Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2014

Pekka Setälä

BITCOIN JA SEN TULEVAISUUS KEHITYSMAISSA

Kryptovaluutta bitcoin vaihtoehtoisena valuuttana kehitysmaissa.

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

Joulukuu 2014 | 40 sivua

Pasi Iivonen

Pekka Setälä

BITCOIN JA SEN TULEVAISUUS KEHITYSMAISSA

Tässä opinnäytetyössä käsitellään kryptovaluutta bitcoinia kehitysmaiden näkökulmasta. Teoriaosuudessa selitetään mikä on bitcoinin historia ja minkälaiseen teknologiaan se perustuu.

Opinnäytteessä käytetään nopeasti kehittyvän teknologian vuoksi lähinnä verkkolähteitä, mutta teoriaosuudessa käytetään myös kirjallisuus- ja tutkimuslähteitä.

Työssä tutkitaan minkälaisia tapoja on hyödyntää avoimen lähdekoodin valuuttaa kehittyvissä valtioissa, joiden köyhimmät kansalaiset eivät pääse käsiksi pankkipalveluihin. Opinnäytetteessä esitellään jo olemassa olevia mobiilimaksamisen tapoja kehitysmaissa ja miten bitcoin voidaan integroida samoihin menetelmiin.

Empiirisessä osuudessa esitellään miten luodaan tekstiviestipohjainen bitcoin–lompakko mobiilitransaktioita varten.

ASIASANAT:

Bitcoin, kryptovaluutta, kehitysmaat, raha, valuutta, mobiilimaksaminen

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

December 2014 | 40 pages

Pasi Iivonen

Pekka Setälä

THE FUTURE OF BITCOIN IN DEVELOPING COUNTRIES

This thesis is about the cryptocurrency Bitcoin in view of the developing countries. The theoretical section discusses the history of Bitcoin and the technology is it based upon.

The thesis used mostly Internet-based sources, because the technology is rapidly evolving but literature and previous studies were also utilized.

The thesis examines ways to implement open source currencies in the developing countries where the poorest citizens do not have access for banking. Current ways for mobile payment in the developing countries are also presented and ways to integrate Bitcoin into the methods.

The empirical part of the thesis introduces how to sign up for SMS based Bitcoin wallet for mobile transactions.

KEYWORDS:

Bitcoin, cryptocurrency, developing countries, money, currency, mobile payment

SISÄLTÖ

KUVAT

KUVIOT

SANASTO

BTC	Bitcoin-rahayksikkö. (Bitcoin 2014.)
Fiat-raha	Raha, jolla ei ole luontaista arvoa ja jonka arvo perustuu sen liikeellä olevaan määrään. (Fiat-raha 2014.)
Mikrofinanssi	Mikrotaloustiede. Kansantalouden pienyksiköitä tutkiva taloustiede. (Mikrotaloustiede 2014.)
P2P (peer to peer)	Vertaisverkko on verkko, jossa ei ole kiinteitä palvelimia. Jokainen verkkoon kytkeytynyt taho toimii sekä asiakkaana että palvelimena verkon jäsenille. (Vertaisverkko 2014.)
TOR-verkko	Avoimen lähdekoodin ohjelmisto, joka reitittää verkkoliikenteen anonyymisti. (Torverkko 2014.)
Transaktio	Allekirjoitettu sektio dataa, joka lähetetään verkkoon ja kerätään talteen lohkoon.Yksittäinen tehty vastineellinen kauppa, vaihto. (Bitcoin 2014.)

1 JOHDANTO

Taantuma on synnyttänyt ihmisissä epäluottamusta pankkijärjestelmän luotettavuuteen ja näyttänyt miten haavoittuvainen rahatalous voi olla. Occupy-liike on esimerkki ilmiöstä, joka levisi Internetin kautta yrittäen saada ihmisten huomiota rahan epäkohtiin. Kryptovaluutat ovat uudenlainen tapa lähestyä rahaa ja vaihdantataloutta.

Kryptovaluutat muodostuvat avoimesta lähdekoodista, jonka tarkoituksena on luoda rahajärjestelmä Internetin sisälle. Valuuttaa luodaan emuloimalla arvometallien louhintaa tietokoneen laskentatehon avulla ja vaihdanta tapahtuu täysin käyttäjältä toiselle ilman kolmatta osapuolta.

Opinnäytteen teoriaosuudessa käsitellään, mikä on kryptovaluutta bitcoin ja mikä on sen historia. Työn empiirisessä osuudessa selvitetään, miten bitcoineja ostetaan ja myydään Suomessa. Sekä otetaan käyttöön tekstiviestipohjainen mobiililompakko. Työssä tutkitaan, miten bitcoinia voidaan käyttää rajoittuneemmalla mobiiliteknologialla kehitysmaissa.

Työn tavoitteena on selvittää millaisia mahdollisuuksia kehittyvien valtioiden asukkailla olisi käyttää virtuaalista rahaa vaihdannan välineenä ja miten lohkoketjuteknologia voisi tuoda vähävaraisemmat ihmiset osaksi kansainvälistä pankkitoimintaa.

2 BITCOININ HISTORIA

2.1 Virtuaalivaluutat

Virtuaalinen käteinen ei ole uusi keksintö, vaan ennen bitcoinin syntyä digitaalista rahaa oli jo kehitetty useammallla taholla. Virtuaalivaluuttojen skeemat voidaan jakaa kolmeen kategoriaan, sen mukaan miten ne ovat vuorovaikutuksessa perinteisen valuutan kanssa:

1. Suljetut virtuaalivaluutat, joilla ei ole mitään yhteyttä perinteisten valuuttojen kanssa.
2. Virtuaalivaluutat, joilla on yksisuuntainen virtaus; niitä voidaan ostaa käyttäen perinteistä valuuttaa.
3. Virtuaalivaluutat, joilla on kaksisuuntainen virtaus; niitä voidaan ostaa ja myydä käyttäen perinteisiä valuuttoja. (Amores, R & Paganini, P. 2013. s.108).

2.2 Satoshi Nakamoton bitcoin

Satoshi Nakamoto–salanimellä kulkeva ohjelmistokehittäjä tai kehittäjäryhmä julkisti kehittäneensä vuodesta 2007 lähtien verkossa toimivaa P2P-virtuaalikäteistä eli kryptovaluuttaa.

Vuonna 2008 pseudonyymi Satoshi Nakamoto julkisti bitcoin-manifeston, jossa esiteltiin uudenlainen hajautettu virtuaalikäteinen, kryptovaluutta, jossa kaikki transaktiot tapahtuvat vertaisverkossa käyttäjältä käyttäjälle.

Nakamoto halusi maailman parhaita kryptografeja ja ohjelmistokehittäjiä mukaan projektiinsa. Vuonna 2009 julkaistiin avoimeen lähdekoodiin perustuva kryptovaluutta bitcoin.

Satoshi Nakamoto tiettävästi louhi bitcoin–verkossa ensimmäisen lohkon, jota kutsutaan myös syntylohkoksi (genesis block), josta hän sai palkkioksi 50 BTC.

Silloin bitcoinilla ei ollut vielä mitään arvoa esimerkiksi Yhdysvaltain dollariin nähden. Käyttäjät itse määrittelivät ensimmäisen transaktion hinnan Bitcointalks-foorumilla, jossa ensimmäinen merkittävä bitcoin–transaktio tapahtui: 10 000 BTC käytettiin kahden pizzan ostamiseen Papa John's –ravintolasta. (History of Bitcoin 2014.)

Altcoin

Altcoin–termillä tarkoitetaan kaikkia virtuaalivaluuttoja bitcoinin ulkopuolella, jotka perustuvat samaan lohkoketjuteknologiaan. Kuka tahansa voi luoda virtuaalivaluutan tällä teknologialla, koska se on avointa lähdekoodia ja kaikkien käytettävissä.

Kaikki eivät ole sitä mieltä että juuri bitcoinin lähdekoodissa on kaikki tarvittavat ominaisuudet, joten ihmiset ovat koodanneet vaihtoehtoisia valuuttoja eri tarpeisiin. Altcoineja myyviä pörssejä on vielä vähän, joten helpoin ja turvallisin tapa ostaa niitä on käyttämällä bitcoinia vaihdon välineenä. Altcoineja voi myös louhia tietokoneen laskentatehoa hyödyntämällä. (Altcoin 2014.)

2.3 Wikileaks ja bitcoin

Wikileaks nosti bitcoinin pinnalle suuremman yleisön tietoisuuteen vuonna 2010 kun isot pankit ja korporaatiot kuten esimerkiksi Visa, Mastercard ja PayPal jäädyttivät kaikki Wikileaksille kohdistetut lahjoitukset. Ihmiset tarvitsivat tavan lähettää rahaa ilman kolmannen osapuolen puuttumista, ja bitcoinin hajautettu toimintamalli osoittautui hyödylliseksi. Ihmiset pystyivät lähettämään varoja Wikileaksin hyväksi ilman kolmannen osapuolen puuttumista rahavirtaan. (Operation Payback 2014.)

2.4 Mt. Gox –pörssin romahtaminen

Mt. Gox vaihtopörssi perustettiin 2010 ja se nousi nopeasti maailman suurimmaksi bitcoineja vaihtavaksi pörssiksi. Vuoteen 2013 menessä se käsitteli 70 %

kaikesta bitcoin–liikenteestä. Bitcoinin arvo nousi hitaasti vuosina 2010 – 2013 muutamasta isommasta notkahduksesta huolimatta. 2013 alussa Bitcoinin arvo dollareihin nähden oli 13 $/1 BTC ja se nousi vuoden mittaan yli 1000 $/1 BTC vuoden loppuun mennessä. (Blockhain 2014.)

