Jay Zeng

Bitcoin ja tietoturva

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

18.04.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Jay Zeng Bitcoin ja tietoturva 32 sivua 18.04.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Janne Salonen, Osaamisaluepäällikkö

Insinöörityössä tutustuttiin syvemmin avoimeen lähdekoodiin pohjautuvaan Bitcoin-kryptovaluuttaan ja sen turvallisuuteen. Bitcoin on mielenkiintoinen niin vaihtokaupan välineenä kuin myös ”virtuaaliraha”-konseptina. Toisin kuin erilaiset viralliset Fiat-rahavaluutat Bitcoin on täysin riippumaton pankeista tai muista kolmannen osapuolen instituutioista.

Bitcoin-protokolla on täysin riippuvainen käyttäjistä ja heidän ylläpitämästä vertaisverkosta sekä siihen liittyvistä salausalgoritmeista. Insinöörityön tärkein tavoite oli Bitcoin-kryptovaluutan tietoturvallisuuden käsittely, mikä mahdollistaa sen olemassaolon ja käyttämisen turvallisena vaihtokaupanvälineenä.

Insinöörityön alkuosassa perehdyttiin lyhyesti Bitcoinin historiaan, peruskäsitteisiin ja teknisiin ominaisuuksiin. Tämän jälkeen työssä tarkasteltiin Bitcoin-vertaisverkkoa sekä käsiteltiin asiakasohjelmien välillä tapahtuvaa tietoliikennettä.

Työn loppuosa omistettiin täysin Bitcoinin tietoturvallisuudelle sekä anonymiteetille. Tietoturvallisuuteen paneuduttiin käsittelemällä erilaisia Bitcoin-protokollassa hyödynnettyjä salausalgoritmeja, kuten hajautusalgoritmia ja julkisen avaimen algoritmia. Teknologian kehittyessä ja salausten heikkouksien löytyessä tulevaisuudessa Bitcoin-protokollaan voidaan toteuttaa vahvempia ja uudempia salausalgoritmeja.

Insinöörityön pohdintaosiossa arvioitiin Bitcoinin tulevaisuutta ja tuotiin esille epäkohtia. Pohdinta sisältää myös omakohtaisen kokemuksen Bitcoin-verkosta, sovelluksista sekä vaihdantapalveluista.

Avainsanat	Bitcoin, virtuaalivaluutta, kryptografia, turvallisuus, anonymiteetti

Author(s) Title Number of Pages Date	Jay Zeng Bitcoin and security 32 pages 18 April 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Head of the Department

This thesis goal is to explore and have a closer look at open source cryptocurrency bitcoin and its security properties. Bitcoin is very interesting concept not only as cryptocurrency but as future payment method. Unlike traditional Fiat-money it is not controlled by government and is build self-sufficient not needing middleman like banks or any third-party institutes.

Bitcoin-protocol depends on network of users running Bitcoin-clients on distributed peer-to-peer network and cryptographic algorithm. The main goal of the thesis is to cover information security about Bitcoin's cryptographic currency which is fundamental to use Bitcoin as a safe payment method.

First part of thesis consists Bitcoin background, basic concepts and technical features including also walk through of Bitcoin peer-to-peer network and network traffic between nodes.

Secondly thesis was devoted entirely to Bitcoin security and anonymity. Security of Bitcoin system was approached by digging into cryptography hash functions and public key algorithms. As technology advances and cryptographic weaknesses are found in future, it is possible to keep Bitcoin secured by implementing stronger and newer algorithms.

The end of thesis evaluates the future of Bitcoin and disadvantages. The evaluation also includes a personal experience of Bitcoin's network, applications, and exchange services.

Keywords	Bitcoin, virtual currency, cryptography, security, anonymity

Sisällys

Lyhenteet

BTC	Bitcoinin valuuttatunnus vastaavasti esim. Euroopan unionin yhteisen valuutan lyhenne on EUR.
P2P	Peer-to-peer. Vertaisverkossa useat yksittäiset tietokoneet voivat olla yhteydessä toisiinsa tietokoneohjelmistojen avulla. Bitcoinin kohdalla vertaisverkkoa hyödynnetään transaktiotietojen välittämisessä muille Bitcoin-käyttäjille ilman keskitettyä palvelinta.
IP	Internet Protocol. TCP/IP-mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa.
Node	Solmu tai yhtymäkohta, jolla tarkoitetaan Bitcoinissa käyttäjän tietokoneella olevaa asiakasohjelmaa. Maailmanlaajuinen Bitcoin-verkko muodostuu asiakasohjelmista, jotka ovat yhteydessä toisiinsa ilman keskitettyä palvelinta.
ASIC	Application-specific integrated circuit eli sovelluskohtainen mikropiiri. ASIC-piirejä kehitetään tiettyjä tehtäviä varten, kun halutaan esimerkiksi säästää piirilevyn pinta-alaa tai minimoida tehonkulutusta.
ECDSA	Elliptic Curve Digital Signature Algorithm. ECDSA on digitaalisen DSA avaimen variantti, joka hyödyntää elliptisen käyrän kryptografiaa.
SHA-256	Secure Hash Algorithm on yleisesti käytetty kryptografinen tiivistefunktio. Numero 256 tarkoittaa tiivisteen pituutta ja samalla ilmaisee suojauksen vahvuutta.
Hash	Hajautusarvo eli tiivisteellä voidaan tarkistaa tiedon eheys, muuttumattomuus tai identtisyys.

1 Johdanto

Tämän lopputyön tarkoituksena on tarkastella ja syventyä tarkemmin avoimeen lähdekoodiin perustuvaan digitaaliseen valuuttaan Bitcoiniin ja sen turvallisuuteen. Kyseisen kryptovaluutan avulla käyttäjät voivat lähettää BTC-rahayksiköitä toisilleen ilman keskitettyä tahoa, kun vastaavasti perinteisten eurojen lähettäminen käyttäjältä toiselle tapahtuu pankkien välityksellä. Bitcoineja hyväksytään maksuvälineenä Suomessa esimerkiksi useissa verkkokaupoissa, ravintoloissa ja jopa lentolippujen ostamiseen. Bitcoin ei ole enää pelkkä ohimenevä ilmiö, sillä yhä useammat palvelun tarjoajat hyväksyvät Bitcoineja maksuvälineinä.

Lopputyön teoriaosuudessa käsitellään aluksi yleisellä tasolla Bitcoin-kryptovaluuttaa ja sen toimintaperiaatteita. Kryptografiaa käytetään hyvin laajasti Bitcoinissa ja sen vuoksi työssä katsastetaan myös julkisen salauksen menetelmää sekä salausavaimia. Työssä käydään tarkemmin Bitcoinin peruskäsitteet, eri komponentit ja vertaisverkon hyödyntäminen verkkoliikenteessä.

Lopuksi työssä tarkastellaan Bitcoinin tietoturvaa ja siinä käytettyjen salausalgoritmien vahvuuksia sekä heikkouksia. Salausalgoritmien turvallisuus on digitaaliselle valuutalle välttämättömyys. Valuutalla ei ole varsinaisesti fyysistä muotoa, kaikki tieto on tallennettu verkkoon. Salausalgoritmien heikkouksia pyritään jatkuvasti etsimään erilaisilla testauksilla ja menetelmillä.

Bitcoinin toimiessa verkon välityksellä on hyvin tärkeää pitää huolta tietoturvasta. Kaikki Internetissä toimivat palvelut ja laitteet ovat alttiita verkkorikollisuudelle. Digitaalisen valuutan anonymiteetti koetaan usein vahvuutena, mutta Bitcoinin mahdollistamaa anonymiteettiä on käytetty hyväksi myös rikollisessa toiminnassa, kuten huume- ja asekaupoissa.

2 Bitcoin

2.1 Yleisesti ja toimintaperiaate

Bitcoin on ensimmäinen ja tunnetuin digitaalinen valuutta, joka on toteutettu avoimen lähdekoodin periaatteella. Vuonna 2008 marraskuuta Satoshi Nakamoton pseudonyymi lähetti ensimmäisen kerran viestin metzdown.comin postituslistalle ja kuvaili Bitcoinien toimintaa julkaisulla Bitcoin: A Peer-to-Peer Electronic Cash System. [1; 2.] Verkon toiminta alkoi 2009 tammikuussa, kun ”Bitcoin-Qt” -niminen asiakasohjelma julkaistiin, mikä myöhemmin päivitettiin ja nimettiin uudelleen Bitcon Coreksi. [3.]

Valuuttana toimivat kolikoiden lyhenteet ovat BTC ja XBT sekä merkki ฿. Yksi BTC voidaan jakaa pienimmillään 100 miljoonaan osaan (0,00000001 BTC), ja pienin yksikkö on nimeltään Satoshi. Bitcoin-valuuttaa kutsutaan myös kryptovaluuttaksi, virtuaalivaluutaksi, bittirahaksi ja Internet-rahaksi. [4.]

Bitcoin-verkkoa ei hallinnoi yksittäinen taho tai keskuspankki. Verkkoa ylläpitää sen käyttäjät. Internetin välityksellä käyttäjät voivat lähettää ja vastaanottaa valuuttaa keskenään ilman, että kolmas osapuoli varmistaisi niiden autenttisuuden. Bitcoinin arvo muihin virallisiin FIAT-valuuttoihin määräytyy täysin kysynnän ja tarjonnan perusteella kuten myös kullan ja muiden hyödykkeiden arvo. Bitcoinien ostaminen ja myyminen onnistuu perinteisillä euroilla tai dollareilla vaihdantapalveluiden kautta. Vaihtoehtoisesti Bitcoinien ostaminen onnistuu myös euroseteleillä bittimaattien avulla, joista maailman ensimmäinen automaattilaite lanseerattiin Helsingin rautatientorin asematunnelin tiloihin vuoden 2013 lopussa. [5.]

Bitcoin on hajautetusti toimiva massiivinen julkinen kirjanpitotietokanta ja maailmanlaajuinen maksujärjestelmä. Kirjanpitotietokantaa kutsutaan lohkoketjuksi, joka sisältää kaikki Bitcoinin siirtotapahtumat ensimmäisestä siirrosta alkaen sisältäen tiedot käytetyistä Bitcoin-osoitteista ja siirretyistä Bitcoineista. Tietokanta on julkinen ja kuka tahansa voi tarkistella ja varmistaa siirtotapahtumien oikeellisuuden tai esimerkiksi tietyn Bitcoin-osoitteen sisältämän kolikoiden määrän. Lohkoketjujen ensisijainen tarkoitus on varmistaa, että Bitcoin-osoitteissa olevia rahoja ei voi käyttää kuin yhden kerran pitäen kirjaa käytetyistä ja käyttämättömistä kolikoista. Samojen kolikoiden kuluttaminen useampaan kertaan on ratkaistu kryptografisella menetelmällä, jonka tarkoituksena on tehdä aikaisempien siirtojen muuttaminen lohkoketjussa hyvin vaikeaksi.

Verkon ylläpito vaatii suuren määrän laskentatehoa ja sitä kutsutaan myös louhimiseksi. Louhimisen sivutuotteena syntyy uusia kolikoita kiertoon. Louhijat palkitaan Bitcoineilla aina uuden löydetyn lohkon yhteydessä. Prosessin tarkoituksena on vahvistaa verkossa kuulutetut siirtotapahtumat ja vahtia verkon sääntöjen noudattamista. Kaikki vahvistetut siirtotapahtumat tallennetaan uuteen lohkoon ja peräkkäiset lohkot muodostavat näin ollen lohkoketjun.

Digitaalisen valuutan liikkeellelasku tapahtuu ennalta määrätyn matemaattisen geometrisen sarjan mukaisesti. Bitcoinien kokonaismäärä on rajallinen ja kaikkiaan Bitcoineja voi olla hieman alle 21 miljoonaa kappaletta. Bitcoinien liikkeellelasku puoliintuu 210 000 lohkon välein ja tämän hetkisen verkon laskentatehon perusteella noin 99,9 % Bitcoineista on luotu vuoteen 2040 menneessä. Vuoden 2017 alussa Bitcoineja on luotu 16 miljoonaa kappaletta, joka on noin 76 % kokonaismäärästä. [6.] Kun viimeisetkin Bitcoinkolikot on luotu, ei palkkiota enää makseta eikä uusia Bitcoineja synny kiertoon. Tämä tapahtuu arvioilta vuonna 2140. Näin Bitcoinien tarjonta on ennalta määrätty ja on kaikkien käyttäjien tiedossa. [2.]

2.2 Kryptografia

Bitcoinien omistajuus määritellään digitaalisten avaimien, Bitcoin-osoitteiden ja digitaalisten allekirjoitusten avulla. Digitaalisia avaimia voidaan luoda ja tallentaa tiedostoihin tai yksinkertaisiin tietokantoihin, joita kutsutaan lompakoiksi. Salaisia avaimia ei tallenneta Bitcoin-verkkoon, mutta esimerkiksi verkkolompakko tai vaihdantapalveluissa salaiset avaimet ovat luonnollisesti vaihdantapalveluiden ylläpidossa. Lompakkojen avaimet ovat täysin riippumattomia Bitcoin-verkosta ja näitä voidaan luoda lompakko-sovelluksilla, ilman Internet yhteyttä. Salausavaimet mahdollistavat Bitcoinin hajautetun toimintamallin ja kryptografisen turvallisuusmallin. [15.] Kryptografisia tiivistefunktiota käytetään Bitcoinissa hyvin laajasti, kuten Bitcoin-osoitteissa, transaktioissa, digitaalisissa allekirjoituksissa ja louhinnassa.

