencies](https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies).
- Cryptocurrencies 2014. Litecoin LTC mining guide, cpu. Viitattu 15.5.2014. <http://cryptocur.com/litecoin/litecoin-mining/>.
- Gilson, D. 2013. What are Namecoins and .bit domains? CoinDesk. Viitattu 22.3.2014. <http://www.coindesk.com/what-are-namecoins-and-bit-domains/>.
- Grigg, I. 1999. How DigiCash blew everything. Cryptome.org. Viitattu 22.3.2014. <http://cryptome.org/jya/digicrash.htm>.
- GUIMiner 2014. GUIMiner a GPU/CPU Bitcoin miner for Windows based on poclbm. Viitattu 15.5.2014. <http://guiminer.org/>.
- Hahtela, J. 2014. Bitcoin: virtuaaliraha murenee tosielämän haasteissa. Nordea. Viitattu 22.10.2014. [http://newsroom.nordea.com/fi/blogpost/bitcoin-virtuaaliraha-murenee-tosielaman-haasteissa/?doing\\_wp\\_cron=1414594209.1463570594787597656250](http://newsroom.nordea.com/fi/blogpost/bitcoin-virtuaaliraha-murenee-tosielaman-haasteissa/?doing_wp_cron=1414594209.1463570594787597656250).
- Kallinen, T & Ruckenstein, M. 2009. Rahan kulttuuri. Tampere: Juvenes print.
- Kelleher, J. 2014. Bitcoin mass hysteria: The disaster that brought down Mt. Gox. Forbes. Viitattu 22.10.2014. <http://www.forbes.com/sites/investopedia/2014/02/28/bitcoin-mass-hysteria-the-disaster-that-brought-down-mt-gox/>.
- Multipool 2014a. Multipool. Viitattu 16.5.2015. <https://www.multipool.us/>.
- Multipool 2014b. Frequently asked questions. Viitattu 15.5.2014. <https://www.multipool.us/help.php>.
- Mycelium.com 2014. Bitcoin wallet. Viitattu 27.8.2014. <https://mycelium.com/bitcoinwallet>.
- Nakamoto, S. 2014. Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org Viitattu 22.3.2014. <https://bitcoin.org/bitcoin.pdf>.
- Paganini, P. & Amores, R. 2013. Digital virtual currency and Bitcoins. Great Britain: Amazon.co.uk.
- Pooled mining. 2014. Bitcoin wiki. Viitattu 15.5.2014, 16.5.2014. [https://en.bitcoin.it/wiki/Pooled\\_mining](https://en.bitcoin.it/wiki/Pooled_mining).
- Pyburn, G. 2014. Bitcoin legal: taxonomy of regulatory reactions, apac's outlook and potential for BTC-linked derivatives. Insightlegal Asia. Viitattu 26.10.2014. <http://www.insightlegalasia.com/blog/bitcoin-legal-taxonomy-regulatory-reactions-apac%E2%80%99s-outlook-and-potential-btc-linked-derivatives>.

- Sag, A. 2014. Bitcoin flaw that caused Mt.Gox disaster gets patched. Brightsideofnews. Viitattu 22.10.2014. <http://www.brightsideofnews.com/2014/03/20/bitcoin-flaw-that-caused-mtgox-disaster-gets-patched/>.
- Selkis, R. 2014. Bitcoin IRS tax guide for individuals filers. Viitattu 26.10.2014. <http://www.investopedia.com/university/definitive-bitcoin-tax-guide-dont-let-irs-snow-you/>.
- Smithers, A.H. 2013. Everything you need to know before buying, selling and investing in bitcoin. Great Britain: Amazon.co.uk.
- Startbitcoin 2014a. Beginner's guide to mining Bitcoins. Viitattu 16.5.2014, 15.5.2014. <http://startbitcoin.com/>.
- Startbitcoin 2014b. Bitcoin profitability calculator. Viitattu 16.5.2014. <http://startbitcoin.com/bitcoin-profitability-calculator/>.
- Startbitcoin 2014c. Mine or buy. Viitattu 15.5.2014. <http://startbitcoin.com/mine-or-buy/>.
- Suomen pankki: Bitcoin ei ole oikea valuutta. 2014. Digitoday. Viitattu 25.10.2014. <http://www.digitoday.fi/bisnes/2014/01/20/suomen-pankki-bitcoin-ei-ole-oikea-valuutta/2014897/66>.
- Trade. 2014. Bitcoin wiki. Viitattu 27.8.2014. <https://en.bitcoin.it/wiki/Trade>.
- Verohallinto 2013. Virtuaalivaluuttojen tuloverotus. Viitattu 26.10.2014. [www.vero.fi](http://www.vero.fi) > Syventävät vero-ohjeet > Verhoallinnon ohjeet > Virtuaalivaluuttojen tuloverotus.
- Willis, N. 2010. Bitcoin: Virtual money created by CPU cycles. LWN.net. Viitattu 22.3.2014. <http://lwn.net/Articles/414452/>.