Heidän sivustonsa koodin tietoturva ei kuitenkaan ollut vaadittavalla tasolla käsittelemään niin isoja summia ja yhtiön tililtä olikin varastettu bitcoineja jo vuosia. Kun tietomurto vihdoin tuli julki huhtikuussa 2014, olivat hakkerit saaneet varastettua 850 000 BTC Mt. Goxin hallusta, joka oli n. 460 miljoonan dollarin arvosta silloisella vaihtokurssilla. Mt. Gox ajautui konkurssiin ja tietomurron jälkeen bitcoinin arvo romahti. (McMillan, R. 2014; Mt. Gox 2014.)

3 BITCOIN YLEISESTI

3.1 Bitcoinin perusteet

Bitcoin on digitaalista käteistä eli kryptovaluuttaa jota luodaan tietokoneiden laskentatehoa hyödyntämällä. Prosessia kutsutaan louhimiseksi ja se toimii avoimeen lähdekoodiin perustuvalla ohjelmistolla. Bitcoinin kehitti joukko anonyymejä Internetin käyttäjiä vuonna 2008 ja se on tällä hetkellä käytetyin kryptovaluutta verkossa. Ihmiset voivat jakaa ja vaihtaa tätä valuuttaa keskenään verkossa ilman kolmatta osapuolta.

BitTorrent-protokolla mullisti tiedon jakamisen käyttäjältä käyttäjälle ilman, että välissä olisi hallinnoivaa elintä kontrolloimassa tiedon kulkua, ja bitcoin toimii samalla periaatteella: tiedonvälitystä ilman keskitettyä elintä. Lohkoketjun ensimmäinen applikaatio on kryptovaluutta bitcoin, mutta protokollan sisällä voi tehdä muitakin asioita, jotka ovat toteutettavissa kryptologian avulla.

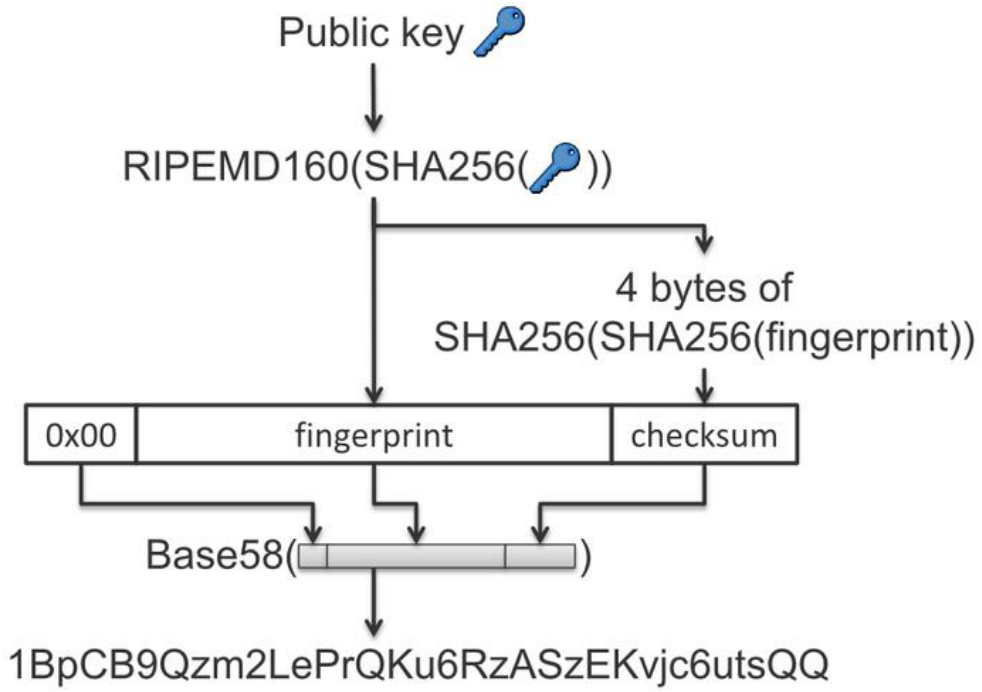
Bitcoinin tarkoituksena on luoda hajautettu valuuttajärjestelmä, joka toimii Internetissä yhtenäisenä verkkona, lohkoketjuna. Bitcoinilla ei ole keskitettyä pankkia, jonka kontrollissa valuuttaa vaihdetaan, vaan kaikki tieto siirtyy käyttäjältä käyttäjälle ja lohkoketju hyväksyy nämä tiedonvaihdot.

Uusia tilejä voi luoda rajattomasti ja niitä ei tarvitse yhdistää omistajan henkilöllisyyteen. Raha liikkuu rajojen yli yhtä helposti ja nopeasti kuin sähköposti. Bitcoin tekee muiden kuin itselle kuuluvien rahavirtojen hallinnasta ja verotuksesta vaikeaa tai mahdotonta. (Introduction 2014.)

3.2 Alfanumeerinen osoite

Kuviossa 1 osoitetut bitcoin–osoitteet muodostuvat 26-36 kirjaimesta tai numerosta ja niitä voi luoda ilmaiseksi niin paljon kuin haluaa. Osoitteen voi generoida esimerkiksi bitcoin-lompakon avulla automaattisesti tai erillisen desktop-ohjelmiston avulla (esim. Bitcoin-Qt). Bitcoin–osoite toimii kuin sähköpostiosoi-

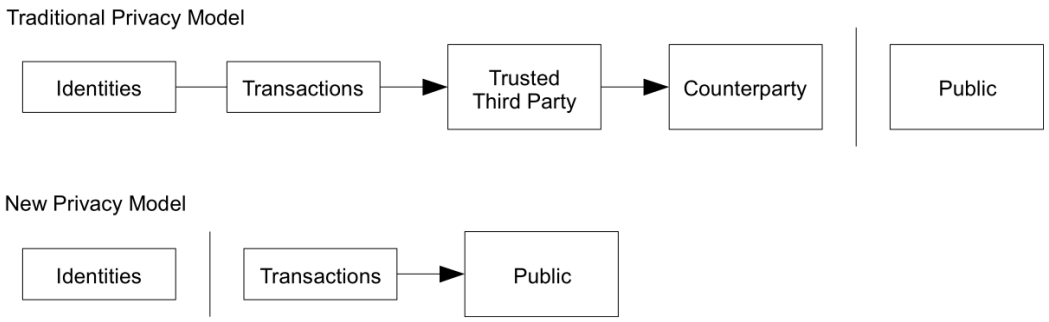
te, sinne voi lähettää bitcoineja käyttämällä asiakasohjelmaa eli bitcoin-lompakkoa.



Kuvio 1. Bitcoin-osoitteen rakenne. (Bitcoin address 2014.)

3.3 Tietoturva

Bitcoin on virtuaalista käteistä, ja kuten tavallinen käteinen raha, on myös bitcoin varastettavissa. Vaikka bitcoin-pankkipalvelut ovat käyttäjälle helppokäyttöisiä, on aina olemassa tietomurron riski, koska isot keskitetyt summat houkuttelevat tietomurtoihin. Kryptovaluutan alkuperäinen idea on kolmannen osapuolen poistaminen, joten on suositeltavaa pitää bitcoinit omassa hallussaan. Kuviossa 2 on esitetty Satoshi Nakamoton alkuperäinen turvallisuusmalli.



Kuvio 2. Bitcoinin turvallisuusmalli. (Nakamoto, S. 2008.)

Useampi lompakko ja hajautetut varat luovat lisää tietoturvaa, kun kaikki bitcoinit eivät ole varastoituna samaan paikkaan. Bitcoin-lompakosta voi siirtää varoja ulos yksityistä avainta käyttäen, joten sen turvassa pitäminen on tietoturvan tukipilari.

Perinteistä käteistä on mahdotonta varmuuskopioida ja varkauden tapahtuessa rahat ovat useimmiten kadoksissa lopullisesti. Kun käteinen on digitaalista, on se mahdollista myös varmuuskopioida ja kryptata. Tällaiset turvatoimet suojaavat kryptovaluuttaa varkausten varalta. (Bitcoin.org 2014.)

Virtuaalivaluuttojen tietoturva kehittyy huimaa vauhtia, kun muualla tietotekniikassa jo käytettävissä olevia turvametodeja aletaan soveltamaan virtuaalivaluuttojen turvassa pitämiseen. Esimerkiksi biometriset turvatoimet, kuten sorminjälki- ja retinaskannaukset voivat tuoda bitcoinien säilyttämiseen ja käyttämiseen turvaa. (Bradbury, D. 2014.)

Anonymiteetti

Bitcoin käyttää julkisen avaimen salausta siirtäessään valuuttaa lompakkojen välillä. Kaikki siirrot ovat julkisia palvelun luonteesta johtuen ja tietoja säilytetään julkisessa hajautetussa tietokannassa, jota kutsutaan lohkoketjuksi. Lohkoketju sisältää bitcoin-osoitteet sekä jokaisen omistajan bitcoin-rahamäärän. Osoitteiden omistajien tietoja ei ole missään näkyvillä.