Bitcoin-järjestelmä perustuu julkisen avaimen kryptografiaan, joka tunnetaan nimellä epäsymmetrinen salaus. Menetelmässä salausavaimet ovat toisistaan riippuvaisia, joista yksi on julkinen ja toinen on salainen avain. Epäsymmetrisellä salausmenetelmällä tarkoitetaan menetelmää, missä viesti salataan eri avaimella kuin millä se puretaan. Sa-

lausavaimilla on aina matemaattinen yhteys, mutta vahvojen salausalgoritmien ja vaativien laskutoimitusten vuoksi yksityistä avainta on lähes mahdotonta päätellä pelkän julkisen avaimen avulla. [20.]

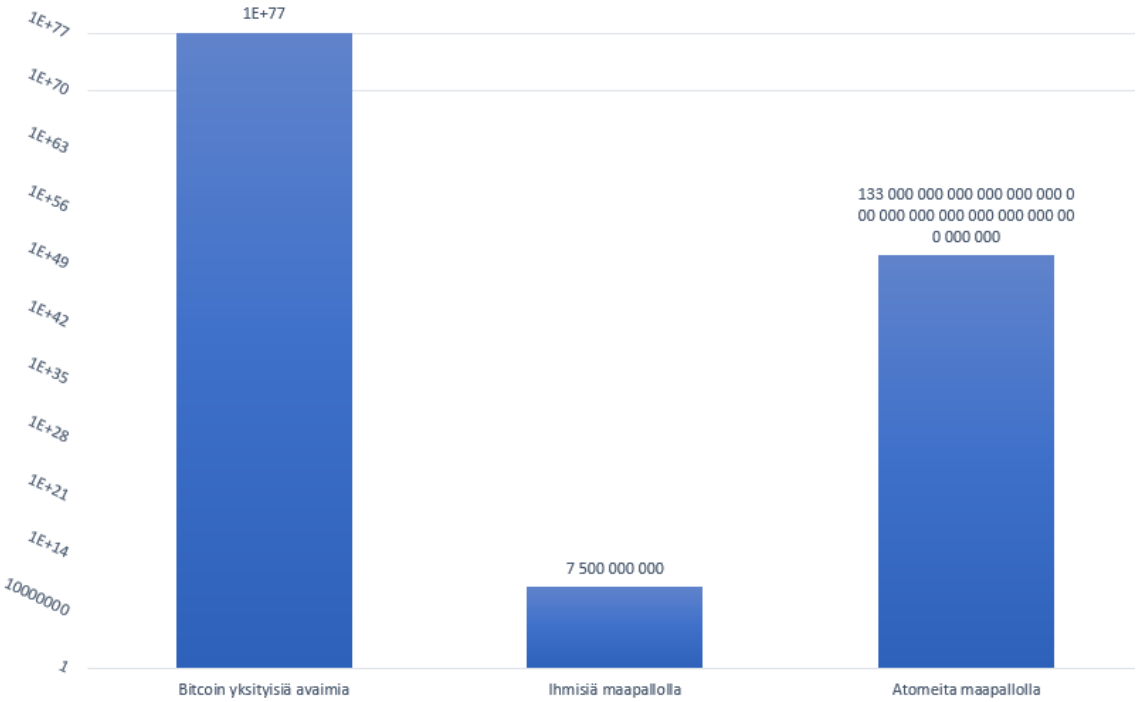
Viestin salaaminen tehdään käytännössä viestin vastaanottajan julkisella salausavaimella, joka voidaan julkaista muiden nähtäväksi. Salattu viesti voidaan avata ainoastaan julkisen avaimen yksityisellä salausavaimella, joka on pelkästään viestin vastaanottajan tiedossa. Bitcoinissa salausavaimet koostuvat myös avainparista eli yksityisestä avaimesta ja julkisesta avaimesta.

Bitcoinissa julkista avainta voidaan verrata esimerkiksi pankkitilinumeroon, jonka avulla voidaan vastaanottaa valuuttaa. Yksityistä avainta vastaavasti PIN-koodiin tai allekirjoitukseen. Bitcoinin luotettavuus pohjautuu siihen, kuinka hyvin käyttäjät pitävät yksityisavaimensa salassa. Käyttäjät harvemmin näkevät salausavaimia, sillä suurin osa avaimista säilytetään lompakkotiedostoissa, jota hallinnoi lompakkosovellus.

2.2.1 Yksityinen avain

Bitcoinin yksityinen avain (private key) on salainen tieto ja on yksinkertaisuudessaan vain satunnainen kokonaisluku. Yksityisen avaimen avulla luodaan digitaalinen allekirjoitus, jota vertailemalla voidaan todistaa Bitcoin-osoitteen omistajuus. Tämä tarkoittaa sitä, että kuka vain henkilö pystyy käyttämään Bitcoin-osoitteen sisältämiä varoja, mikäli yksityinen avain on tiedossa. Salauksen murtaminen on mahdotonta sen vahvan salaus algoritmin ansiosta. On tärkeää pitää yksityisestä avaimesta huolta, sillä avaimen hukkuessa Bitcoin-osoitteella olevia varoja ei pystytä enää käyttämään tai palauttamaan. Vastaavasti Bitcoin-kolikot voidaan varastaa, mikäli yksityinen avain paljastuu muiden nähtäväksi.

Yksityiset avaimet ovat Bitcoinissa tyypillisesti 256-bittisiä numeroita ja erilaisia avaimia on näin ollen 2^{256} kappaletta. Todellisuudessa käytettävissä olevia yksityisiä avaimia on noin 10^{77} kappaletta, joka on hieman vähemmän kuin 2^{256}. [15.] Osa uudemmista lompakoista käyttää myös 128 – 512-bittisiä numeroita. [8.] Kymmenen potenssiin 77 on äärettömän iso luku tarkoittaen 77 kappaletta nollia, kun esimerkiksi miljardissa on 9 nollaa. Maailman väkiluku on suunnilleen 7,5 miljardia. Bitcoin-järjestelmässä käytettäviä yksityisiä avaimia on paljon enemmän kuin esimerkiksi atomeita maapallolla, kuten kuvassa 1 nähdään. Atomien lukumäärä maapallolla on arviolta noin 1.33×10^{50}. [19.]



Kuva 1. Logaritminen kaavio Bitcoin yksityisten avaimien määrästä verrattuna ihmisten ja atomien lukumäärään maapallolla.

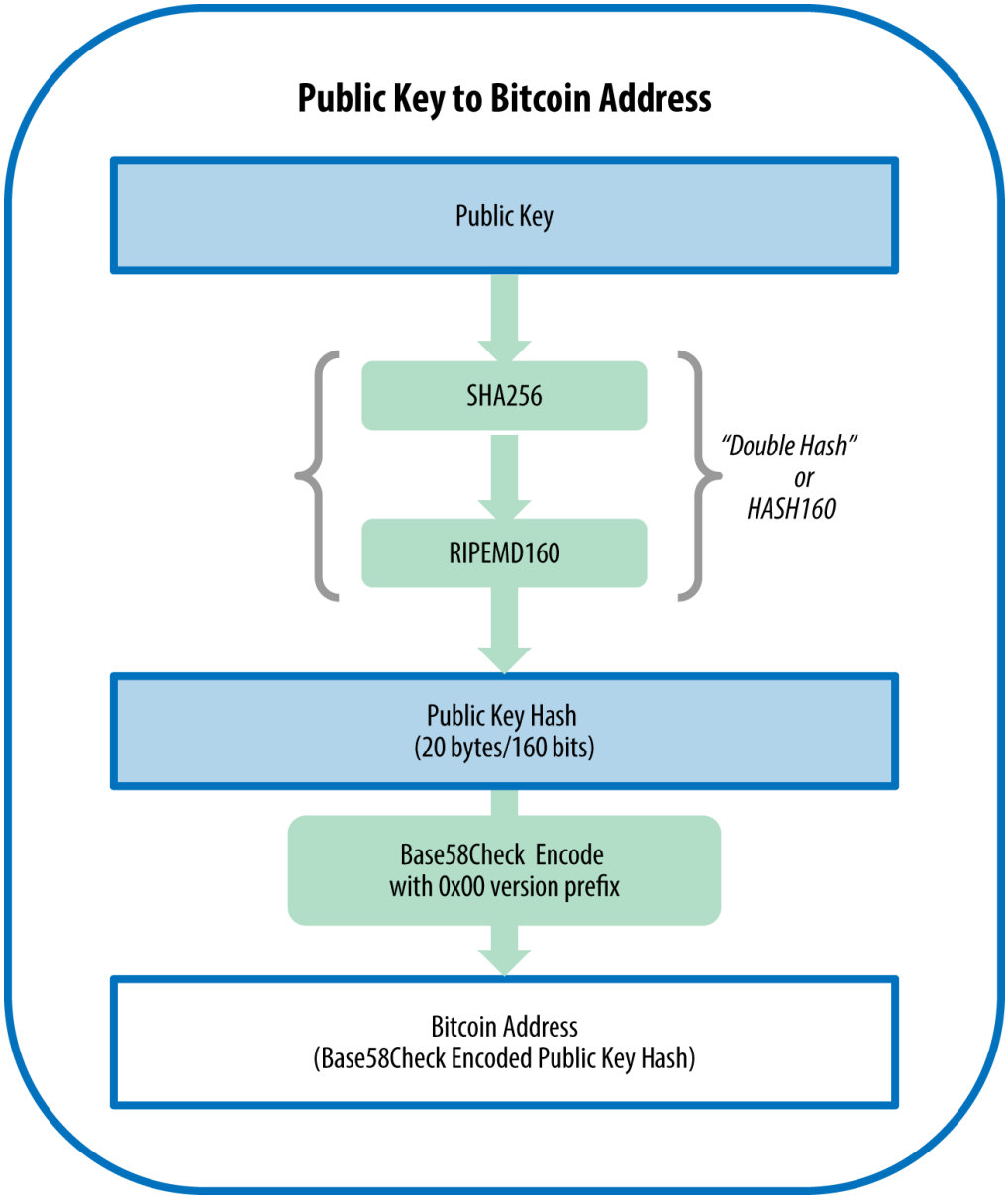
Yksityisten avaimien ollessa numeroita on aina mahdollista joskin epätodennäköistä, että kaksi eri tahoa luovat identtisen yksityisen avaimen. Siinä tapauksessa molemmat tahot pystyisivät käyttämään Bitcoin-kolikoita tästä johdetusta Bitcoin-osoitteesta. Todennäköisyys tällaiselle tapahtumalle on erittäin pieni ja teoriassa lähes mahdotonta suuren salausavainavaruuden vuoksi. [16.] Tätä todennäköisyyttä voidaan verrata esimerkiksi kolikonheittoon, jossa kolikkoa heitetään 256 kertaa peräkkäin. Jokainen kolikonheitto päättyy joko kruunaan tai klaavaan, joita voidaan verrata binäärinumeroihin. Saman identtisen yksityisen avaimen luominen vaatisi täsmälleen samat 256 kolikon heittämistä samalla tavalla.

2.2.2 Julkinen avain ja Bitcoin-osoite

Julkinen avain lasketaan yksityisestä avaimesta käyttäen yksisuuntaista elliptisen käyrän salausmenetelmää. Tämä tarkoittaa sitä, että julkisen avaimen takaisin mallintaminen yksityiseksi avaimeksi on vaikeaa ja vie aikaa, mutta kuitenkin mahdollista yrittämällä kaikkia mahdollisia, kunnes oikea arvo löytyy. Tätä kutsutaan brute-force-hyökkäykseksi.

Julkinen avain ei ole täysin sama asia kuin Bitcoin-osoite. Osoitteet johdetaan julkisesta avaimesta laskemalla tälle kolmet yksisuuntaiset tiivistefunktiot SHA-256 (Secure Hash

Algorithm) ja RIPEMD160 (RACE Integrity Primitives Evaluation Message Digest) sekä lopuksi tehdään Base58Check-koodaus. [15.] Kuvassa 2 havainnollistetaan, kuinka Bitcoin-osoite muodostuu julkisesta avaimesta laskemalla tälle useita tiivistefunktioita. Julkinen avain kuulutetaan tietoturvasyistä verkkoon vasta siinä vaiheessa, kun Bitcoin-osoitteesta kuulutetaan siirtotapahtuma verkkoon. Jokaiseen julkiseen avaimeen liittyy vähintään yksi yksityinen avain.



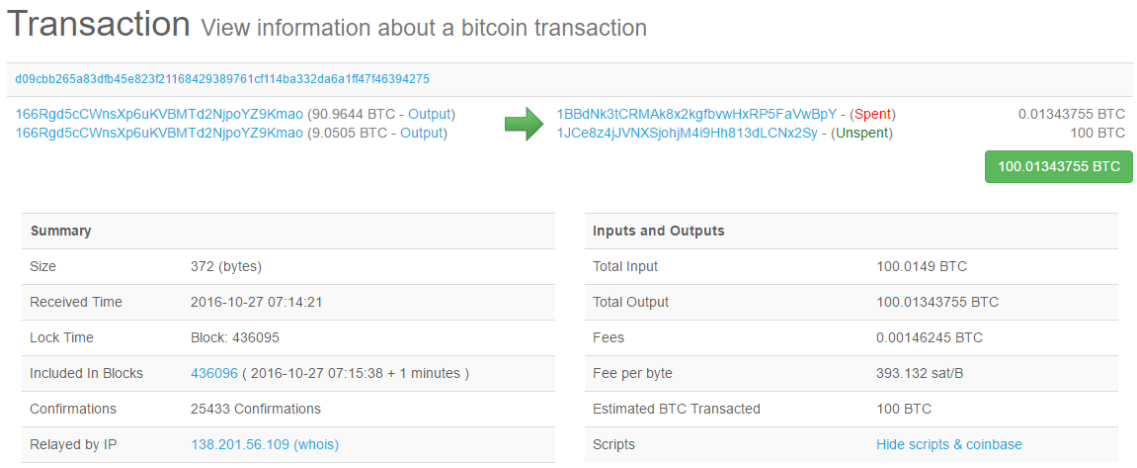
Kuva 2. Julkisen avaimen muuttaminen Bitcoin-osoitteeksi. [15.]

