

Wille Kuutti



Kryptovaluutat ja lohkoketjut, mahdollisuus vai uhka?



Kryptovaluutat ja lohkoketjut, mahdollisuus vai uhka?

Tämä teos on saanut tukea Suomen tietokirjailijat Ry:ltä.

Wille Kuutti

Kryptovaluutat ja lohkoketjut, mahdollisuus vai uhka?

© 2017 Kuutti, Wille / Kuutti International Oy
Kustantaja: BoD – Books on Demand, Helsinki, Suomi
Valmistaja: BoD – Books on Demand, Norderstedt, Saksa
ISBN: 978-951-568-063-1

Sisällysluettelo

Alkusanat	8
Lukijalle	12
Luku 1 – Rahan historia	14
Vaihdantataloudesta rahatalouteen	14
Metallirahan aika	16
Kultakannasta luopuminen	17
Näkymätön raha	18
Valuuttakriisit	18
Bitcoinin arvo	19
Bitcoinin lyhyt historia	20
Luku 2 - Kryptovaluutat	22
Bitcoin	22
Historiaa	22
Tekniikkaa	23
Bitcoin osoite	24
Bitcoin siirto	24
Lompakon varmuuskopiointi	26
Bitcoinien liikkeellelasku	27
Bitcoin kuitti	28
Muut kryptovaluutat	29
Litecoin	29
Muut kryptovaluutat	30
Namecoin	30
Luku 3 - Bitcoinin matemaattinen perusta	32
Salausmenetelmistä	32
Julkisen ja yksityisen avaimen salaus	32
Tiivistefunktiot	35
Bitcoin	36
Elektroninen kolikko	36
Bitcoin tili/lompakko	38
Bitcoin osoite	38
Vertaisverkko	39
Maksutapahtuma	41

Merkle Tree	45
Lohko	46
Lohkoketju	49
Lukitus ja avaus-skriptit	50
Luku 4 - Bitcoinien käyttö käytännössä	57
Bitcoin asiakasohjelma	57
Web-lompakot	58
Bitcoin Core	58
Luku 5 – Muut maksujärjestelmät vs. kryptovaluutat	71
Perinteiset pankit ja tilisiirrot	71
Luottokortit	73
Paypal	75
Western Union	76
Mobiililompakot ja maksut	77
Luku 6 - Bitcoinien louhinta	79
Mitä louhinta tarkalleen ottaen on?	79
Vaikeusaste	80
Louhiminen tietokoneella	81
Louhiminen näytönohjaimella	81
ASIC-louhinta	82
Alustava kannattavuuslaskelma	83
Luku 7- Kryptovaluutat ja verotus Suomessa	85
Johdanto verotukseen	85
Luovutusvoiton verotus	85
Hyödykkeiden ja palveluiden hankinta kryptovaluutalla	86
Louhimisen verotus	87
Arvonlisävero kohtelu	88
Luku 8 - Kryptovaluuttojen sääntelystä ja verotuksesta maailmalla	90
Kryptovaluuttojen käyttörajoitukset	90
Tekniset käyttörajoitukset	91
Intia	91
Islanti	92
Kiina	92
Thaimaa	92
Viro	93
Venäjä	93
Luku 9 – Kryptovaluutat ja rikollisuus	94

Huumekauppa	94
Huijaukset.....	95
”Guerrilla mining”	96
Luku 10 – Salaperäinen Satoshi Nakamoto.....	97
Dorian Nakamoto	97
Nick Szabo.....	98
Hal Finney	98
Wei Dai	98
Craig Steven Wright	99
Suomalaiset ehdokkaat	99
Nakamoton bitcoinit.....	99
Luku 11 – Kryptovaluuttojen mahdollisuuksia ja uhkia	101
Kryptovaluutat kehittyvissä maissa ja kriisialuilla	101
Lohkoketjun hyödyntäminen esimerkiksi logistiikassa	102
Kryptovaluutta uhkana	103
Kryptovaluutat ovat pyramidihuijaus	103
Kryptovaluutat ja kasvihuoneilmiö	105
Bitcoinin kapasiteetti ei riitä suosion kasvaessa	105
Bitcoinit loppuvat kesken	106
Parempi kryptovaluutta syrjäyttää Bitcoinin	107
Luku 12 – Bitcoinin script ohjelmointikieli.....	108
Arvoja pinoon	108
Ehdollista käsittelyä	109
Pinon käsittely	110
Merkkijonojen käsittely	112
Binääriaritmetiikka.....	113
Laskutoimituksia	114
Kryptografisia ja tiivistefunktioita.....	117
Varattuja sanoja.....	118

Alkusanat

Kryptovaluutat, ensimmäinen käytännössä toimiva ja laajalle levinnyt kryptovaluutta Bitcoin etunenässä ovat saaneet viimevuosina varsin laajalti mediahuomiota. Suomestakin löytyy jo kauppajoissa maksuvälineeksi kelpaavat perinteisen riihikuivan käteisen ja korttien lisäksi myös bitcoinit. Rautatieasemalta löytyy jo useampikin automaatti, jolla voi ostaa itselleen bitcoineja niin seteleillä kuin korteillakin. Maailmalla ovat yleistyneet myös automaattit, joissa bitcoineilla voi nostaa oikeaa rahaa pankkiautomaatin tapaan ja ovatpa nämä rantautuneet jo suomeenkin, tätä kirjoitettaessa niitä löytyy jo niin Helsingistä kuin Tampereeltakin. Automaatit ovat alkaneet levittäytyä myös Helsingin ulkopuolelle suurimpiin kaupunkeihin.