Tietokanta sisältää kaikki tapahtumat palvelun alusta alkaen ja tämän takia bitcoinin käyttö ei ole täysin anonyymiä, vaikka henkilötietoja ei näkyvissä olekaan. Transaktioista jää lohkoketjuun aina jälki. (Anonymity 2014.)

3.4 Bitcoin verrattuna fiat-valuuttoihin

Koska kryptovaluuttojen idea on poistaa kolmas osapuoli dataliikenteen välistä, on pankkien asema rahaliikenteen kontrolloijana uhattuna. Koska fiat-valuutatkaan eivät ole olleet kiinnitettynä kultakantaan enää vuosikymmeniin, ovat ne uhattuna manipulaatiolle. Esimerkiksi Yhdysvaltain dollarin ja euron arvot perustuvat täysin liikkeellä olevaan rahan määrään, eivätkä ne ole sidottuna esimerkiksi arvometalleihin kuten kultaan. (Fiat-raha 2014.)

Bitcoinin louhintaprosessin periaatteena on simuloida arvometallien louhintaa ja siihen tarvitaan resursseja; tietokoneen laskentatehoa ja siihen sähköä. Louhittavien kolikoiden määrä on rajattu, joten se on verrannollinen oikeiden arvometallien louhintaan ja harvinaisuuteen. (Amores, R & Paganini, P. 2013. s.41)

Verotus Suomessa

Verohallinnon mukaan olemassa olevat virtuaalivaluutat eivät ole oikeaa ja virallista valuuttaa, koska sitä ei ole laskenut liikkeelle minkään valtion keskuspankki. Sen arvoa ei ole sidottu pankkien valuutavaihtokursseihin, vaan sen arvo suhteessa virallisiin valuuttoihin määräytyy kysynnän ja tarjonnan perusteella.

Kryptovaluutan louhimisesta saatu virtuaalivaluutta on verottajan mukaan ansiotuloa. Kun kryptovaluuttaa vaihdetaan perinteisiin valuuttoihin, arvonnousua pidetään pääomatulona ja se on siten verotettavaa tuloa. Tällä hetkellä verkossa tapahtuvaa kryptovaluuttakauppaa on verottajan erittäin vaikea seurata. Vaikka transaktiot ovat lohkoketjussa kaikkien näkyvillä, vastaanottajat ja lähettäjät ovat anonyymejä. (Verohallinto 2013.)

3.5 Ekologisuus

Bitcoinin ekologisuudesta on mielipiteitä puolesta ja vastaan. Louhintaprosessi vaatii energiaa, jotta uusia kolikoita voidaan luoda lohkoketjuun. Tämä on ollut argumenttina, että kryptovaluutat eivät olisi ekologinen vaihtoehto perinteiselle valuutalle.

Vasta-argumenttina tälle väitteelle on arvometallien louhinnan saastuttavuus, joka tuhoaa ympäristöä sekä kuluttaa luonnonvaroja ympäri maailmaa. Bitcoinin louhintaan kehitetään jatkuvasti energiatehokkaampia tapoja, koska louhinta on kovin kilpailtu markkina. Louhinnasta syntynyttä lämpöenergiaa pystyisi myös käyttämään hyväksi vaikkapa lämmitykseen.

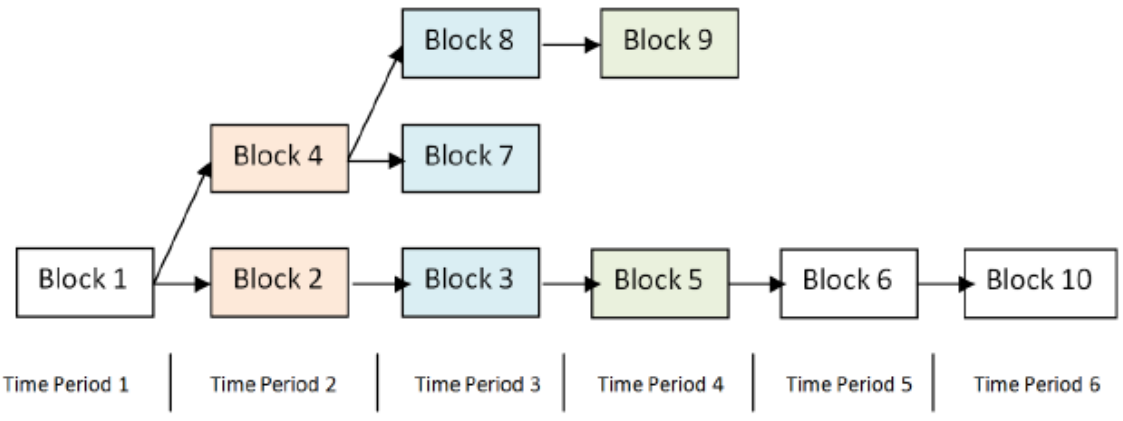
4 BITCOIN LOHKOKETJU

Uudet bitcoinit syntyvät bitcoin-verkossa louhintaprosessin sivutuotteena. Louhintaan voi valjastaa esimerkiksi oman tietokoneen, jonka laskentatehoa käytetään monimutkaisten algoritmien ratkaisemiseksi erillisen ohjelmiston avulla.

Kun lohko on ratkaistu, saavat louhijat siitä palkkioksi bitcoineja. Tämä luo louhijoille rahallisen kannusteen ylläpitää lohkoketjun turvallisuutta laskentatehoillaan. Bitcoinien louhinnalla on pyritty jäljittelemään arvometallien louhintaa. Louhiminen vaikeutuu ja siitä saadut palkkiot pienenevät ajan myötä. (Nakamoto, S. 2008.)

4.1 Bitcoinin lohkot

Bitcoin perustuu julkiseen tietokantaan, joka sisältää ketjutettuja lohkoja eli lohkoketjuja. Kuviossa 3 näkyy malli bitcoinin lohkoketjusta. Tämä tietokanta sisältää kaikki transaktiot bitcoinin historian aikana. Keskitetysti hallituista valuutoista poiketen ei ole olemassa mitään tahoa, joka kykenisi luomaan bitcoineja yksinoikeudella tai rajattomasti.



Kuvio 3. Bitcoin lohkoketju (Bitcoin Security 2014.)

Lohkoketju muodostuu siitä, että jokainen uusi lohko sisältää edeltävän lohkon tiivisteen. Jos lohkoketju on jostain kohdasta haarautunut kahdeksi haaraksi, niin voimassa oleva on se haara, jonka lohkojen yhteenlaskettu vaikeustaso on suurempi. Jotta lohkoketjun historiaa voisi muuttaa, pitäisi ensin uudelleenluoda sekä se lohko, johon muutos tulee, että kaikki sen jälkeiset lohkot.

Verkko säätää lohkoilta vaadittavaa vaikeustasoa 2016:n lohkon välein sellaiseksi, että uusi lohko synnyttää 25 uutta bitcoinia keskimäärin kuusi kertaa tunnissa. Palkkioksi saatavien bitcoinien määrä puolittuu joka neljäs vuosi ja laskettavat algoritmit vaikeutuvat ajan myötä. (Block chain 2014.)

4.2 Yhteislouhinta

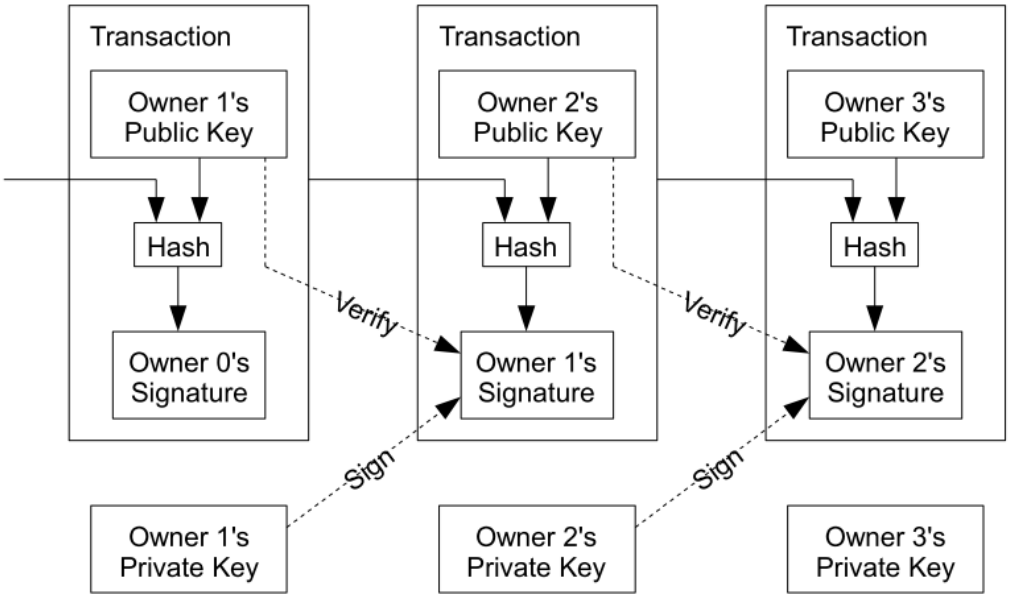
Yhteislouhinta eli louhintapoolit ovat keskitettyjä louhintaryhmiä, jotka keskittävät yhdessä oman laskentatehonsa saman lohkon louhimiseen. Kun lohko on ratkaistu, jaetaan siitä saatu palkkio kaikkien lohkon louhijoiden kesken. Palkkiot ovat siis pienempiä, mutta niitä tulee useammin, koska saman lohkon louhimiseen osallistuu useampi.