Uuden Bitcoin-osoitteen luominen ei vaadi yhteydenottoa muihin Bitcoin-verkon solmuihin ja niitä voidaan luoda käyttöön lähes rajattomasti. Käyttäjällä voi olla monia eri osoitteita käytössä ja eri osoitteiden käyttäminen siirtotapahtumissa edesauttaa käyttäjän anonymiteetin säilyttämistä.

2.3 Transaktiot

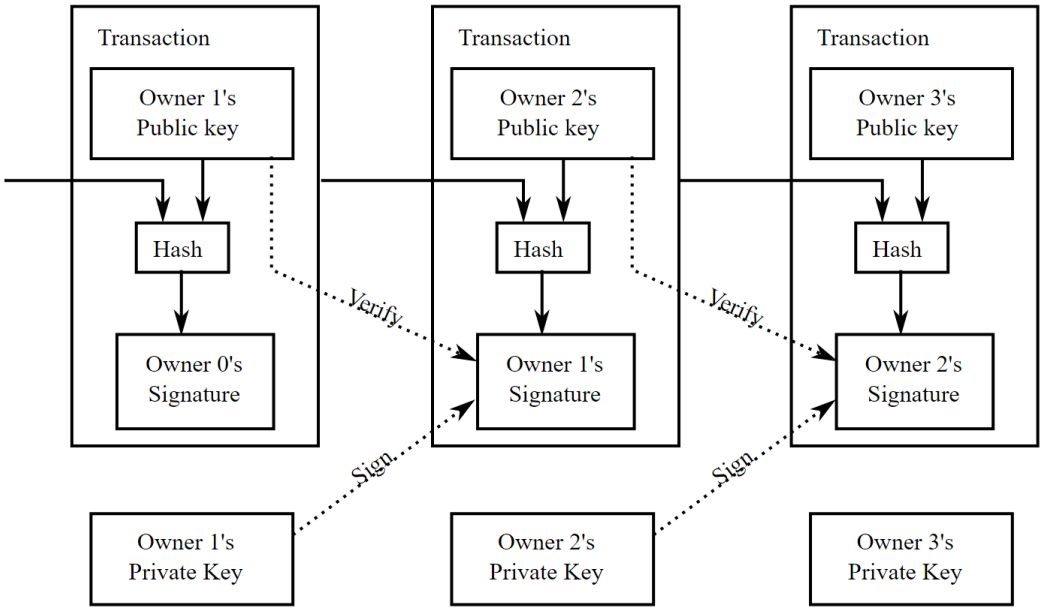
Transaktiot eli siirtotapahtumat tarkoittavat Bitcoinien siirtämistä aiemmasta osoitteesta uudelle osoitteelle. Käytännössä tämä tapahtuu niin, että transaktio kuulutetaan verkkoon, joka lopulta kerätään uuteen lohkoon, kunnes lohko lopulta ratkaistaan louhijoiden toimesta. Transaktioiden hyväksyminen kestää keskimäärin 10 minuuttia, mutta Bitcoinien kasvaneen suosion myötä siirtotapahtumien hyväksyminen voi kestää tunnin tai pidempään. Jos transaktiota ei ole hyväksytty 72 tunnin aikana, varat palautetaan käyttäjälle alkuperäiseen Bitcoin-osoitteeseen. [11.]

Coinbase-transaktio tapahtuu aina uuden lohkon löydyttyä. Coinbase-transaktio on ainoa tapa luoda uutta valuuttaa järjestelmään ja nämä siirretään palkkioina verkkoa ylläpitäville louhijoille. Julkisen lohkoketjun avulla jokaista siirtotapahtumaa voi tarkastella kuka tahansa, jolloin kolikot voidaan aina jäljittää edellisiin osoitteisiin ja lopulta alkuperäisiin coinbase-transaktioihin. Kuvassa 3 nähdään siirtotapahtuma, jossa siirretään 100 Bitcoinia toiseen osoitteeseen ja ~0.0134 Bitcoinia maksetaan siirtokuluina verkkoa ylläpitäville louhijoille. Kuvasta nähdään myös aikaleima, lohkon numero ja transaktion kuuluttajan IP-osoite.



Kuva 3. Transaktiossa siirretään 100 Bitcoinia toiseen osoitteeseen.

Uusi siirtotapahtuma sisältää tyypillisesti siirrettävien kolikoiden alkuperäisten transaktioiden tiivisteet, lähetettävien kolikoiden määrän, vastaanottajan Bitcoin-lompakon osoitteen ja digitaalisen allekirjoituksen. Bitcoin-valuutta ei ole yksittäisinä tiedostoina tietokoneilla tai fyysisessä muodossa seteleinä, vaan ovat ketju digitaalisia allekirjoituksia Bitcoin-verkossa kuten kuvassa 4 nähdään. Hyväksytyt siirtotapahtumat tallennetaan pysyvästi lohkoihin, jonka jälkeen Bitcoinit ovat uuden omistajan käytettävissä.



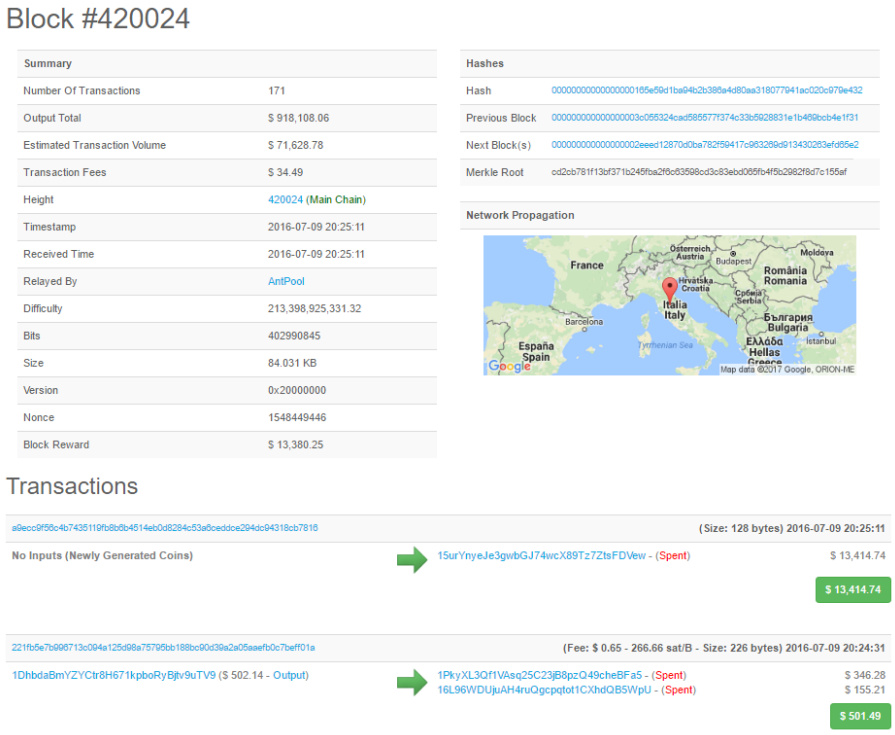
Kuva 4. Bitcoin-kolikoiden omistajuuden siirtyminen käyttäjältä toiselle [1.]

Bitcoinien omistajuus määritellään elliptisen käyrän digitaalisella allekirjoituksella, joiden käyttäminen onnistuu vain nykyisen hetken omistajan yksityisellä avaimella. Tarkastellaan esimerkiksi kuvassa 4 keskimmäistä transaktiota, jossa siirretään Bitcoineja 2. omistajalta kolmannelle omistajalle. Kyseinen transaktio sisältää 1. omistajan siirtotapahtuman tiivisteen, koska 3. omistajan täytyy tietää Bitcoinien alkuperä. Transaktio pitää sisällään myös 2. omistajan julkisen avaimen, 3. omistajan Bitcoin-osoitteen ja toisen omistajan yksityisen avaimella tehdyn allekirjoituksen. Näiden tietojen avulla 3. omistaja pystyy todentamaan, että Bitcoinit on varmasti lähetetty kolmannen omistajan Bitcoin-osoitteeseen ja että 2. omistajalla oli oikeus käyttää näitä Bitcoineja. Tämän jälkeen 3. omistaja voi lähettää Bitcoinit eteenpäin allekirjoittamalla uuden transaktion yksityisellä avaimella.

2.4 Lohko ja lohkoketjut

Aivan ensimmäistä Bitcoin-lohkoa kutsutaan nimellä ”Genesis block” ja tämä niin sanotusti kovakoodattu eli valmiiksi kirjoitettu ohjelmiston lähdekoodiin. Genesis block on siitä erikoinen, että se eroaa muista Bitcoin-lohkoista siten, että siinä ei ole viittausta edeltävään lohkoon. Uusi lohko sisältää aina edeltävän lohkon tiivisteen ja näin peräkkäiset lohkot muodostavat kronologisen lohkoketjun (Blockchain), joka on linkitetty aivan ensimmäiseen lohkoon. [9.]

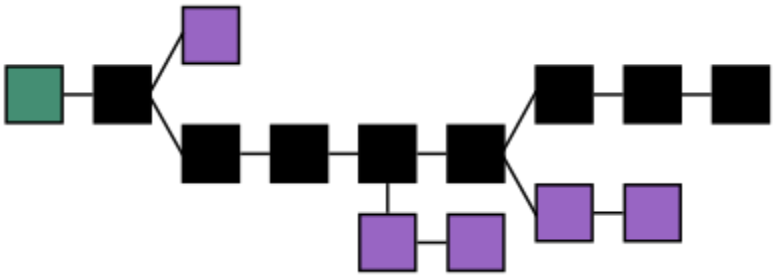
Kaikki hyväksytyt siirtotapahtumat tallennetaan pysyvästi tiedostoihin, ja näitä kutsutaan lohkoiksi (Block). Uusia lohkoja syntyy noin 10 minuutin välein, jota säädetään Bitcoin-järjestelmässä vaikeustasolla. Verkko asettaa lohkoilta vaadittavaa vaikeustasoa 2016 lohkon välein siten, että uusia lohkoja syntyy keskimäärin kuusi kertaa tunnissa. Uuden lohkon löydettyä louhijat palkitaan Bitcoineilla coinbase-transaktion kautta, mikä on ainoa tapa luoda Bitcoineja lisää verkkoon. Lohkojen ratkaisemisesta palkittiin aluksi 50 Bitcoinilla. Palkkio puoliintuu ajan myötä aina 210 000 lohkon välein, joka tarkoittaa suunnilleen 4 vuotta. Lohkoja voidaan luoda rajattomasti, myös sen jälkeen, kun viimeisetkin Bitcoinit on luotu vuoteen 2140 mennessä. [9.] Kuvassa 5 nähdään #420024 lohkon tiedot ja alempana osa lohkon transaktioista.



Kuva 5. Lohko #420024 (blockchain.info).

Lohkon voi mieltää esimerkiksi perinteisen kirjanpidon yhdeksi sivuksi, jossa transaktiot ovat järjestyksessä aikaleimojen perusteella. Uusia siirtotapahtumia työstetään verkossa jatkuvasti louhintaprosessin menetelmällä. Lohkoon sisällytetään vain sääntöjä noudattavat transaktiot. Kun lohko hyväksytään Bitcoin-verkon toimesta, sitä ei voida enää muuttaa tai poistaa.

Mikäli samanaikaisesti syntyisi useita lohkoja, vain yksi niistä huomioidaan, jolloin siitä tulee osa lohkoketjua. Lohkoketjun haarautuminen on mahdollista, jos kaksi lohkoa ratkaistaan lähes samaan aikaan. Tämän tapahtuessa osa verkon solmuista työstää ensimmäisen lohkon jatkoa, kun taas toiset työstävät toisen lohkon jatkoa riippuen siitä, kumpi lohko heille on ensin kuulutettu. Seuraavan lohkon ratkeamisen myötä päästään verkon yhteisymmärrykseen, jolloin pidempi haara liitetään osaksi lohkoketjua. Lyhyempää lohkohaaraa ei käytetä mihinkään, ja kaikki Bitcoin-verkon solmut siirtyvät työstämään pidemmän haaran lohkoketjua. [2.] Kuvassa 6 nähdään lohkoketjujen muodostuminen ja violetilla haarautuneet lohkot, joita ei huomioida.



Kuva 6. Lohkoketjun muodostuminen ja haarautuminen. [10.]