Maailmalla taas on kohistu rikollisten SilkRoad kauppapaikasta, hieman eBaytä muistuttavalla kauppapaikalla on pystynyt bitcoineilla ostamaan mm. huumeita ja muuta laitonta tavaraa. Viranomaiset ovat myös pystyneet vastaamaan haasteeseen ja sulkemaan tällaisia kauppapaikkoja, mutta uusia on noussut varsin nopeasti.

Bitcoin piireissä aikamoinen kohu oli myös hyvin suosituksen bitcoinpörssi Mt Goxin sulkeutuminen ja hakeutuminen konkurssiin sen väitettyä hukanneen suuren määrän asiakkaidensa bitcoineja. Vaikka osa löytyikin, suurin osa asiakkaista jäivät nuolemaan näppejään. Mt Goxin kohtalo on edelleen jossakin määrin epäselvä rikostutkinnan ollessa käynnissä, eikä ole täyttä selvyyttä siitä, hukkasiko Mt Gox bitcoinit vahingossa, joutuiko se rikoksen uriksi vai oliko peräti yrityksen johto vastuussa bitcoinien "katoamisesta". Myös osa muista bitcoinpörseistä ovat törmänneet samantyyppisiin ongelmiin.

Suomalainen bitcoinin kehityksessä lähes alkumetreiltä saakka mukana ollut Martti Malmi kertoi julkisuudessa myyneensä ainakin osan hallussaan pitämistään suurehkoista määrästä bitcoineja ja tienanneensa tällä varsin mukavasti vaikka ajoittikin myyntinsä ennen suurempaa bitcoinin arvon-

nousua. Tästä intoutuneena varmasti moni suomalainenkin hankki bitcoineja arvonnousun toivossa. Näistä varmasti moni on myös joutunut pettymään bitcoiniensa arvon laskettua huonosti ajoitettujen ostojen ja bitcoinin suuren volatiliteetin vuoksi.

Bitcoinin ympärille kietoutuu myös lukuisia salaliittoteorioita, eikä vähiten liittyen bitcoinin alkuperäisen idean esittäjään Satoshi Nakamotoon, jonka todellinen henkilöllisyys on edelleenkin hämärän peitossa, vaikka kansainvälinen lehdistö onkin tuonut useampiakin ehdokkaita päivänvaloon. Onpa jopa suomalaista Martti Malmia väläytelty Satoshi Nakamotoksi, mutta monien faktojen valossa tämä vaikuttaa hyvin epätodennäköiseltä.

Bitcoinin liittyy myös suuria tunteita, liberaalien piireissä vapaa, itsenäinen, valtioista vapaa valuutta on saavuttanut suuren suosion. Bitcoinin saavuttaman suosion vuoksi monet tahot ovat alkaneet nähdä sen myös uhkana, valtaapitäville nimettömästi valtioiden rajat helposti ylittävä maksuväline voi olla pelottava ja se varmasti hankaloittaa esimerkiksi rikostutkintoja. Myös perinteinen pankkimaailma näkee bitcoinissa uhkia omalle bisnekselleen, onhan se näin kansainvälisen verkkokaupan kulta-aikana varsin kätevä ja kustannustehokas kilpailija jopa luottokorttimaksuille, hinnavista kansainvälisistä tilisiirroista nyt sitten puhumattakaan. Toisaalta maailmalla suurimmat pankit ovat jo jonkin aikaa tutkineet bitcoinin toiminnan perusteena olevaa lohkoketjua ja sen tai samantapaisen tekniikan hyödyntämistä niiden omiin tarpeisiin. Lohkoketjuteknologiaa voidaan hyödyntää myös esimerkiksi sopimusten vahvistamiseen ja erilaisten asiakirjojen notariointiin. Tämän ympärille on jo kehittynyt liiketoimintaa, niin esimerkiksi bitcoinin lohkoketjua hyödyntäviä kuin myös omaa teknologiaa markkinoivia yrityksiä jotka kenties imagosyistä haluavat tehdä pesäeroa kryptovaluuttoihin.