Nykyään bitcoinien louhintaan tarvitaan yhä tehokkaampaa laitteistoa, jotta louhiminen olisi kannattavaa, koska lohkot ovat yhä vaikeampia ratkaista. Yhteislouhintaan pääsee mukaan pienemmällä investoinnilla louhintalaitteistoon, ja saa nopeammin vastinetta louhimiseen käyttämäänsä resursseihin. (Pooled mining 2014.)

4.3 Transaktiot

Krpytovaluutta on pelkistettynä ketju digitaalisia allekirjoituksia. Yksityisellä avaimella voidaan lähettää bitcoineja ja yhdellä tai useammalla julkisella avaimella voi vastaanottaa bitcoineja (kuvio 4). Transaktio allekirjoitetaan lohkoketjussa.

Kun suorittaa siirron bitcoin-lompakosta X osoitteeseen Y, bitcoin-lompakko luo ilmoituksen, todistaa ja allekirjoittaa tämän siirron sekä kuuluttaa sen verkkoon louhijoille osaksi seuraavaa lohkoketjua. Siirtoa on siksi mahdotonta väärentää tai peruuttaa. (Nakamoto, S. 2008.)



Kuvio 4. Bitcoin transaktiot käyttäjältä toiselle. (Nakamoto, S. 2008.)

5 BITCOIN–LOMPAKOT JA SÄILYTYS

Perinteistä rahaa käytetään fyysiseti käteisellä, maksukortilla tai verkkopankissa. Pankit ovat jatkuvana kohteena ryöstöille ja erilaisille verkkohyökkäyksille. Tämän päivän luottokorttiteknologia on ollut käytössä jo 1950–luvulta lähtien ja ne ovat edelleen haavoittuvaisia tietomurroille ja varkauksille. (Credit card 2014.)

Kryptovaluutat ovat digitaalisuutensa vuoksi hyvin monimuotoisia käyttää ja säilyttää. Bitcoinit ja muut kryptovaluutat ovat digitaalista käteistä, joita säilytetään perinteisen käteisen tapaan lompakoissa. Valuutan säilyttämiseen ja käyttöön kannattaa valita erityyppinen lompakko.

Valuutan hajauttaminen on kryptovaluuttoja käyttäessä viisasta, koska jos lompakko varastetaan tai se häviää, ei kaikki varat katoa kerralla. Jos omistaa paljon bitcoineja, ei kannata pitää kaikkia esimerkiksi mobiililompakossa tai tietokoneen kovalevyllä, koska tietomurron ja fyysisen varkauden riski on olemassa. (Securing your wallet 2014.)

5.1 Lompakko tietokoneella

Bitcoineja voi käyttää tietokoneen kovalevylle asennettavalla ohjelmistolla, joka tallentaa yksityisen avaimen tietokoneen kovalevylle. Esimerkiksi Armory-ohjelmisto on suosittu bitcoin-lompakko tietokoneella käytettäväksi.

Lompakko suojataan salasanalla ja kryptataan turvallisuuden lisäämiseksi. Tietokoneella säilytettävä lompakko on kuitenkin tietoturvariski, jos tietokone on verkossa ilman kunnon tietoturvaa. Verkkohyökkäykset voivat vaarantaa kovalevylle talletetut avaimet. (Bitcoinarmory 2014.)

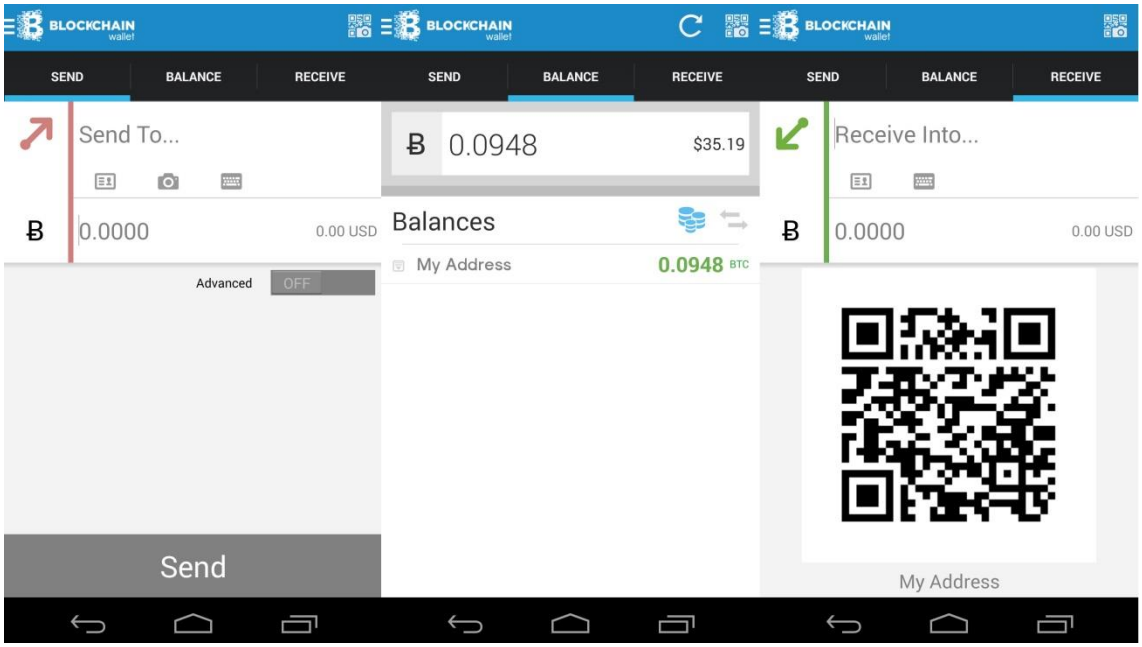
5.2 Lompakko matkapuhelimessa

Mobiililompakot ovat esimerkiksi älypuhelinapplikaatioita, jotka mahdollistavat bitcoinien lähettämisen ja vastaanottamisen suoraan matkapuhelimeen. Tämän takia mobiililompakot ovat suositumpia käyttölompakoita helpon käytettävyyden vuoksi. Valuuttaa voi lähettää kätevästi vain skannaamalla QR-koodin ja asettamalla summan.

Mobiililompakoita on saatavilla kaikille suosituimmille mobiilialustoille, kuten Androidille, iOSille ja Windows Phonelle. Lompakko on kryptattuna puhelimen muistissa ja se suojataan salasanalla. Lompakon voi myös varmuuskopioida, jotta sen voidaan palauttaa oikealle omistajalleen varkauden tapahtuessa. (Bitcoin.org 2014.)

QR-koodit

Koska bitcoin–osoitteet ovat pitkiä ja vaikeita muistaa ulkoa, on mobiilimaksamista helpottamaan valjastettu QR-koodit, jotka pitävät sisällään pitkän alfanumeerisen koodin joka toimii lompakon vastaanottavana osoitteena. Mobiililompakko käyttää älypuhelimen kameraa lukeakseen QR-koodin ja bitcoinin lähettäminen onnistuu nopeasti. Kuvassa 1 oikealla on Blockchain-lompakkoon sidottu QR-koodi.



Kuva 1. Kuvakaappaus Blockchain–mobiililompakosta.

Deterministinen lompakko

Toisin kuin perinteiset bitcoin-lompakot, jotka generoivat yksityisen avaimen ja julkisen avaimen satunnaisesti tarvittaessa, deterministinen lompakko generoi datan samasta ”siemenestä” käyttäen tiettyä algoritmiä.

Esimerkiksi jos tietokoneella oleva bitcoin-lompakko korruptoituu, voi deterministisen lompakon luoda uudelleen kaikkine yksityisavaimineen, kunhan siemenen koodi on tallessa. Tällaisen lompakon tietoturva on parempi, koska transaktiot eivät tule samasta osoitteesta ja lompakko on helppo palauttaa. (Deterministic wallet 2014.)

5.3 Fyysiset lompakot

Mikään ohjelmisto ei ole täysin haavoittumaton ja immuuni tietomurroille. Kryptovaluuttojen säilyttämiseen kehitetään jatkuvasti yhä turvallisempia menetelmiä. Turvallisin tapa säilyttää bitcoineja on fyysinen lompakko, jota säilytetään Internet-verkon ulottumattomissa. Näiden offline-lompakoiden tarkoituksena on poistaa verkkohyökkäyksien uhka bitcoinin säilytyksessä.

Paperilompakko

Paperilompakko on yksinkertaisin fyysinen lompakko. Yksityinen avain generoidaan esimerkiksi selaimessa toimivalla ohjelmistolla ja se tulostetaan tai kirjoitetaan paperille. Ohjelmistolla luotu avain kannattaa säilyttää turvassa, sen voi laittaa vaikkapa perinteisen käteisen tavoin kassakaappiin tai pankin talletuslokeroon. Aivolompakoksi kutsutaan sitä, kun generoitu koodi ainoastaan opetellaan ulkoa, eikä kirjata minnekään. (Paper wallet 2014.)

Kuva 2. Piper–paperilompakkotulostin. (Cryptograpgi Inc 2014.)