Lohkoketjutekniikan avulla toisilleen tuntemattomat tahot voivat yhdessä tuottaa ja ylläpitää tietokantaa hajautetusti. [16.] Lohkoketju on edellytys Bitcoinin olemassaololle, sillä sen läpinäkyvyyden ansiosta kuka tahansa voi todentaa ja tarkastaa jokaisen verkossa tehdyn transaktion esimerkiksi web-pohjaissilla käyttöliittymillä, kuten https://blockchain.info tai https://blockexplorer.com. Lohkoketjua ylläpidetään hajautetusti ympäri maailmaa käyttäjien toimesta, jonka takia lohkon muokkaaminen jälkikäteen on käytännössä mahdotonta, sillä se vaatisi näin ollen kaikkien muokattujen lohkojen jälkeen myös uusien syntyneiden lohkojen muokkaamisen. Tämä vaatisi erittäin paljon laskentatehoa ja on lähes mahdotonta, koska vastassa olisi käytännössä muut Bitcoin-verkon louhijat.

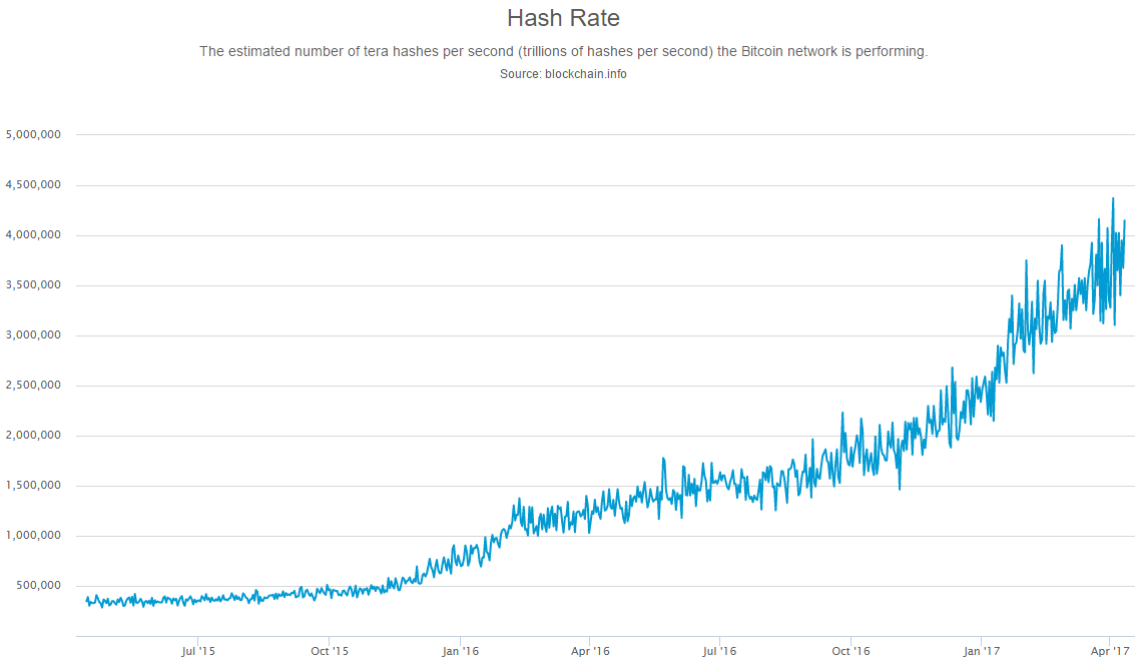
2.5 Louhinta ja laskentatyön todistaminen

Bitcoin-järjestelmässä verkon ylläpitoa kutsutaan usein louhinnaksi. Se on ainoa tapa, jolla Bitcoineja syntyy kiertoon. Uusien lohkojen löytyessä todennetaan myös verkkoon kuulutetut siirtotapahtumat. Käytännössä louhintaan tarvitaan tietokone ja Bitcoin-sovellus ratkaisemaan monimutkaisia matemaattisia SHA-256-tiivistefunktioita. Kyseisen tiivistefunktion ratkaisua kutsutaan nimellä Proof-of-Work, joka käytännössä todistaa uuden lohkon ratkaisuun käytettyä laskentatehoa. Yksilöllisen tiivisteen ideana on, että sen muodostamiseen vaaditaan paljon laskentatehoa, mutta ratkaiseminen mahdollisimman helppoa. Tiivisteen löydettyä se kuulutetaan verkon muille jäsenille todennettavaksi.

Verkon laskentatehon lisääntyessä tai alentuessa lohkojen vaikeustasoa korjataan 2016 lohkon välein protokollan mukaisesti siten, että tavoitteena on saada lohkojen välille ratkaisuajaksi keskimäärin kymmenen minuuttia. Vaikeustasolla säädetään lohkojen ratkaisemiseen tarvittavien laskutoimitusten määrää. Nykyään louhijoita on paljon, mikä nos-

taa louhinnan vaikeustason korkeaksi. Käytännössä kukaan ei louhi yksin. Louhijat tekevät nykyään yhteistyötä käyttämällä louhinta palvelujen avulla, joita kutsutaan mining pooleiksi. Tarkoituksena on yhdistää useiden satojen tai tuhansien laitteiden laskentateho ja lohkon löytyessä jakaa ansaitut Bitcoinit kaikkien osallistujien kesken.

Aluksi louhintaa tehtiin CPU:n (central processing unit) eli prosessoreiden avulla, mutta GPU (graphics processing unit) -grafiikkasuorittimia hyödyntävät louhintaohjelmistot syrjäyttivät perinteiset prosessorit louhintakäytöstä niiden suuremmilla laskentatehoilla ja energiatehokkuuksilla. Nykyisin Bitcoinien louhinta tapahtuu vielä energiatehokkaammilla ASIC-laitteilla (Application-specific integrated circuit) eli sovelluskohtaisilla piireillä, joiden laskentateho ja energiatehokkuus ovat moninkertaisesti parempia grafiikkapiireihin verrattuna. Kuvassa 7 esitetään Bitcoin-verkon laskentateho kaaviona, joka on kasvanut räjähdysmäisesti. Tällä hetkellä laskentateho on noin 3 800 000 TeraHash sekunnissa, joka vastaa keskimäärin 47 500 000 PetaFlopsia sekunnissa. [17.] Maailman tehokkaimpaan supertietokoneeseen verrattuna Bitcoin-verkko on noin 500 000 kertaa nopeampi, sillä tehokkaimman supertietokoneen laskentateho on lopputyötä kirjoittaessa 93 PetaFLOP/s. [18.]



Kuva 7. Bitcoin-verkon laskentateho 12.4.2017 (blockchain.info).

Bitcoin on teoreettisesti altis 51 % -hyökkäykselle, mutta toistaiseksi tämän uhan kasvaessa on Bitcoin-yhteisö vastannut siihen nopeasti. Teoriassa taho tai hyökkääjät voivat

muokata lohkoketjun historiaa, mikäli hyökkääjällä on hallussa yli 50 % Bitcoin-verkon laskentatehosta.

2.6 Tuplakulutus

Bitcoin-verkko itsestään on hyvin suojattu, mutta riskit tuplakulutukseen ovat aina olemassa. Double Spending eli tuplakulutus tarkoittaa tilannetta, jossa pahantahtoinen käyttäjä pyrkii lähettämään Bitcoin-lompakossaan olevia samoja Bitcoineja kahdelle tai useammalle vastaanottajalle samanaikaisesti. Tämän estämiseksi Bitcoin-verkossa todennetaan jokainen transaktio louhinnalla ja liittämällä transaktiot lohkoihin. Siirtotapahtuma saa ensimmäisen vahvistuksen, kun se ratkaistaan ja lisätään lohkoon. Toisen vahvistuksen sitten kun sitä seuraava lohko ratkaistaan. Bitcoinin alkuperäiseen sovellukseen on määritelty, että siirtotapahtuma merkitään vahvistetuksi vasta 6. lohkon jälkeen, mutta nykyisellä Bitcoin-verkon laskentateholla kolme vahvistusta on riittävästi. [13.] Ilman lohkoketjuteknologiaa digitaalinen valuutta olisi kopioitavissa, kuten muutkin digitaaliset omaisuudet esimerkiksi musiikki, elokuvat ja sähköpostien liitetiedostot. [16.]

2.7 Energiankulutus

Bitcoinin louhintaprosessi vaatii paljon laitteita ja laskentatehoa matemaattisten funktioiden laskemiseen, mikä puolestaan kuluttaa paljon virtaa. Ideana on ylläpitää Bitcoin-verkko mahdollisimman turvallisena sekä varmentaa että tallentaa verkossa tapahtuvat transaktiot lohkoihin ilman keskitettyä tahoa. Bitcoin-verkon laskentateho tätä kirjoittaessa on lähes 3 800 000 TeraHash/s. [17.]

Bitcoin-verkon sähkönkulutusta on haastavaa arvioida, koska verkon laskentateho ja louhintaan käytettävien erilaisten laitteiden energiatehokkuudet vaihtelevat. Marc Bevand arvioi 2017 helmikuun artikkelissaan Bitcoin-verkon virrankulutukseksi 470-540 Megawattia, kun esimerkiksi Suomen olkiluoto-2 ydinvoimalan nettosähköteho on 880 MW. [21; 22.]. Kuvan 8 taulukosta nähdään myös alaraja-arvot, jossa kaikilla olisi käytössä mahdollisimman energiatehokkaat louhintalaitteet ja yläraja-arvot taas niin, että ASIC-laitteita ei ole päivitetty niiden julkaisujen jälkeen. Taulukosta voidaan päätellä, että Bitcoin-verkko voi huonoimmassa tapauksessa kuluttaa jopa yhden ydinvoimalan sähkötuotannon verran. Kuvan 8 taulukossa näkyy alimpana myös prosenttiluku, joka viittaa

IEA:n (International Energy Agency) laatimien raporttien perusteella Bitcoin-verkon sähkönkulutuksen suhteessa koko maapallon energiakulutukseen. [21.]

Lower bound	Best guess	Upper bound
325 MW	470-540 MW	774 MW
2.85 TWh/yr	4.12-4.73 TWh/yr	6.78 TWh/yr
0.100 J/GH	0.145-0.166 J/GH	0.238 J/GH
$142M/yr	$206-237M/yr	$339M/yr
0.00260%	0.00376-0.00432%	0.00619%

Kuva 8. Arviot Bitcoin-verkon sähkön kulutuksesta [21.]

Monesti on argumentoitu, että Bitcoin ei olisi kestävällä pohjalla eikä olisi ekologinen vaihtoehto perinteiselle Fiat-rahajärjestelmälle. Bitcoin-verkon ylläpito kuluttaa valtavan-määrän energiaa. Vasta-argumenttina tälle väitteelle on nykyisen vähimmäisvarantojär-jestelmän (Fractional-reserve banking) energiakulutus, kun mukaan lasketaan keskus-pankkien ylläpito, pankki rakennuksien kuluttama energia, raha-automaatit, seteleiden painaminen. Tämän näkemyksen kannalta Bitcoin-verkon energiatehokkuus ei kuulosta enää kovin huonolta. Bitcoinin louhintaan kehitetään jatkuvasti energiatehokkaampia laitteita. Tavoitteena on hyödyntää keskitetystä louhinnasta syntynyttä hukkalämpöä muun muassa kotien lämmityksen, kuten perinteiset keskitetyt konesalit.

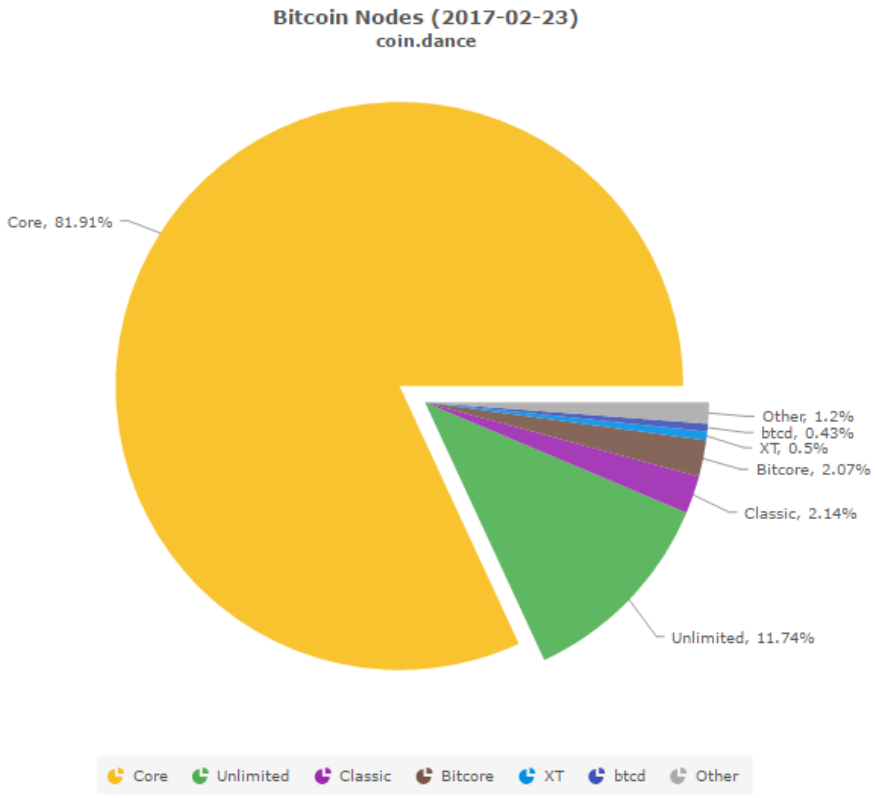
3 Bitcoin-verkko

3.1 Vertaisverkko

Bitcoin-verkko perustuu sen käyttäjien ja tietokoneiden muodostamaan vertaisverkkoon Internetissä. Vertaisverkon (P2P, peer to peer) kaikki jäsenet keskustelevat suoraan tois-tensa kanssa ilman keskitettyä palvelinta. Etuna perinteiseen palvelin-asiakas-malliin verrattuna on resurssien järkevämpi käyttö, jossa asiakkaat eivät jonota pääsyä palveli-melle. Vertaisverkossa jäsenet ovat tasavertaisia ja toimivat muille jäsenille resursseina jakamalla laskentatehoa, kaistanleveyttä ja tallennustilaa yhteiseen käyttöön. [12.]