Bitcoinin liittyy siis monenlaisia intressejä, tästä hyvin kuvaavaa on kun eräs tuttavani oli kuullut Suomen Tietokirjailijat Ry:ltä saamastani apurahan tämän kirjan kirjoittamiseen; Ensimmäinen kysymys oli että heillä on sitten jokin intressi bitcoinin suhteen? Tässä tapauksessa intressiä ei varmasti ole, ellei sellaiseksi lasketa sitä että halutaan mahdollisimman puolu-eeton faktateos aiheesta. Suomen Tietokirjailijat Ry ei ole millään tapaa pyrkinyt vaikuttamaan teoksen sisältöön. Muualla näitä intressejä varmasti

on ja välillä ne paistavat varsin räikeästi läpi. Itse olen huomannut useita virheitä ja väärinkäsityksiä esimerkiksi lehtikirjoittelussa, joskus kyse on ehkä toimittajan heikosta perehtymisestä asiaan, mutta valitettavasti mitä todennäköisimmin tarjolla on myös tarkoituksella harhaan johtavaa informaatiota, jolla pyritään ajamaan jonkin ryhmän intressejä tässä asiassa.

Toki bitcoin on yleistymisensä myötä saanut myös aivan arkista käyttöä, varsinkin nuoret edelläkävijät ovat omaksuneet sen aivan arkipäiväiseksi maksuvälineeksi aivan samaan tapaan, kuten nykyiset aikuiset ovat tottuneet käyttämään luottokortteja ja vanhukset käteistä rahaa.

Tämän teoksen tarkoitus on kertoa mahdollisimman puolueetonta faktatietoa bitcoinista ja myös muista sen kanssa kilpailevista kryptovaluutoista. Perehdymme myös seikkaperäisesti kryptovaluutoiden teknologiaan ja lohkoketjuteknologian hyödyntämismahdollisuuksiin. Tarkoituksena ei ole säikäyttää ketään olemaan käyttämättä bitcoineja, eikä myöskään houkutella ketään bitcoineja käyttämään. Päätöksen siitä lähtee, ja missä laajuudessa lähtee, kryptovaluutoita käyttämään tekee lukija aivan itse. Suosittelemme kuitenkin kaikkia bitcoineja jo käyttäviä ja niiden käyttöä harkitsevia lukemaan tämän kirjan ja harkitsemaan itse faktatiedon pohjalta miten ja missä laajuudessa bitcoinien maailmaan mukaan lähtee.

Tämän kirjan myötä pyrin myös lanseeraamaan suomalaiseen kielenkäyttöön mielestäni paremmin bitcoinin kaltaisia valuuttoja kuvaavan termin kryptovaluutta aiemmin enemmän käytetyn virtuaalivaluutan tilalle. Englanninkielisessä kirjallisuudessa kryptovaluutta (cryptocurrency) on jo varsin vakiintunut termi. Tämänkin kirjan alkuperäinen työnimi oli ”Virtuaalivaluutat, mahdollisuus vai uhka?”, mutta kuten tulemme ensimmäisessä rahan historiaa käsittelevässä luvussa huomaamaan, myös perinteiset valuutat ovat nykyään mitä suuremmissa määrin virtuaalisia. Harvemmin enää käsittelemme ainakaan suurempia summia fyysistä rahaa, vaan valtaosa jokapäiväisestä rahaliikenteestä on jo nyt täysin ”virtuaalisia” bittejä. Nykyinen raha, kuten jo myös monenlaiset historiassa käytetyt rahat, perustuu myös kryptovaluutoiden tapaan pitkälti luottamukseen, eikä sillä ole minikäänlaista itseisarvoa, eikä se ole taatusti vaihdettavissa mihinkään jos luottamus on mennyt. Se on siis myös siinä mielessä varsin virtuaalista.

Bitcoin ja sen johdannaiset perustuvat pitkälti kryptografiaan ja siihen lähe-

Kryptovaluutat, ensimmäinen käytännössä toimiva ja laajalle levinnyt kryptovaluutta Bitcoin etunenässä ovat saaneet viimevuosina varsin laajalti mediahuomiota. Suomestakin löytyy jo kauppoja joissa maksuvälineeksi kelpaavat perinteisen riihikuivan käteisen ja korttien lisäksi myös bitcoinit. Rautatieasemalta löytyy jo useampikin automaatti, jolla voi ostaa itselleen bitcoineja niin seteleillä kuin korteillakin. Maailmalla ovat yleistyneet myös automaattit, joissa bitcoineilla voi nostaa oikeaa rahaa pankkiautomaatin tapaan ja ovatpa nämä rantautuneet jo suomeenkin, tätä kirjoitettaessa niitä löytyy jo niin Helsingistä kuin Tampereeltakin. Automaattit ovat alkaneet levittäytyä myös Helsingin ulkopuolelle suurimpiin kaupunkeihin. Tämä kirja pyrkii käytännönläheisesti esittelemään kryptovaluuttojen teknologian ja niiden käytön käytännössä helposti ymmärrettävässä muodossa. Tutustumme myös lyhyesti kryptovaluuttojen historiaan ja vertailemme niitä perinteisten maksutapojen kanssa, sekä selvitämme kryptovaluuttojen laillisen ja verotuksellisen aseman niin Suomessa kuin maailmalla.