Rautalompakot

Hardware –lompakot eli rautalompakot ovat fyysisiä laitteita, jotka ovat erikseen suunniteltu kryptovaluuttojen vastaanottoon, lähettämiseen ja säilyttämiseen. Näitä lompakoita käytetään pääasiassa Internet-verkon ulkopuolella turvallisuuden lisäämiseksi. Kuvassa 2 Raspberry Pi -tietokoneesta rakennettu bitcoin-lompakko ja tulostin. (Hardware wallets 2014.)

Rautalompakon etuja:

- Yksityinen avain on usein tallennettu mikropiirin suojatulle alueelle ja sitä ei voida siirtää laitteelta toiselle tekstinä.
- Immuuni viruksille jotka varastavat lompakko-ohjelmistoista.

- Kryptovaluuttaa voidaan säilyttää turvallisesti, mutta myös interaktiivisesti. Toisin kuin paperilompakoita, joka täytyy tuoda lompakko-ohjelmistoon, jotta valuutan voi ottaa käyttöön. (Hardware wallet 2014.)

6 BITCOIN-PÖRSSIT

Helpoin tapa hankkia itselleen bitcoineja on ostaa sitä jollain toisella valuutalla bitcoineja myyvissä vaihtopörsseissä. Käytännössä tämä toimii samalla tavalla kuin mikä tahansa valuuttakauppa; toista valuuttaa vaihdetaan toiseen, mutta bitcoinin hinnan määrittelee kysyntä ja tarjonta.

Bitcoin on korkean inflaation valuutta, koska uusia bitcoineja syntyy louhinnan tuloksena lisää noin 10 minuutin välein. Se on ollut suhdanneherkkä valuutta koko elinkaarensa ajan, koska kryptovaluuttojen vaihdossa liikkuu vielä perinteiseen valuutanvaihtoon verrattuna vähän pääomaa.

Jos iso sijoittaja tai taho ostaisi bitcoineja miljoonasummilla, se heilauttaisi bitcoinin kurssia merkittävästi. Isojen valuuttojen kurssit pysyvät melko tasaisena, koska suuria summia vaihdetaan jatkuvasti.

Suosittuja bitcoinia vaihtavia pörssejä ovat esimerkiksi:

- Coinbase: vaihtaa bitcoineja ainoastaan Yhdysvaltain dollareihin, tarjoaa myös pankkipalveluja, mm. selaimessa toimivan lompakon. (Coinbase 2014.)
- Bitstamp: Euroopan isoin pörssi, vaihtaa Yhdysvaltain dollareita ja euroja bitcoineihin. (Bitstamp 2014.)
- BTCChina: Kiinassa sijaitseva pörssi, jonka vaihtovolyymi on toiseksi suurin maailmassa. (BTCchina 2014.)

Bitcoinin ostaminen ja myyminen Suomessa

Suomalaiselle helpoin ja turvallisi tapa ostaa bitcoineja on Bittiraha.fi:n tarjoama palvelu, jossa he hoitavat transaktion euroista bitcoineihin asiakkaan puolesta. Hinta määräytyy sen hetkisen kurssin mukaan ja bitcoinit saa useimmiten saman päivän aikana lompakkoonsa. Maksun voi suorittaa suomalaisessa verkkopankissa, kuten minkä tahansa laskun.

Ostaessa verkkosivun laskuri näyttää suoraan paljonko haluttu euromäärä on bitcoineissa. Palvelusta peritään palvelumaksu, joten se ei ole halvin tapa ostaa bitcoineja. Ostaessa kulu on 1,99 % + 1 € ja myydessä kulu on 1,99 % + 0,002 BTC. (Bittiraha.fi 2014.)

Bittimaatti

Bitcoineja on mahdollista ostaa myös käteisellä ns. Bittimaateista. Kuvassa 3 on Suomessa käytössä oleva Lamassu Bittimaatti. Näitä automaatteja löytyy 25.11.2014 Helsingistä, Turusta, Tampereelta, Jyväskylästä, Kuopiosta ja Espoosta. Bittimaateissa käytetään Bitsampin tarjoamaa vaihtokurssia +5 %. Ostosummat alkavat viidestä eurosta, ja se hyväksyy kaikki setelit 5 ja 500 euron välillä. Bittimaateilla on päivittäiset ostorajoitukset.

Kuva 3. Lamassu Bittimaatti. (Bittimaatti.fi 2014.)

Bittimaatin käyttö:

1. Ensin valitaan haluttu kieli.
2. Mobiililompakon QR-koodi asetetaan Bittimaatin lukijaan.
3. Syötetään haluttu määrä seteleitä ja painetaan ”lähetä bitcoinit”.

7 BITCOIN KEHITYSMAISSA

Bitcoin on tällä hetkellä käytännössä täysin Internet-verkon varassa ja kryptovaluuttoja käytetään lähinnä tietokoneilla ja mobiililaitteilla. Kehitysmaissa Internet-verkot eivät ole kaikkien saatavilla ja tietokoneet ja älypuhelinteknologia on köyhimmille liian kallista hankittavaksi. Kryptovaluuttojen tuominen kehitysmaiden ihmisten ulottuville on haasteellista tarpeellisen infrastruktuurin puuttuessa.

Lohkoketjuteknologiasta hyötyisivät kuitenkin mahdollisesti eniten ihmiset, joilla ei ole pääsyä kansainväliseen pankkitoimintaan tai joiden valtion virallinen valuutta on todella epävakaata. Kehitysmaiden pankkitoiminta saattaa usein olla korruptoitunutta ja epäluotettavaa.

Afrikasta, Etelä-Amerikasta ja Aasian köyhemmistä osista arvioidaan tulevan iso markkina bitcoinille. Kansainvälinen P2P-valuutta voisi voimaannuttaa ja parantaa ihmisten asemaa maailman köyhimmissä osissa. Se toisi myös mahdollisuuden kuluttaa rahaa verkossa ilman pankki- ja luottokortteja. Tämän myötä myös Internetissä tapahtuva kaupankäynti lisääntyisi. (Pew Research Center 2014.)

Tekninen infrastruktuuri

Virtuaalisen rahan laaja käyttöönotto on teknologinen haaste valtioissa joiden tekninen infrastruktuuri ei ole samalla tasolla kuin länsimaissa. Lohkoketjuteknologia on kuitenkin mukautuva eri tarpeisiin ja avoimen lähdekoodin ansiosta se on kenen tahansa muokattavissa.

Vaikka tietokoneet ja Internet tekevät hitaasti tuloa kehittyviin maihin, on matkapuhelinteknologia kuitenkin todella laajalti levinnyt ympäri maailmaa. Matkapuhelimen käyttöön perustuva maksaminen ja valuutan vaihto on jo joissain Afrikan maissa jo arkipäivää. Esimerkiksi Keniassa n. 68 % ja Ugandassa n. 50 % väestöstä käyttää jo nyt mobiilimaksamista säännöllisesti. (Pew Research Center 2014.)

7.1 Rahalähetykset ulkomaille

Monet maailman köyhimmistä ihmisistä ovat riippuvaisia rahalähetyksistä sukulaisilta tai ystäviltä ulkomailta. Maailmanpankin mukaan vuonna 2011 lähes puolet Tadžikistanin bruttokansantuotteesta on peräisin rahalähetyksistä, Liberiassa, Lesothossa, Nepalissa ja Haitilla määrä on yli viidesosta bruttokansantuotteesta. (Anderson, M. 2014.)

Vuonna 2013 ulkomaalaisten työntekijöiden rahasiirtojen määrä oli yli 400 miljardia dollaria vuodessa ja määrän arvioidaan kasvavan yli 500 miljardiin dollariin vuoteen 2016 mennessä. (The World Bank 2014.) Suurin osa rahalähetyksistä tehdään perinteisen pankkijärjestelmän ulkopuolella, koska rahaa lähettävä maahanmuuttaja on usein ilman virallisia papereita maassa ja vastaanottajan köyhällä seudulla ei useimmiten pankkeja ole. Pankkisiirrot ovat myös hitaampia kuin esimerkiksi Western Unionin kaltaiset rahansiirtopalvelut. (Unric.org 2014.)

Afrikkaan lähetettävien rahasiirtojen siirtomaksut ovat n. 1,8 miljardia Yhdysvaltain dollaria vuodessa. Summalla pystyisi maksamaan peruskouluopetuksen 14 miljoonalle lapselle tällä alueella. Heikko kilpailu, markkinoiden keskittyminen ja taloudellisen sääntelyn puute lisäävät siirtomaksujen hintaa Afrikassa. (Watkins, K. & Quattri, M. 2014.)

7.2 Hyväntekeväisyys ja mikrolainaaminen

Koska bitcoinin lähettäminen on ilmaista tai lähes ilmaista, mahdollistaa se ns. mikrofinanssit käyttäjien välillä. Mikrofinanssit käsittelee pieniä rahasummia, jotka pankista lainattuna olisivat kuluineen kannattamattomia. Rahaa lainataan P2P-periaattella, joten pankin haluamat korot ja siirtomaksut jäävät rahanvaihdosta pois.

Mikrolainaaminen tuo pankkipalvelut maailman ihmisille, joilla ei ole mahdollisuutta ottaa lainaa pankista. Palvelut kuten Kiva (Kiva 2014.) toimii sosiaalisen median tapaan verkostona ihmisille, jotka haluavat projekteilleen rahoitusta.

Lainan tarve voi olla vaikkapa uuden kaluston hankkimista intialaiselle maanviljelijälle tai opintojen rahoittamista perulaiselle opiskelijalle. Kivan kaltaiselle alustalle kuka tahansa voi helposti laittaa projektinsa ja rahoitustarpeensa ja useampi ihminen voi tähän lainaan osallistua.