Bitcoin-verkossa toimivat solmut keskustelevat ja jakavat tietoja keskenään transaktioista, lohkoista, lohkoketjuista ja muiden solmujen IP-osoitteita. Kun verkkoon kuulutetaan esimerkiksi siirtotapahtuma, verkon solmut siirtävät tiedon eteenpäin muille verkon jäsenille, kunnes tieto on saavuttanut verkon kaikki käyttäjät. Vertaisverkot ovat luonteeltaan sinnikkäitä, hajautettuja ja avoimia. Bitcoinin lisäksi vertaisverkko teknologiaa käytetään myös tiedostojen jakamiseen tai VoIP-ratkaisuissa (Voice over Internet Protocol). Näistä tunnetuimmat ovat BitTorrent, Napster, eDonkey, Freenet ja Skype. [15.]

Kaikki viestintä Bitcoin-verkossa tapahtuu TCP-protokollan välityksellä ja tavanomaisesti sovellukset käyttävät 8333 -porttia, mutta Bitcoinia voi tarvittaessa käyttää myös muillakin porteilla -portti parametria käyttämällä. [14.] Bitcoinin vertaisverkkoon on liitettynä noin 7000 – 10000 laitetta, joista suurin osa suorittavat eri versioita Bitcoinin alkuperäistä ohjelmistoa Bitcoin Corea. Samassa vertaisverkossa ajetaan myös muita variaatioita Bitcoin protokollasta kuten BitcoinJ, Libbit, btcd, ja Unlimited. Kuvassa 9 nähdään Bitcoin-verkon sovellusten jakauma. Bitcoin-Corea käyttävät ovat Bitcoin-verkossa niin sanottuja ”full node” eli täysimääräisiä jäseniä, jotka pitävät koko lohkoketjun eli siirtohistorian tallessa. Näiden täysimääräisten jäsen solmujen kautta rakentuu esimerkiksi vaihtopörssit, verkkolompakot ja kauppiasjärjestelmät. [15.]



Kuva 9. Bitcoin vertaisverkon eri sovellusten jakauma (https://coin.dance).

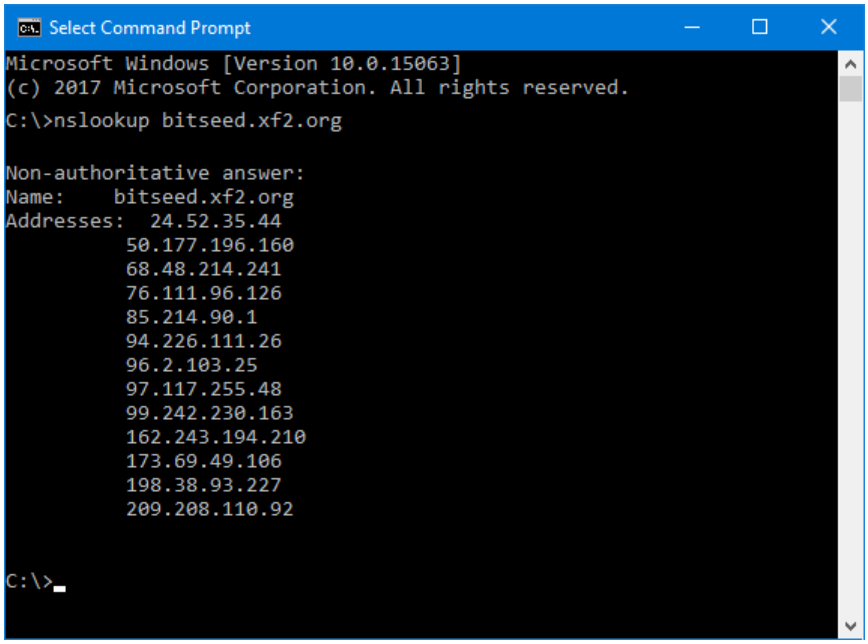
Bitcoin-vertaisverkon lisäksi käytössä on myös muita protokollia, kuten stratum, jota käytetään louhinnassa ja mobiililompakoissa. [15.] Laajennetut verkkoprotokollat toteutetaan yhdyskäytävä palvelimien avulla niin, että palvelimet ovat yhteydessä Bitcoinin varsinaiseen vertaisverkkoon ja tarjoavat laajennettua verkkoa eteenpäin muille käyttäjille eikä näiden käyttäjien tarvitse ladata suurta lohkoketjua tietokoneelleen tai älypuhelimiin. Lohkoketjun koko kasvaa eksponentiaalisesti ja on ohittanut juuri 100 gigatavun tallennustarpeen. Vuonna 2014 aikana lohkoketjun koko kasvoi noin 9 gigatavua ja vastaavasti vuonna 2015 kasvoi 11 gigatavua, kun taas vuoden 2016 aikana lohkoketju kasvoi 25,2 Gt:n vuosivauhtia.

3.2 Yhteyden muodostaminen

Uuden solmun liittyessä Bitcoin-verkkoon sen täytyy ensiksi havaita ja löytää muut solmut. Prosessin käynnistämiseksi sovellus tarvitsee listan IP-osoitteista, joiden avulla sovellus osaa ottaa yhteyden muihin verkon käyttäjiin. Tätä varten alkuperäiseen Bitcoin Core -sovelluksen lähdekoodiin on lisätty joukko DNS-isäntänimiä:

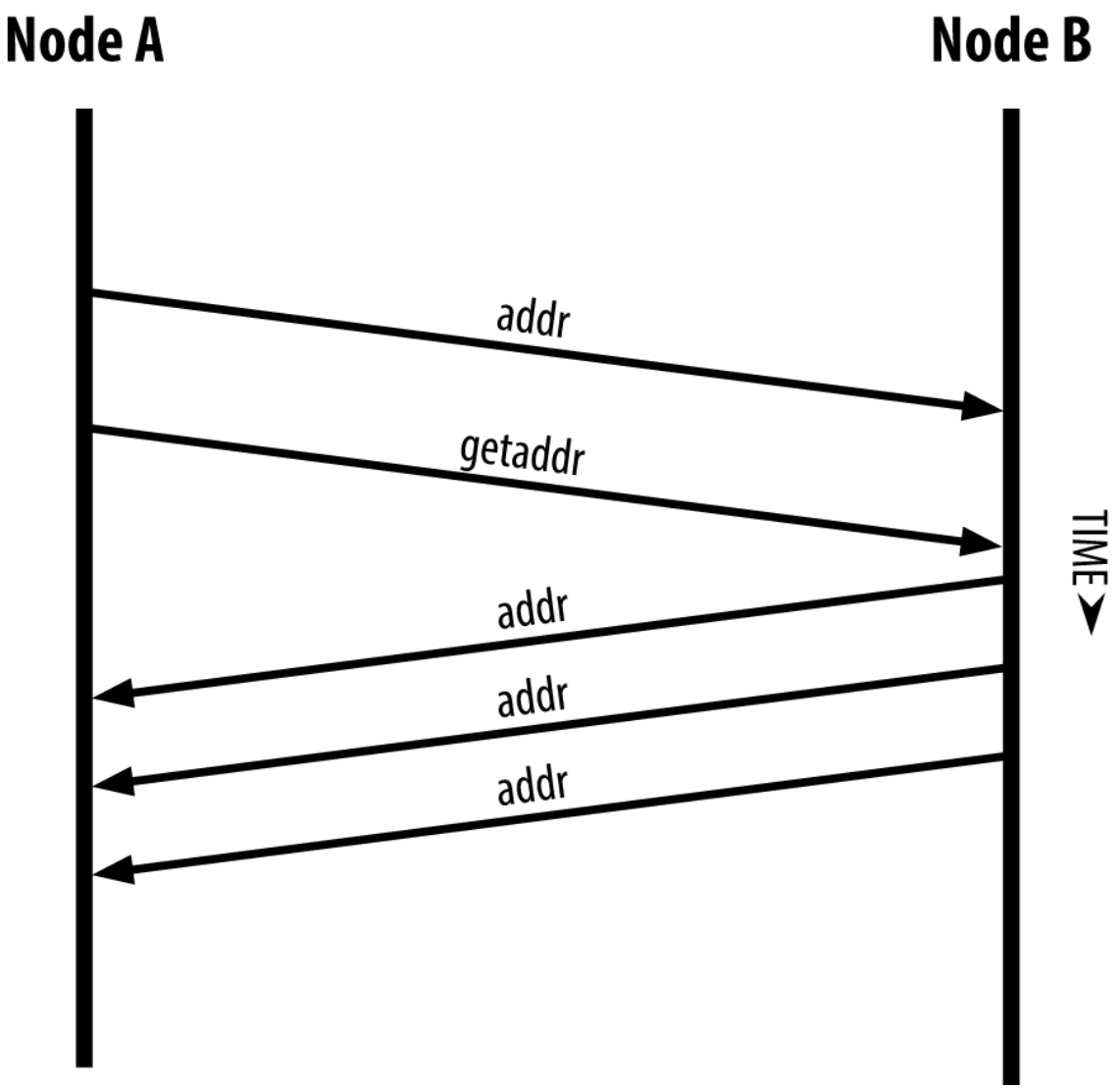
- bitseed.xf2.org
- dnsseed.bluematt.me
- seed.bitcoin.sipa.be
- dnsseed.bitcoin.dashjr.org
- seed.bitcoinstats.com. [7.]

Näiden DNS-isäntänimien takana olevat IP-osoitteet päivittyvät automaattisesti. Suorittamalla nslookup-komennon näille isäntänimille palautuu lista IP-osoitteita verkon käyttäjistä, kuten kuvassa 10 nähdään.



Kuva 10. Windows-komentorivillä suoritettu komento: nslookup bitseed.xf2.org.

Sovellukset löytävät ensimmäisen yhteydenottojen jälkeen muut solmut vaihtamalla käyttäjien tietoja protokollan mukaisilla addr- ja getaddr-viesteillä. Uusi solmu lähettää naapurisolmuilleen addr-viestin sisältäen sen oman IP-osoitteen, jonka jälkeen naapurisolmu lähettää kyseisen IP-osoitteen eteenpäin tämän naapurisolmuille. Vastaavasti uudet verkon käyttäjät voivat lähettää getaddr-viestin naapureilleen ja kysyä heiltä muiden solmujen IP-osoitteista, kuten kuvassa 11 nähdään.



Kuva 11. IP-osoitteiden viestintä kahden solmun välillä. [15.]

Solmut mainostavat myös oman IP-osoitteen muille naapurisolmuille 24 tunnin välein ylläpitääkseen yhteyden muihin solmuihin. [7.] Bitcoinin alkuperäisessä sovelluksessa voi käyttää addnode <ip> -komentoa, jonka avulla sovellukselle syötetään tietty IP-osoite. Sovellus lukee ja kirjoittaa löydettyjen solmujen IP-osoitteet "peers.dat"-nimiseen tiedostoon, joka löytyy Bitcoin-sovelluksen kansiosta.

3.3 Bitcoin-verkon toiminta vaiheittain

Tässä luvussa kootaan yhteen edellä mainitut Bitcoin-verkon vaiheet järjestyksessä, jonka avulla kuvataan solmujen ja käyttäjien muodostama toimiva Bitcoin-verkko.

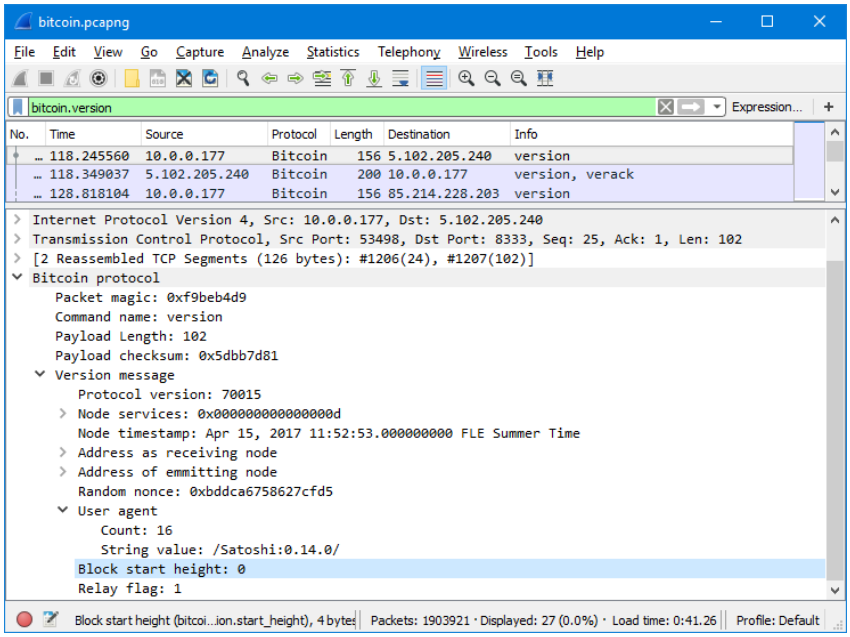
1. Uudet transaktiot kuulutetaan vertaisverkkoon muille solmuille.
2. Jokainen solmu kerää uudet transaktiot omaan lohkoon ja pyrkivät liittämään sen osaksi lohkoketjua.
3. Verkon solmut pyrkivät löytämään oikean tiivistefunktion tälle kyseisellä lohkolle käyttäen massiivista laskentatehoa.
4. Kun jokin solmuista löytää oikeanlaisen tiivistefunktion uudelle lohkolle, se tuodaan julki muille verkon solmuille kuuluttamalla oikea ratkaisu verkon muille käyttäjille.
5. Lohko tiivistefunktio hyväksytään muiden solmujen toimesta, jos lohkoon valitut transaktiot ovat vahvistettuja eikä lohko pidä sisällään jo käytettyjä siirtotapahtumia.
6. Verkon solmut ilmaisevat hyväksynnän liittämällä lohkon osaksi lohkoketjua ja alkavat työstämään seuraavaa lohkoa. [2.]