Palveluun luodaan profiili ja selvitetään mihin rahaa olisi tarkoitus lainata. Laina maksetaan takaisin saman palvelun kautta ja takaisinmaksusuunnitelma on näkyvillä profiilissa. Rahaa voi lainata perinteisellä fiat–rahalla tai bitcoinilla. Bitcoinin joustavan luonteen takia rahansiirto on kustannustehokasta ja nopeaa.

7.3 M-Pesa

M-Pesa on teleoperaattori Vodacomin vuonna 2007 julkaisema mobiilimaksujärjestelmä Safaricomille ja Vodacomille, jotka ovat suurimmat mobiiliverkkooperaattorit Keniassa ja Tansaniassa. Sen toimintaa on laajennettu sen jälkeen mm. Afganistaniin, Etelä-Arfrikkaan, Intiaan ja Romaniaan. (M-Pesa 2014a.)

Palvelu tarjoaa tilin, johon ihmiset voivat tallettaa rahaa matkapuhelimiinsa ja lähettää sitä käyttäen SMS-viestejä. M-Pesa tukee myös laskujen mobiilimaksamista ja rahan voi nostaa tililtä käteisenä. Rahaliikenteestä otetaan kuitenkin palvelumaksu. (M-pesa 2014b.)

Bitpesa

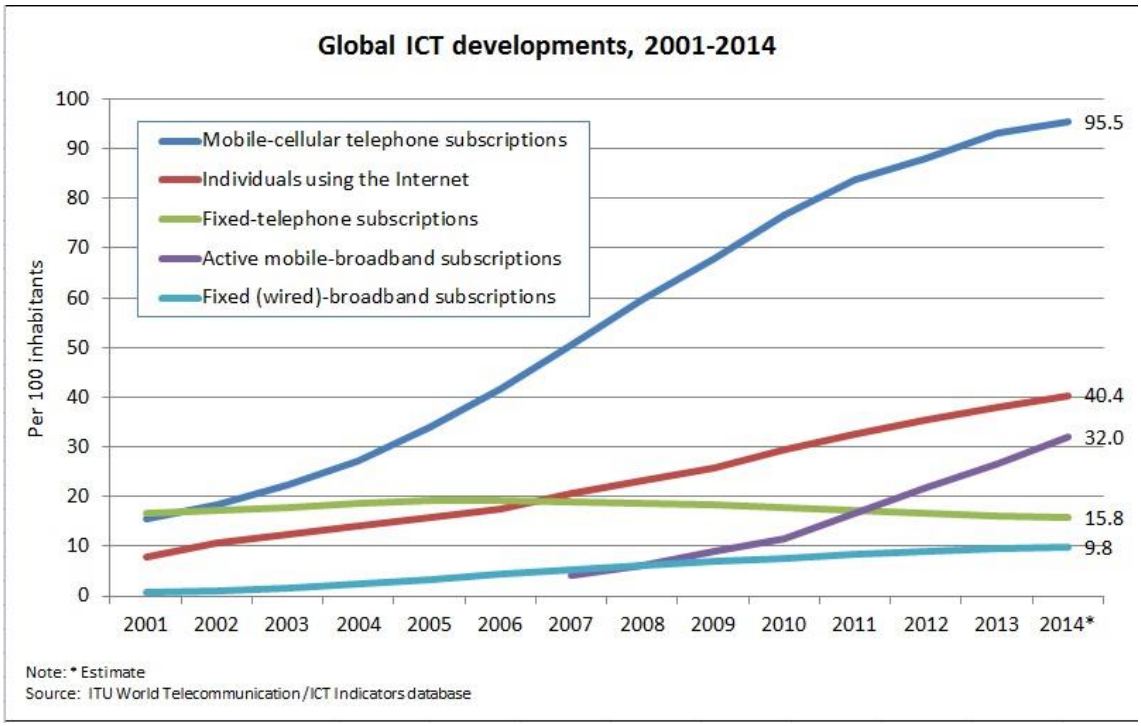
BitPesa tuo bitcoinin jo laajalti käytössä olevaan M-Pesa-alustalle. Se toimii valuutanvaihtona Bitcoinin ja fiat–valuutan välillä. Palvelun avulla voi lähettää bitcoineja M-Pesa-tilille. BitPesa hoitaa valuutanvaihdon bitcoineista Kenian shillingeiksi asiakkaan puolesta.

Bitcoinin lähettämisestä ei peritä lähetysmaksua, mutta BitPesa ottaa 3 % marginaalin valuutanvaihdosta. Rahan siirtyy vastaaottajan M-Pesa-tilille minuuteissa. Palvelu on tällä hetkellä halvin tapa lähettää rahaa Keniaan. (Bitpesa 2014.)

7.4 SMS-palvelut

Tekstiviestipohjaiset bitcoin-palvelut ovat vielä uusi ilmiö bitcoin-maailmassa. Vuonna 2014 on julkaistu useita eri palveluita joilla voi käyttää bitcoineja SMS-viestien välityksellä. Tämä on tärkeä edistysaskel tuoda kryptovaluutat kehittyvien valtion asukkaille, koska matkapuhelinteknologia on levinnyt myös maailman köyhimpiin osiin. Kuviossa 5 näkyy, että matkapuhelimen omistaa arviolta 95,5 % maapallon väestöstä.

SMS-lompakot ovat yksinkertainen tapa lähettää ja vastaanottaa bitcoineja. Tekstipohjaisen järjestelmän ansiosta mikä tahansa matkapuhelin muuntautuu helposti bitcoin-lompakoksi. Tekstiviestipohjaisia palveluita kehitetään koko ajan lisää ja niiden luotettavuus ja käytettävyys paranee innovaatioiden myötä.



Kuvio 5. Globaali IT-kehitys vuosina 2001-2014. (Satellitetoday.com 2014.)

SMS–toimintoa tarjoavat palvelut ovat (20.11.2014) seuraavat:

- Coinbase
    - Ensimmäisiä bitcoin-ekosfäärejä, joka tarjoaa valuutanvaihdon palvelun sisällä ja monipuoliset lompakkovaihtoehdot. Palveluun tehdään tili verkossa ja puhelinnumero verifioidaan, jonka jälkeen tekstiviestilompakko on valmis käytettäväksi. (Coinbase 2014.)

- Blockchain
    - Suosittu lompakkosovellus, joka toimii applikaationa puhelimessa sekä selaimen kautta. Selaimen lompakosta voi lähettää matkapuhelimeen yksityisen avaimen, joka generoidaan käyttäen javascriptiä. Vastaanottaja saa linkin, joka avaa selaimeen valintaruudun miten haluaa vastaanottaa bitcoinin. Sen voi liittää omaan Blockhain-lompakkoonsa tai siirtää johonkin toiseen lompakkoon kirjoittamalla lompakon osoitteen. Kopio lähetetystä yksityisavaimesta pidetään lähettäjän lompakossa, kunnes transaktio on verifioitu, jotta lähetyksen voi tarvittaessa perua. (Blockchain 2014.)
- 37Coins
    - 37Coinsin ydin on pelkästään bitcoinissa ja tekstiviesteissä. Se on suunnattu halvemmille Android-pohjaisille järjestelmille, jotka toimivat yksityisinä ”porttioperaattoreina”, jotka hyväksyvät tekstiviestitransaktion paikallisen puhelinnumeron ja Internet-yhteyden avulla. Porttioperaattorina toimimisesta saa palkkioksi pienen määrän bitcoinia kuin palvelumaksuna. Muut käyttäjät voivat lähettää bitcoineja käyttäen tavallisia matkapuhelimia, ja transaktiot varmennetaan porttioperaattoreiden kautta. (37coins 2014.)
- Coinkite
    - Coinkite tarjotaa monenlaisia bitcoin-lompakkoratkaisuja. Tekstiviestilompakko toimii samalla periaatteella kuin Blockchainissa, mutta tarjoaa muutaman turvallisuutta lisäävän ominaisuuden. Erillinen PIN-koodi vähentää varkauden mahdollisuutta ja SMS-

viestit tulevat palvelun omasta numerosta lisäten anonyymiyttä. Jos kaipaa vielä lisää tietoturvaa niin lompakkoon voi kirjautua käyttäen TOR-verkkoa. (Coinkite 2014.)

- Coinapult
    - Coinapult on ensimmäinen verkkolompakko joka tarjoaa bitcoinien lähettämisen sähköpostilla tai tekstiviestillä. Coinapultin erottaa kilpailijoistaan LOCKS-palvelu, jonka avulla voi sitoa bitcoinostoksensa arvon suoraan esimerkiksi kultaan tai yhdysvaltain dollariin. (Coinapult 2014.)

8 COINBASE TEKSTIVIESTILOMPAKON KÄYTTÖÖNOTTO

Valitsin Coinbase-lompakkopalvelun, koska se on tällä hetkellä suosituin bitcoin-palvelu ja ekosfääri, joka tarjoaa mahdollisuuden lähettää bitcoineja myös tekstiviestillä. Tekstiviestilompakot ovat yleisesti vielä kehitysasteella ja kaikki palvelut eivät toimi kaikissa maissa eri operaattorien liittymillä. Coinbasen toimintamalli on kuitenkin looginen ja esimerkkinä kilpailijoilleen.