3.4 Verkkoliikenne

Verkkoliikenne on helposti seurattavissa esimerkiksi ilmaisella avoimen lähdekoodiin perustuvalla Wireshark-pakettianalysaattorilla. Wireshark soveltuu lähes kaikentyyppisen verkkoliikenteen seurantaan ja analysointiin. Verkkopaketit näkyvät välittömästi ja verkkoliikenteen voi tallentaa myöhempää analysointia varten.

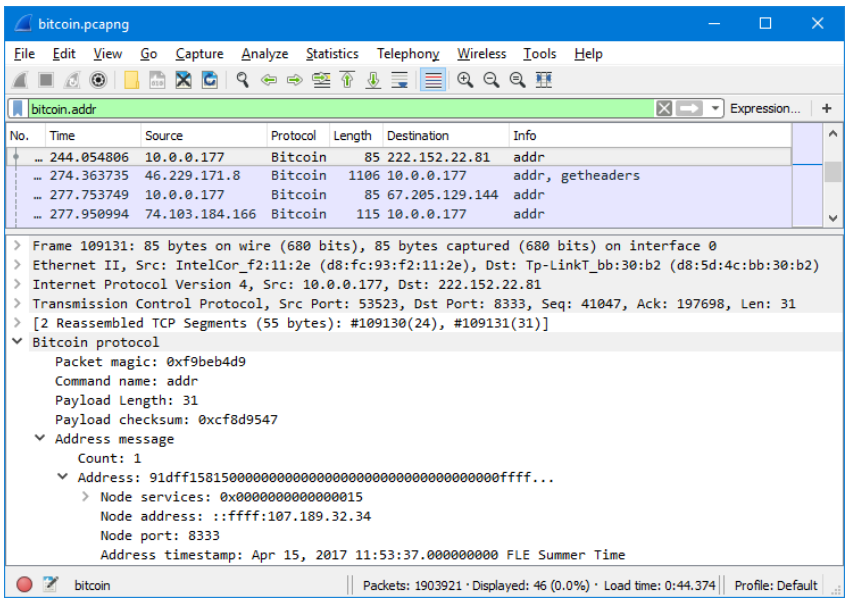
Bitcoin pohjautuu vertaisverkkotekniikkaan ja näin ollen käyttää erittäin paljon verkkoliikennettä perusfunktioiden suorittamiseen. Saatavilla on monenlaisia Bitcoin-sovelluksia, mutta kaikki nämä sovellukset käyttävät samaa protokollaa.

Bitcoin-sovellukset lähettävät aina uusille solmuille versio viestin. Ilman versioviestin kättelyä kaksi solmua eivät pysty keskustelemaan. Kuvassa 12. nähdään esimerkiksi sisäverkon IP-osoitteen 10.0.0.177 ja ulkoisen IP-osoitteen 5.102.205.240 välinen kättelyviestintä. Versioviestin avulla jokainen solmu mainostaa verkkoon olemassaolostaan.



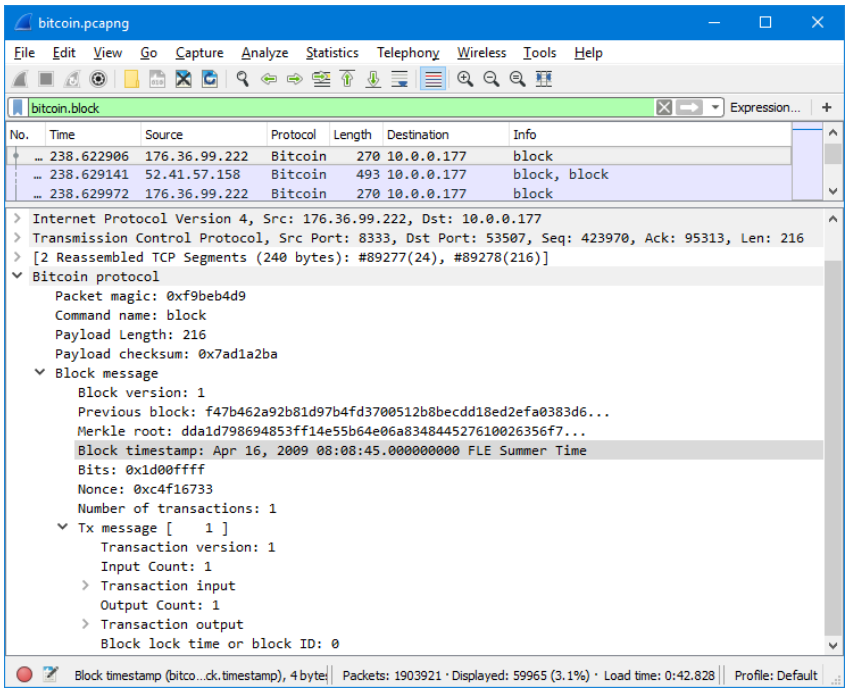
Kuva 12. Versioviestit voidaan tarkastella Wiresharkilla käyttämällä bitcoin.version-suodatinta.

Kuvassa 13 nähdään bitcoin.addr-viesti, joiden avulla Bitcoin-solmut vaihtavat IP-osoitetietoja muiden solmujen kanssa. Tämä on olennainen osa Bitcoin-protokollaa, jonka avulla sovellukset löytävät muut solmut ja näin viestittämään viimeisimmät tiedot muiden käyttäjien kanssa.



Kuva 13. bitcoin.addr-viestien avulla Bitcoin-sovellukset jakavat IP-osoitteet toisille solmuille.

Täysin synkronoidut solmut eivät aiheuta suurta määrää verkkoliikennettä, mutta solmut, joilla ei ole koko lohkoketjua ladattuna, muodostavat huomattavan määrän verkkoliikennettä. Uuden Bitcoin Core-sovelluksen asennuksessa ja koko lohkoketjun lataamisessa voi kestää pitkään, sillä lohkoketjun vie tilaa noin 100 gigatavua. Vaihtoehtoisesti on mahdollista käyttää myös muita Bitcoin-sovelluksia, jotka eivät tarvitse toimiakseen koko lohkoketjun latausta. Näitä kutsutaan kevytlompakoiksi (lightweight wallet) ja näistä suosituimmat ovat esimerkiksi MultiBit-, Coinbase- ja Exodus- Bitcoin-sovellukset. Kevytlompakot käyttävät SPV (Simple Payment Verification) -tekniikkaa, jotka lataavat ainoastaan lohkojen otsikkotiedot ja varmentavat siirtotapahtumat täysimääräisten solmujen kautta kysyen ainoastaan tiettyjen lohkojen tietoja. Kuvassa 14 nähdään lohkojen viestintä sisältöineen Wiresharkissa.



Kuva 14. Lohkojen lähetykset näkyvät bitcoin.block-suodattimella.

Halutun verkkoliikenteen löytämiseksi voi käyttää lukuisia erilaisia suodattimia, joilla saadaan tietty liikenne näkyviin protokollan, portin, IP-osoitteen tai minkä tahansa muun mahdollisen kriteerin perusteella. Wiresharkin kotisivuilta löytyy kattavat ohjeistukset ja oppaat. Esimerkiksi lista Bitcoin-protokollan suodattimista löytyy osoitteesta ”https://www.wireshark.org/docs/dfref/b/bitcoin.html”.

4 Tietoturva

4.1 SHA-256

SHA eli Secure Hash Algorithm on yleisesti käytetty kryptografinen tiivistefunktio, jonka on suunnitellut yhdysvaltalainen NSA-virasto (National Security Agency). Kyseisiä tiivistefunktioita käytetään muun muassa useissa eri ohjelmistoissa kuten TLS:ssä, SSL:ssä, PGP:ssä, SSH:ssä, S/MIME:ssä ja IPSec:ssä. [23.] SHA-256 kuuluu SHA-2-versioon, joka on julkaistu vuonna 2001 ja numero 256 lyhenteen perässä tarkoittaa hajautusarvon eli tiivisteen pituutta. SHA-variantteja on olemassa neljä eri päätyyppiä, joista käytössä ovat SHA-1, SHA-2 ja SHA-3 sekä käytöstä poistettu SHA-0.

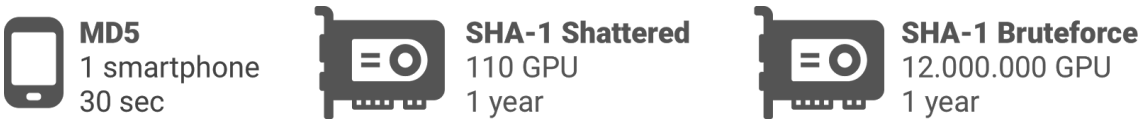
Tiivistefunktiosta käytetään myös muita nimityksiä, kuten sekoite, hajautus- ja hash-funktio. Kryptografinen tiivistefunktio on matemaattinen funktio, joka ottaa syötteeksi pituudeltaan mielivaltaisen merkkijonon ja tuottaa kiinteämittaisen tulosteen. [24.] Nämä tiivistefunktiot ovat yksisuuntaisia, mikä tarkoittaa sitä, että alkuperäisestä syötteestä on helppo laskea tiiviste, jonka muuntaminen takaisin alkuperäiseksi syötteeksi on erittäin hankalaa tai jopa mahdotonta. Alkuperäisen syötteen yhden merkin vaihtuminen muuttaa tiivisteen täysin, kuten kuvasta 15 nähdään.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Kuva 15. Erilaisia syötteitä ja niistä laskettuja SHA-256-tiivisteitä [25.]

Bitcoinissa SHA-256-tiivistefunktioita käytetään lohkojen laskentatyön todistamisessa (Proof-of-work) laskemalla lohkoille sellainen tiiviste, jossa on tietty määrä nollia alussa. Lopputyötä kirjoittaessa lohkojen tiivisteet alkoivat 18 kappaleen nollilla esim. ”000000000000000000001108b99cee1738c0c2b05871d6b4a5d24da64987b4f26f”. Tällaisen lohko tiivisteen laskemiseen kuluu nykyisellä verkon laskentateholla (3 800 000 TeraHash/s) noin kymmenen minuuttia. Nykyiset tietokoneiden grafiikkapiirit kykenevät suorittamaan ~800 MegaHash laskutoimitusta sekunnissa ja uusimmat ASIC-laiteet kykenevät 13,5 TeraHash/s-laskentatehoon.

SHA-1-version tiivistefunktiosta on löydetty uusia heikkouksia vuonna 2015, mitkä helpottivat tiivistefunktioiden törmäyksen laskemisen. [26.] Kaksi vuotta myöhemmin 2017 helmikuussa Marc Stevens ilmoitti löytäneen ensimmäisen SHA-1-tiivistefunktioiden törmäyksen Shattered-hyökkäyksellä, jonka myötä on kehotettu siirtymään uudempaan varianttiin SHA-256:een. Shattered-hyökkäyksellä onnistuttiin löytämään sama tiivistearvo suorittamalla 2^{63} SHA-1 laskutoimituksia, joka on paljon vähemmän kuin brute-forceen tarvittava laskentamäärä. Kuvassa 16 nähdään esimerkki SHA-1-tiivistefunktioiden laskemiseen kulutettu aika ja tarvittavien grafiikkapiirien määrä. [27.]



Kuva 16. Shattered-hyökkäys on 100 000 kertaa nopeampi kuin brute-force-hyökkäys. [27.]

Uudemmasta SHA-2-version SHA-256-tiivistefunktiosta ei ole löytynyt heikkouksia ja SHA-1-varianttiin verrattuna SHA-256-tiivistefunktiossa käytetään 256 bitin kokoisia tiivisteitä, kun SHA-1-versiossa on pienemmät 160-bittiset tiivisteet. Mikäli SHA-256-version tiivistefunktioon löydetään jonain päivänä heikkouksia. Tämä tarkoittaisi samalla, että Bitcoinin lohkojen tiiviste arvoja voitaisiin manipuloida ja haavoittuvuuden avulla pystytään louhimaan lohkoja muita nopeammin tai vastaavasti syöttämään Bitcoin-verkkoon vääränlaisia transaktioita. Bitcoin-protokollaan pitäisi tällaisessa kuvitteellisessa tapauksessa toteuttaa ja siirtyä käyttämään turvallisempaa, kuten SHA-384-algoritmia.

4.2 ECDSA

ECDSA eli Elliptic Curve Digital Signature Algorithm on variantti DSA (Digital Signature Algorithm) kryptografisesta algoritmista, joka käyttää elliptisen käyrän kryptografiaa (Elliptic Curve Cryptography). Bitcoinissa käytetään tarkemmin ottaen ECDSA secp256k1 -variaation parametreja, jotka ovat 30 % nopeampia kuin muut elliptiset käyrät. [29.] Turvallisuus perustuu yksisuuntaisen laskutoimituksen käänteisoperaatioon, tässä tapauksessa diskreetin logaritmin vaikeuteen. [28.] Bitcoinissa tätä kyseistä algoritmia käytetään julkisen avaimen muodostamiseen ja näin ollen myös digitaaliseen allekirjoitukseen. Julkisen avaimen kryptografiassa syöte voidaan allekirjoittaa yksityisellä avaimella, ja tämän jälkeen muut tahot voivat vahvistaa allekirjoituksen oikeudellisuuden julkisella avainparilla.