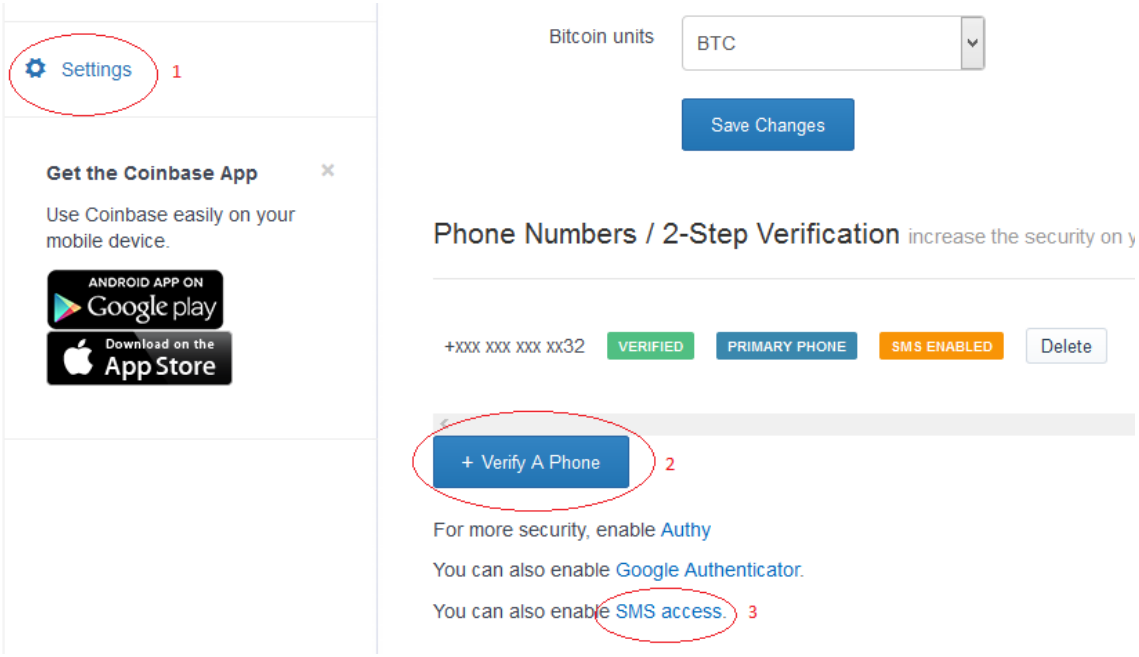
Kuvassa 4 näkyy Coinbase-palvelun etusivu johon luodaan tili syöttämällä haluttu sähköpostiosoite ja salasana.

Kuva 4. Coinbase etusivu.

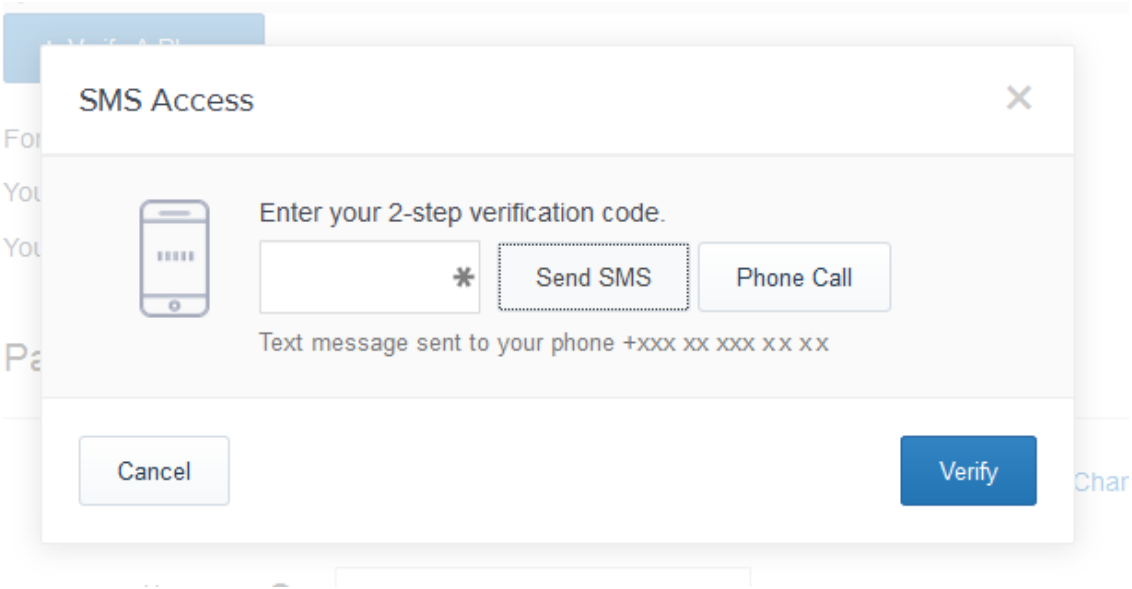
Kun tili on luotu pääsee sähköpostin ja salasanan avulla kirjautumaan Coinbase–selainlompakkoon. Jotta tekstiviestilompakon saisi käyttöön, täytyy ensin käydä verifioimassa oma puhelinnumero asetuksista. Kuvassa 5 on esitelty kolme kohtaa joiden avulla matkapuhelin rekisteröidään Coinbaseen.

1. Lompakkonäkymässä painetaan vasemmassa reunassa sijaitsevaa Settings, josta pääsee lompakon asetuksiin (kuva 5).
2. Puhelinnumero syötetään ja verifioidaan tekstiviestinä tulevalla koodilla (kuva 6).

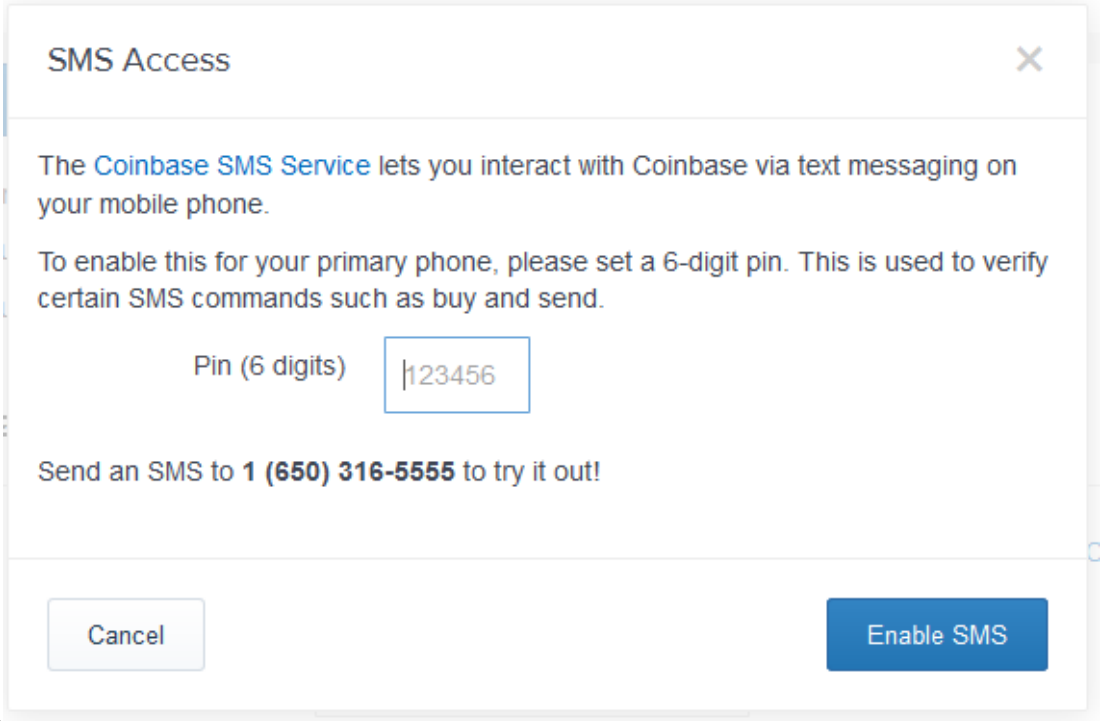
3. SMS Access -valikosta asetetaan käyttöön tekstiviestilompakko. Kuusinumeroinen PIN-koodi asetetaan, jotta Coinbasesta ei voi ostaa lisää bitcoineja tai lompakosta ei voi lähettää rahaa tietämättä tätä koodia (kuva 7).



Kuva 5. Coinbase-lompakon rajattu näkymä.



Kuva 6. Coinbase-lompakon tekstiviestipalvelun verifiointi.



.

Kuva 7. Coinbase-lompakon tekstiviestipalvelun PIN-koodin syöttö.

Kun tekstiviestilompakko on otettu käyttöön selaimessa, se toimii sen jälkeen ilman verkkoyhteyttä pelkän tekstiviestin välityksellä. Halutut komennot lähetetään Coinbasen numeroon 1 (650) 316-5555 ja haluttu tieto tulee paluuviestinä omaan puhelimeen

Tekstiviestilompakon komennot:

- Tilin saldo (**b** tai **bal**) lähettää sen hetkisen saldon.
- Transaktiot (**t** tai **txns**) näyttää tilin 3 viimeisintä transaktiota.
- Osoite (**a** tai **addr**) lähettää oman bitcoin-osoitteen.
- QR (**q**) lähettää QR-koodin kuvalinkkinä.
- Hinta (**p**) sen hetkinen BTC/USD kurssi Coinbasen palvelussa.
- Pyyntö (**r** tai **req**) pyydä bitcoineja sähköpostista tai puhelinnumerosta.
- Lähetä (**s**) lähetä bitcoineja sähköpostiin, puhelinnumeroon, tai bitcoin-osoitteeseen.
- Osta (**buy**) osta bitcoineja Coinbasesta.
- Myy (**sell**) myy bitcoineja.

9 POHDINTA

Lohkoketjuteknologia on vielä alkuvaiheessaan ja kryptovaluutat ovat vasta ensimmäinen applikaatio, joka tästä teknologiasta on kehittynyt. Bitcoinista innostuneet kehittäjät ja puolestapuhujat arvioivat lohkoketjuteknologian olevan yhtä tärkeä teknologinen innovaatio kuin Internet. Avoin lähdekoodi mahdollistaa vapaan kehityksen ja ideoiden leviämisen. Käyttäjät lopulta päättävät mitkä palvelut jäävät elämään ja mitkä unohdetaan.

Bitcoin on valuuttana vielä kehitysvaiheessa ja sen arvon heilahtelut tekevät siitä epävakaan. Vielä harva palvelu ja kauppias hyväksyy bitcoineja perinteisten valuuttojen sijasta, mutta kehitystä on tapahtunut paljon viime vuosina. Bitcoinin alkuaikoina sitä käytettiin lähes ainoastaan ”darknetin” puolella laittomien kauppojen tekemiseen, mutta maailmanlaajuisesti sitä aletaan hyväksymään yhä enemmän perinteisten rahojen kanssa kaupan välineenä.

Kehittyvillä valtioilla voi olla merkittävä rooli kryptovaluuttojen tulevaisuuden kannalta, koska ne ovat suuret markkinat vaihtoehtoisille maksumenetelmille ja valuutoille. Bitcoinin hyväksyntä Etelä-Amerikassa ja Aasiassa on ollut vaihtelevaa, kun sitä ollaan eri valtioiden ja pankkien tahoilta yritetty kontrolloida.

Lohkoketjuteknologia on keksintö jota ei voi enää peruuttaa. Sen etenemistä on minkään virallisen tahon vaikea lopulta estää, koska se toimii itsenäisenä organismina Internetissä käyttäjien välillä. Tämä kryptografinen innovaatio voi tuoda kokonaan uuden kerroksen ihmisten keskenäiseen kommunikointiin verkossa.

LÄHTEET

37coins 2014. SMSwallet. Viitattu 23.11.2014 https://www.37coins.com/en/.

Altcoin 2014. Bitcoin Wiki. Viitattu 20.9.2014 https://en.bitcoin.it/wiki/Altcoin.

Amores, R & Paganini, P. 2013. Digital virtual currency and Bitcoins. London: Amazon.co.uk.

Anderson, M. 2014. Bitcoin shakes up remittances as poorer people offered digital deals. 18.8.2014 The Guardian. Viitattu 28.10.2014 http://www.theguardian.com/global-development/2014/aug/18/bitcoin-remittances-market-digital-cash.

Anonymity 2014. Bitcoin Wiki. Viitattu 10.9.2014 https://en.bitcoin.it/wiki/Anonymity.

Bitcoin 2014. Wikipedia. Viitattu 2.12.2014 https://fi.wikipedia.org/wiki/Bitcoin.

Bitcoin Address 2014. Bitcoin Wiki. Viitattu 5.9.2014 http://en.bitcoinwiki.org/images/a/a6/BitcoinAddress.png.

Bitcoin Security 2014. What is Bitcoin? Viitattu 6.10.2014 http://www.bitcoinsecurity.org/wp-content/uploads/2012/07/block-chain.png.

Bitcoin.org 2014. Securing your wallet. Viitattu, 10.11.2014 https://bitcoin.org/en/secure-your-wallet.

Bitcoinarmory 2014. About Armory. Viitattu 20.9.2014 https://bitcoinarmory.com/about/about-armory/.

Bitpesa 2014. Frequently Asked Questions. Viitattu 17.11.2014 https://www.bitpesa.co/faq.

Bitstamp.net 2014. Yleisnäkymä. Viitattu 2.11.2014 https://fi.bitstamp.net/.

Bittimaatti.fi 2014. Galleria. Viitattu 26.11.2014 http://bittimaatti.fi/gallery.

Bittiraha.fi 2014. Bitcoinien osto. Viitattu 12.11.2014 https://bittiraha.fi/bitcoin/buy.

Blockchain 2014. Market Price (USD). Viitattu 23.10.214 (https://blockchain.info/charts/market-price?timespan=2year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address.

Blockchain 2014. Wallet. Viitattu 23.11.2014 https://blockchain.info/wallet.

Block chain 2014. Bitcoin Wiki. Viitattu 2.12.2014 https://en.bitcoin.it/wiki/Block_chain.

Bradbury, D. 2014. What's Next for Bitcoin Wallet Security? Viitattu 10.9.2014 http://www.coindesk.com/whats-next-bitcoin-wallet-security/.

BTCchina.com 2014. Yleisnäkymä. Viitattu 2.11.2014 https://www.btcchina.com.

Coinapult 2014. Yleisnäkymä. Viitattu 23.11.2014 https://coinapult.com/.

Coinbase 2014. Yleisnäkymä. Viitattu 2.11.2014 https://www.coinbase.com/home.

Coinkite 2014. FAQ Index. Viitattu 23.11.2014 https://coinkite.com/faq/.

Credit Card 2014. Wikipedia. Viitattu 10.11.2014 https://en.wikipedia.org/wiki/Credit_card.

Cryptograpgi Inc. 2014. Piper Wallet. Viitattu 20.11.2014 http://cryptographi.com/collections/frontpage/products/piper.

Deterministic wallet 2014. Bitcoin Wiki. Viitattu 28.11.2014 https://en.bitcoin.it/wiki/Deterministic_wallet.

Fiat-raha 2014. Sivistyssanakirja. Viitattu 2.12.2014 http://www.suomisanakirja.fi/fiat-raha.

Hardware wallet 2014. Bitcoin Wiki. Viitattu 2.11.2014 https://en.bitcoin.it/wiki/Hardware_wallet.

History of Bitcoin 2014. Wikipedia. Viitattu 4.10.2014 https://en.wikipedia.org/wiki/History_of_Bitcoin.

Introduction 2014. Bitcoin Wiki.Viitattu 5.9.2014 https://en.bitcoin.it/wiki/Introduction.

Kiva 2014. About Us. Viitattu 20.11.2014 http://www.kiva.org/about.

McMillan, R. 2014. The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster. Viitattu 23.10.2014 http://www.wired.com/2014/03/bitcoin-exchange/.

Mikrotaloustiede 2014. Sivistyssanakirja. Viitattu 2.12.2014 http://www.suomisanakirja.fi/mikrotaloustiede.

M-Pesa 2014a. FAQs. Viitattu 17.11.2014 https://www.mpesa.in/portal/customer/FAQ.jsp.

M-Pesa 2014b. Wikipedia. Viitattu 17.11.2014 https://en.wikipedia.org/wiki/M-Pesa.

Mt. Gox 2014. Wikipedia. Viitattu 23.10.2014 https://en.wikipedia.org/wiki/Mt._Gox.

Nakamoto, S. 2008 Bitcoin: A Peer-to-Peer Electronic Cash System. Viitattu 1.9.2014 https://bitcoin.org/bitcoin.pdf.

Operation Payback 2014. Wikipedia. Viitattu 23.10.2014 https://en.wikipedia.org/wiki/Operation_Payback.

Paper wallet 2014. Bitcoin Wiki. Viitattu 28.11.2014 https://en.bitcoin.it/wiki/Paper_wallet.

Pew Research Center 2014. Emerging Nations Embrace Internet, Mobile Technology. Viitattu 16.11.2014 http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-technology/.

Pooled mining 2014. Bitcoin Wiki.Viitattu 15.10.2014 https://en.bitcoin.it/wiki/Pooled_mining.

Satellitetoday.com 2014. Global ICT Development, 2001-2014. Viitattu 17.11.2014 http://cdn.satellitetoday.com/wp-content/uploads/2014/05/ICT-graph-ITU.jpg.

Securing your wallet. 2014. Bitcoin Wiki. Viitattu 10.11.2014 https://en.bitcoin.it/wiki/Securing_your_wallet

Tor-verkko 2014. Wikipedia. Viitattu 2.12.2014 https://fi.wikipedia.org/wiki/Tor_%28verkko%29.

Unric.org 2014. Remittances – A high-cost lifeline to developing countries. Viitattu 16.11.2014 http://www.unric.org/en/un-newsletter/29294-remittances-a-high-cost-lifeline-to-developing-countries viitattu 16.11.2014.

Watkins, K. & Quattri, M. 2014. Lost in intermediation: How excessive charges undermine the benefits of remittances for Africa. Viitattu 26.11.2014 http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/8901.pdf.

The World Bank 2014. Migration and Development Brief 22. Viitattu 16.11.2014 http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief22.pdf.

Verohallinto 2013. Virtuaalivaluuttojen tuloverotus. Viitattu 2.11.2014 www.vero.fi > Syventävät vero-ohjeet > Verhoallinnon ohjeet > Virtuaalivaluuttojen tuloverotus.

Vertaisverkko 2014. Wikipedia. Viitattu 2.12.2014 https://fi.wikipedia.org/wiki/Vertaisverkko.