ECDSA-algoritmissa ei ole havaittu haavoittuvuuksia, mutta muutamia tietoturvaloukkauksia on havaittu, jotka liittyivät algoritmin huonoon toteutukseen tai ohjelmointivirheeseen. Esimerkiksi vuonna 2010 Sonyn Playstation 3 käyttämästä ECDSA-toteutuksesta löytyi ohjelmointivirhe, joka liittyi satunnaisten numeroiden luomiseen. Toinen hyvin samantyyppinen haavoittuvuus löytyi vuonna 2013, joka liittyi vakavaan Java SecureRandom -kirjaston ohjelmointivirheeseen. Android-sovelluksilla luodut Bitcoin-lompakot käyttivät ohjelmointivirheen vuoksi samoja yksityisiä avaimia, minkä vuoksi näiden Bitcoin-lompakkojen käyttäjät menettivät Bitcoin-osoitteissa olevat virtuaalivaluutat vuonna 2013 [28.]

Kaikki yleisesti käytössä olevat julkisen avaimen kryptografiaan perustuvat algoritmit ovat murrettavissa tulevaisuuden kvanttitietokoneilla. Bitcoinin käyttämä Elliptic Curve Digital Signature Algorithm salaus ei ole turvassa kvanttitietokoneilta, ja sama uhka koskee myös muita algoritmeja, kuten RSA ja DSA sekä muita elliptisiä käyriä. [32.] Kvanttitietokoneet kykenevät suorittamaan ja ratkaisemaan monimutkaisia matemaattisia laskutoimituksia paljon nopeammin kuin perinteiset tietokoneet. Tulevaisuuden kvanttitietokoneet mahdollistavat Bitcoinin yksityisen salausavaimen murtamisen esimerkiksi Bitcoinin yksityisen salausavaimen murtamisen, kun julkinen avain on tiedossa. Bitcoinissa kyseinen julkinen avain kuulutetaan aina verkkoon siirtotapahtumien yhteydessä protokollan mukaisesti. Esimerkiksi perinteisiltä tietokoneilta vaaditaan keskimäärin 2^{128} bittioperaatiota yksityisen avaimen murtamiseen, kun kvanttitietokoneilla murtamiseen tarvitaan vain 128^3 kvanttioperaatiota käyttäen matemaatikon Peter Shorin suunnittelemaa kvanttialgoritmia. [31; 33.]

- 2^{128} = 340 282 366 920 938 463 463 374 607 431 768 211 456
- 128^3 = 2 097 152

Laskuoperaatio lukujen auki laskemisen myötä huomataan, että 2^{128} on erittäin iso luku ja olisi erittäin epäkäytännöllistä lähteä näin suurta määrää laskutoimituksia perinteisillä tietokoneilla. Kvanttioperaatioita tarvittaisiin ainoastaan vähän yli 2 miljoonaa, mutta toisaalta uudet kvanttitietokoneet tulevat olemaan hitaita laitteita, sillä uuden teknologian kehittäminen on aina hidasta ja hyvin kallista. Vuonna 2016 kvanttitietokoneiden nopeus oli alle 10 kubittia (qubits), kun Bitcoin yksityisen avaimen murtamiseen tarvittaisiin suurin piirtein 1500 kubitin nopeudella toimiva laite. Kryptografia organisaation ECRYPT II (European Network of Excellence in Cryptology II) mukaan Bitcoinissa käytetty 256-bittiset ECDSA avaimet ovat turvassa arviolta 2031 – 2040 vuoteen asti, kuten kuvan 17

taulukossa nähdään. [31; 34.] Taulukosta nähdään myös muiden organisaatioiden arvioita ja suosituksia ECDSA-256-bittisen salauksen suhteen.

Method	Date	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
[1] Lenstra / Verheul	2084	135	7813 6816	241	7813	257	269
[2] Lenstra Updated	2090	128	4440 6974	256	4440	256	256
[3] ECRYPT II	2031 - 2040	128	3248	256	3248	256	256
[4] NIST	2016 - 2030 & beyond	128	3072	256	3072	256	256
[5] ANSSI	2021 - 2030	128	2048	200	2048	256	256
[6] IAD-NSA	-	256	3072	-	-	384	384
[7] RFC3766	-	136	3707	272	3707	257	-
[8] BSI	> 2022	128	3000	250	3000	250	256

Kuva 17. 256-bittisen ECDSA-algoritmin arvioitu elinkaari. [34.]

Bitcoinissa on omalla tavallaan sisäänrakennettu kvanttitietokoneiden vastustuskyky, kun Bitcoin-osoitteita käytetään ainoastaan yhden kerran. ECDSA-salauksen julkinen avain kuulutetaan ja paljastetaan Bitcoin-verkkoon vasta siirtotapahtumien yhteydessä. Nopeillakin kvanttitietokoneilla olisi hyvin lyhyt aikaväli Bitcoinin yksityisen salausavaimien murtamiseen. Tällä kyseisellä aikavälillä tarkoitetaan aikaa, joka alkaa siirtotapahtuman kuuluttamisesta siihen asti, kunnes siirtotapahtuma louhitaan lohkoon. [31.] Tässä vaiheessa voidaan todeta, että Bitcoinin käyttämä ECDSA-salausalgoritmi on hyvin vahva, eikä se ole murrettavissa nykyisillä tietokoneilla. Tulevaisuudessa teknologian kehittyessä Bitcoinin-protokollaan voidaan myös implementoida uusia vahvempia julkisen salauksen algoritmeja, kuten ajamalla verkkoon ”soft fork” -tyylisen muutoksen. Soft fork vaatii 70 prosenttisen äänestyksen Bitcoin-verkon louhijoilta ja yhteensopiva alkuperäisen lohkoketjun sekä osoitteiden kanssa. [31.]

4.3 Anonymiteetti

Bitcoinia on usein kuvailtu anonyymiseksi valuutaksi, koska sen avulla on mahdollista lähettää ja vastaanottaa Bitcoineja ilman, että henkilöllisyys välttämättä paljastuisi. Bitcoinissa valuutta kulkeutuu suoraan käyttäjän virtuaalisesta lompakosta toiseen riippumatta pankkien aukioloista tai muista rajoituksista, joita liittyy perinteisten pankkien

välisiin rahansiirtoihin. Perinteisen FIAT-valuutan käyttämisen yhteydessä maksajan nimi ja tilinumero voidaan käytännössä aina jäljittää pankkien avulla. [35.]

Täydellistä anonymiteettiä on hankalaa, ellei mahdotonta saavuttaa Bitcoineja käyttämällä. Valuutan lähettämistä ja vastanottamista voidaan verrata pseudonyymi eli salanimen taakse piiloutumiseen. Jos Bitcoin-osoite pystytään liittämään tiettyyn henkilöllisyyteen, Bitcoin-osoitteen kaikki aikaisemmat ja tulevat siirtotapahtumat voidaan yhdistää tähän samaan henkilöön. Satoshi Nakamoton alkuperäisessä ”whitepaper” -kuvauksessa suositellaan käyttäjiä käyttämään täysin uusia Bitcoin-osoitetta jokaiselle transaktiolle. [2.] Näin Bitcoin-osoitteista lähetetyt Bitcoinit eivät ole helposti yhdistettävissä tiettyyn pseudonyymiin. Julkisen lohkoketju teknologian vuoksi jokainen voi halutessaan tarkastella tiedossa olevaa Bitcoin-osoitetta ja transaktioiden tietoja. Jokaiseen transaktioon jää myös merkintä IP-osoitteesta, josta kyseinen transaktio on alun perin kuulutettu Bitcoin-verkkoon. Bitcoin virtuaalivaluuttaa käytettäessä anonymiteetti on täysin käyttäjän vastuulla, joka vaatii erityistä tarkkuutta ja osaamista.

Käyttäjä voi piilottaa käyttämänsä IP-osoitteen käyttäen VPN-yhteyttä (Virtual private network) tai TOR (The Onion Router) palveluita. Näiden kahden palveluiden avulla käyttäjä muodostaa ensiksi salatun yhteyden turvallisen tunneloinnin läpi ja näin käyttäjää identifioiva IP-osoite ei näkyisi Bitcoin-siirtotapahtumissa. VPN-yhteydet ovat käytetyimpiä suojaustekniikoita, jotka mahdollistavat turvallisen pääsyn organisaation lähiverkkoon tai yhdistävät yritysten verkot toisiinsa. VPN-yhteyksiä hyödynnetään nykyisin myös yksityiskäyttäjien verkkoviestinnän suojaamiseen ja anonymiteetin saavuttamiseen. [36.]

TOR-verkko on suunniteltu mahdollistamaan anonyymi liikennöinti liikenteen sisältö salaamalla ja reitittämällä liikenne tuhansien eri solmujen kautta. TOR-verkon kenelle tahansa tarjoama anonyymi on huomattu myös verkkorikollisten parissa. TOR-verkko salaa alkuperäisen datan ja IP-osoitteen useita kertoja lähettäen verkkopaketit sattumanvaraisesti valittujen TOR-solmujen läpi. [37.]

Bitcoinin anonymiteetin edistämiseksi on luotu myös jaettuja osoitteita ja web-pohjaisia lompakoita, joiden kautta Bitcoineja voidaan kierrättää ja ns. sekoittaa Bitcoinit muiden käyttäjien Bitcoinien kanssa. Tällaisen palvelun avulla Bitcoineja voidaan lähettää jaet-

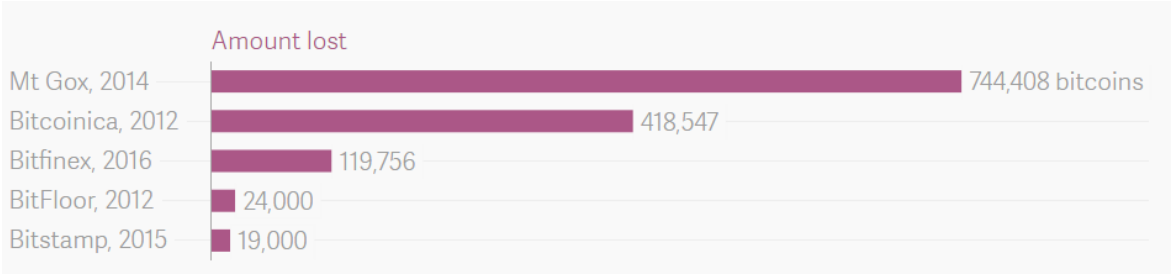
tuun Bitcoin-osoitteeseen ja mutkien kautta eteenpäin toiseen Bitcoin-osoitteeseen. Tarkoituksena on vaikeuttaa Bitcoinien seurantaa ja varjella Bitcoin-osoitteiden omistajatietoja [35.]

Bitcoin-valuutan anonymiteetissä on toisaalta myös haittapuolensa, sillä sen myötä rikollisten on helpompi käyttää Bitcoineja tarkoituksiinsa. Bitcoinin vuosien olemassaolon aikana raportoitu useita eri tapauksia, joissa Bitcoineja on käytetty huume- ja asekaupoissa sekä kiristyksissä, kuten tietokoneille asentuvissa haittaohjelmissa. Nimettömään Bitcoin-lompakkoon siirretyt lunnaat ovat vaikeasti jäljitettävissä, eikä Bitcoin-järjestelmässä ole mahdollisuutta jäähdyttää tiettyjen Bitcoin-osoitteiden käyttöä kuten perinteisiä pankkitilejä.

4.4 Tietomurrot

Digitaalinen vallankumous on mahdollistanut tehokkaiden tietoverkkojen rakentamisen ja tietokoneiden välisen tiedonvälityksen. Teknologian ja sähköisten palveluiden räjähdysmäisen kehityksen kannalta on tärkeää, että uudet palvelut, tietoverkot ja järjestelmät ovat luotettavia, turvallisia sekä suojattuja. Verkkopalveluiden yleistyessä on uutisoitu paljon kybertuvallisuudesta ja verkossa tapahtuvista palvelunestohyökkäyksistä, vakoiluista sekä identiteettivarkauksista. Verkkorikollisille ja muille netin väärinkäyttäjille kaikella tiedolla on arvoa, joita he voivat käyttää rahan ansaitsemiseen. Uhreiksi joutuvat niin suuryritykset kuin yksityiset käyttäjät. Lisääntyvä verkkorikollisuus jatkaa kasvuaan digitalisten palveluiden yleistymisen myötä. [38.]

Verkkopankkeihin tai SWIFT-rahansiirtojärjestelmiin kohdistuva verkkorikollisuus ja tietomurrot ovat lisääntyneet merkittävästi. Esimerkiksi vuonna 2016 helmikuussa Bangladeshissa keskuspankilta vietiin noin 81 miljoonaa dollaria. [38.] Bitcoin on myös herättänyt verkkorikollisten kiinnostuksen. Bitcoin vaihdantapalveluissa, rahaa liikkuu päivittäin kymmenien miljoonien dollareiden edestä. Bitcoinin olemassaolon aikana on moneen otteeseen uutisoitu varkauksista ja vaihdantapalveluiden tietoturvaloukkauksista. Näistä suurimmat ja viimeisimmät tapaukset näkyvät kuvan 18 kaaviossa.



Kuva 18. Bitcoin-vaihdantapalveluiden menetykset. (https://www.theatlas.com/charts/Bk1RzceF)

Bitcoin-vaihdantapalvelu Bitfinex kertoi 2016 elokuussa joutuneensa tietomurron ja massiivisen varkauden kohteeksi, minkä myötä kaupankäynti kyseisessä pörssissä keskeytettiin. Verkkorikollisten matkaan lähti 119 756 Bitcoinia eli sen aikaisella vaihtokurssilla noin 71 miljoonan dollarin edestä varoja. Vaihdantapalvelun kärsimät tappiot jaettiin kaikkien palvelun käyttäjien kesken niin, että käyttäjille annettiin tietty määrä Bitfinexin poletteja. [39.] Bitfinex-pörssi lunasti viimeisetkin jakamansa poletit käyttäjiltään 2017 huhtikuussa. Näin hyvin ei suinkaan ole aina käynyt kaikkien Bitcoin-vaihdantapalvelu varkauksien kohdalla. Vuoden 2014 suurin Bitcoin-vaihdantapalvelu nimeltä Mt. Gox ajautui konkurssiin menetettyään 744 408 Bitcoinia varkaille, joka vastasi siihen aikaan 460 miljoonaa dollaria. Myöhemmin palvelu suljettiin, ja käyttäjät jäivät ilman rahoja. [40.]

Bitcoin-protokollassa ei ole mahdollista estää varastettujen Bitcoinien siirtoa tai palauttaa varastettuja kolikoita takaisin alkuperäiselle omistajalle. Keskusviranomaisten tai kolmannen osapuolen puuttuminen voidaan nähdä niin vahvana kuin heikkona puolena. Perinteisen valuutan käytössä väärään tilinumeroon lähetetyt varat voidaan jäljittää ja mahdollisesti palauttaa takaisin alkuperäiselle omistajalle. Vaihdantapörssien varkaustapauksissa on vaikeampaa pitää Bitcoin-pörssejä vastuussa, sillä Bitcoinia ja sen vaihdantapörssejä ei ohjaa eikä valvo viranomainen. Vaihdantapalveluissa ei myöskään ole talletussuojaa, kun taas perinteisessä pankki toiminnassa talletuksille on asetettu pankkitalletusten suoja, joka on EU-maissa 100 000 euroa. [41.]

5 Pohdinta

Bitcoin opinnäytetyön kohteena oli hyvin mielenkiintoinen. Se sisälsi monelta tapaa paljon teknisiä käsitteitä ja käytännöllistä tietoa niin kryptografiasta kuin vertaisverkossa tapahtuvasta liikenteestä. Lopputyötä kirjoittaessa Internetistä löytyi valtavasti tietoa Bitcoin-protokollasta ja sen eri komponenteista, mutta niiden omaksuminen oli osittain haastavaa. Bitcoinin tekninen tuntemus oli itselle varsin uutta, sillä digitaalisen valuutan käyttäminen ei ole edellyttänyt teknistä tuntemusta kryptografiasta tai salausalgoritmeista.

Omien käyttökokemuksien perusteella voin todeta, että digitaalisten valuuttojen käyttö on tehty suhteellisen helpoksi asiakasohjelmilla, vaihdantapalveluilla ja bitcoin-automaateilla ilman, että käyttäjiltä vaadittaisiin asiantuntevaa teknistä osaamista. Tulevaisuudessa digitaaliset valuutat tulevat keräämään varmasti entistä isompaa suosiota, kun digitaaliset valuutat tulevat tutummaksi suuremmalle yleisölle. Bitcoinin ekologisuutta tarkastellessa huomattiin, että Bitcoin-verkon ylläpitoon kulutettu energia määrä on varsin suuri, mutta ei kuitenkaan sietämätön kuten on uutisoitu. Energiatehokkuus paranee varmasti tulevaisuudessa louhinta laitteiden ja ASIC-laitepiirien kehittyessä.

Digitaalinen valuutta Bitcoin on erittäin volatiili ja vuosien olemassaolonsa aikana kokenut useita arvon romahduksia. Bitcoinien arvo määräytyy täysin kysynnän ja tarjonnan mukaan. Epävarmuus on kasvanut entisestään, kun Bitcoinin suurimpiin vaihdantapalveluihin on tehty tietomurtoja ja anastettu käyttäjien varallisuutta. Tietomurtojen seurauksena vaihdantapalvelut ovat joutuneet sulkemaan palvelunsa väliaikaisesti tai jopa kokonaan menettäen asiakkaidensa Bitcoin-varat.

Turvallisuusnäkökulmasta katsottuna Bitcoin-protokolla on itsestään erittäin turvallinen sen käyttämien vahvojen salausalgoritmien ansiosta. Tietomurrot ja varkaudet eivät ole liittyneet Bitcoinissa käytettyihin salausalgoritmeihin vaan ainoastaan web-palveluiden ylläpitoon liittyvään tietoturvaan. Bitcoinissa on erittäin tärkeätä pitää salausavaimet suojattuina, koska yksityisavaimen avulla voidaan käyttää Bitcoin-osoitteessa olevat varat ja vastaavasti yksityisavaimen kadotessa menetetään Bitcoin-osoitteen käyttöoikeus. Kadotettuja yksityisavaimia ei myöskään ole mahdollista palauttaa, sillä yksityisten avaimien kokonaismäärä on erittäin suuri ja saman yksityisen avaimen luominen on lähestulkoon mahdotonta.

Julkisen avaimen salausmenetelmiä tutkimalla selvisi, että Bitcoinissa käytetty ECDSA-salausalgoritmi on haavoittuvainen teknologian ja varsinkin kvanttitietokoneiden kehittyessä. Tulevaisuudessa on mahdollista ja todennäköistä, että tehokkaiden kvanttitietokoneiden avulla voidaan murtaa matemaattiseen perustuvat salausalgoritmit ja näin ollen laskea Bitcoinin yksityisen salausavaimet käyttäen julkisia avaimia. Tämänhetkisen tietojen perusteella voidaan todeta, että ECDSA-salausalgoritmi on erittäin turvallinen ja tarvittaessa Bitcoiniin voidaan tulevaisuudessa toteuttaa vahvempia salausalgoritmeja.

Digitaalisen valuutan anonymiteettiä tarkastelemalla selvisi, että Bitcoin ei ole täysin anonyymi vaan enemmänkin pseudonyymi. Bitcoin-osoitetta ja siirtotapahtumia tarkastelemalla voidaan tietyissä tilanteissa yhdistää henkilöllisyyteen tai käyttäjään. Bitcoin-osoitteella voidaan yhdistää identiteettiin, mikäli kyseinen Bitcoin-osoite on mainittu keskustelupalstoilla tai allekirjoituksissa maksujen sekä lahjoituksien vastaanottoon. Siirtotapahtumiin kirjautuu IP-osoite, josta tapahtuma on kuulutettu verkkoon, joskin oman IP-osoitteen voi piilottaa helposti esimerkiksi VPN-yhteyttä käyttämällä. Tavallinen kuluttaja voi suhtautua epäilevästi Bitcoiniin anonymiteetin vuoksi, sillä anonyymi digitaalisia valuuttoja on uutisoitu kytköksistä rikolliseen toimintaan, kuten rahanpesuun, huume- ja asekauppaan.

Lähteet

1 Satoshi Nakamoto. 2008. Bitcoin P2P e-cash paper. <http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html> 31.10.2008. Luettu 5.1.2017.

2 Satoshi Nakamoto. 2008. Bitcoin White Paper. <https://bitcoin.org/bitcoin.pdf>. 31.10.2008. Luettu 5.1.2017.

3 Satoshi Nakamoto. 2009. Bitcoin v0.1 released. <http://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html>. 8.1.2009. Luettu 5.1.2017.

4 Bitcoin. 2017. Wikipedia. <https://en.wikipedia.org/wiki/Bitcoin>. Luettu 5.1.2017.

5 Henry Brade. 2013. Europe's First Bitcoin ATM is here. <https://bittiraha.fi/content/europes-first-bitcoin-atm-here-0>. Luettu 5.1.2017.

6 Bitcoin wiki. 2016. Controlled supply, Projected Bitcoins Long Term. <https://en.bitcoin.it/wiki/Controlled_supply>. Luettu 12.1.2017.

7 Bitcoin wiki. 2015. Satoshi Client Node Discovery. <https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery>. Luettu 15.1.2017

8 Bitcoin wiki. 2015. Private key. <https://en.bitcoin.it/wiki/Private_key>. Luettu 17.1.2017.

9 Bitcoin wiki. 2016. Block. <https://en.bitcoin.it/wiki/Block>. Luettu 23.1.2017.

10 Bitcoin wiki. 2015. Blockchain. <https://en.bitcoin.it/wiki/Block_chain>. Luettu 23.1.2017.

11 Bitcoin wiki. 2016. Transaction. <https://en.bitcoin.it/wiki/Transaction>. Luettu 4.2.2017.

12 Wikipedia. 2017. Peer-to-peer. <https://en.wikipedia.org/wiki/Peer-to-peer>. Luettu 12.1.2017.

13 Bitcoin wiki. 2016. Confirmation. <https://en.bitcoin.it/wiki/Confirmation>. Luettu 25.1.2017

14 Bitcoin wiki. 2016. Network. <https://en.bitcoin.it/wiki/Network>. Luettu 15.2.2017.

15 Andreas M. Antonopoulos. 2014. Mastering Bitcoin, 1st Edition.

16 Melanie Swan. 2015. Blockchain - Blueprint for a New Economy - 1st Edition.

17 Bitcoincharts. 2017. <http://bitcoincharts.com/bitcoin>. Luettu 20.3.2017

18 Top500. 2016. Supercomputer site. <https://www.top500.org/lists/2016/11/>. Luettu. 12.4.2017.

19 Drew Weisenberger, Jefferson Lab. <http://education.jlab.org/qa/mathatom_05.html>. Luettu 17.1.2017.

20 Wikipedia. 2017. <https://en.wikipedia.org/wiki/Public-key_cryptography>. Luettu 11.3.2017.

21 Marc Bevand. 2017. Electricity consumption of Bitcoin: a market-based and technical analysis. <http://blog.zorinaq.com/bitcoin-electricity-consumption>. Luettu 12.3.2017.

22 Wikipedia. 2017. Ydinvoima Suomessa. <https://fi.wikipedia.org/wiki/Ydinvoima_Suomessa>. Luettu 12.3.2017.

23 Wikipedia. 2017. SHA-2. <https://en.wikipedia.org/wiki/SHA-2>. Luettu 13.4.2017.

24 Wikipedia. 2017. Hash function. <https://en.wikipedia.org/wiki/Hash_function>. Luettu 13.4.2017.

25 Bitcoin wiki. 2016. Proof-of-work. <https://en.bitcoin.it/wiki/Proof_of_work>. Luettu 13.4.2017.

26 Viestintävirasto. 2015. SHA-1-tiivisteiden kelpoisuus on päättymässä. <https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/10/ttn2015102 71004.html>. Luettu 13.4.2017.

27 Google Security blog. 2017. Announcing the first SHA1 collision. <https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>. Luettu 13.4.2017.

28 Wikipedia. 2017. Elliptic Curve Digital Signature Algorithm. <https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm>. Luettu 14.4.2017.

29 Bitcoin wiki. 2016. Secp256k1 <https://en.bitcoin.it/wiki/Secp256k1>. Luettu 14.4.2017.

30 Bitcoin. 2013. Android Security Vulnerability. <https://bitcoin.org/en/alert/2013-08-11-android>. Luettu 14.4.2017.

31 Bitcoin wiki. 2016. Quantum computing and Bitcoin. <https://en.bitcoin.it/wiki/Quantum_computing_and_Bitcoin>. Luettu 14.4.2017.

32 Wikipedia. 2017. Post-quantum cryptography. <https://en.wikipedia.org/wiki/Post-quantum_cryptography>. Luettu 14.4.2017.

33 Wikipedia. 2017. Shor's algorithm. https://en.wikipedia.org/wiki/Shor%27s_algorithm>. Luettu 14.4.2017.

34 Damien Giry. 2017. Cryptographic Key Length Recommedation. <https://www.keylength.com/en/compare>. Luettu 14.4.2017.

35 Bitcoin wiki. 2017. Anonymity. <https://en.bitcoin.it/wiki/Anonymity>. Luettu 15.4.2017.

36 Wikipedia. 2017. Virtual Private Network. <https://en.wikipedia.org/wiki/Virtual_private_network>. Luettu 15.4.2017.

37 Wikipedia. 2017. Tor (anonymity network). <https://en.wikipedia.org/wiki/Tor_(anonymity_network)>. Luettu 15.4.2017

38 Viestintävirasto. 2017. Tietoturvan vuosi 2016. <https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf>. Luettu 15.4.2017.

39 Bloomberg. 2016. Hacked Bitcoin Exchange Users to Lose 36%. <https://www.bloomberg.com/news/articles/2016-08-07/hacked-bitcoin-exchange-users-to-lose-36-will-receive-tokens>. Luettu 15.4.2017.

40 Wired. 2014. The Inside Story of Mt. Gox, Bitcoin’s $460 Million Disaster. <https://www.wired.com/2014/03/bitcoin-exchange/>. Luettu 15.4.2017.

41 Finanssivalvonta. 2007. Talletussuoja. <http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Asiakkaansuoja/Korvausrahastot/Talletussuoja/Pages/Default.aspx>. Luettu 15.4.2017.