VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Santeri Kirjonen & Jarno Kuisma

# Bitcoin ja lohkoketjuteknologia

Liiketalous
2019

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

# TIIVISTELMÄ

| | |
|---|---|
| Tekijä | Santeri Kirjonen & Jarno Kuisma |
| Opinnäytetyön nimi | Bitcoin ja lohkoketjuteknologia |
| Vuosi | 2019 |
| Kieli | suomi |
| Sivumäärä | 53 |
| Ohjaaja | Antti Mäkitalo |

Tutkimuksemme tarkoituksena on tutkia bitcoin kryptovaluuttaa, sekä lohkoketjuteknologiaa, jonka avulla tämä toimii. Uskomme kryptovaluutan sekä lohkoketjuteknologian olevan suuri osa tulevaisuuden digitalisointia.

Elämme aikaa, jolloin kaikki meille aikaisemmin tutut käsitteet käyvät läpi teknologiavallankumousta, kuten myös valuutat ja rahansiirtomenetelmät. Kryptovaluuttojen tarkoituksena onkin syrjäyttää nykyiset rahansiirtomenetelmät pois pankkien piiristä, ja luoda luotettava järjestelmä, jossa asiakas ja myyjä voivat suorittaa maksutilanteensa ilman pankkien välikättä.

Tutkimuksemme tavoitteena on käydä läpi lohkoketjuteknologian toimintaperiaatteita, bitcoinin tietoturvaa sekä tämän mahdollista tulevaisuutta. Käymme läpi bitcoinia käsittelevää kirjallisuutta, sekä internetistä löytämiämme lähteitä.

Lohkoketjuteknologia on vielä monelle uusi käsite. Ja toivottavasti opinnäytetyömme lukija saisi paremman käsityksen siitä, miten tämä toimii, ja onko tämä turvallista.

Avainsanat Bitcoin, kryptovaluutta, lohkoketjuteknologia

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Business Information Technology

# ABSTRACT

| | |
|---|---|
| Author | Santeri Kirjonen & Jarno Kuisma |
| Title | Bitcoin and blockchain technology |
| Year | 2019 |
| Language | Finnish |
| Pages | 53 |
| Name of Supervisor | Antti Mäkitalo |

The goal of our thesis was to study bitcoin as a virtual currency, and the technology behind blockchain technology. Our belief is that cryptocurrencies and block-chain technology will have relevant a role in digitalization in the future.

We are living in the age of digitalization, where everything that used to be common and known, is rapidly transforming into something new and digital, including currencies and how we use them to purchase and sell products. Blockchain technology is a revolutionary technology that is aiming to make the third party, like a bank, obsolete in currency transactions.

In this thesis, we examined step by step the blockchain technology which makes cryptocurrencies possible. Also, the security which makes bitcoin a reliable and safe currency, and how this de-centralized security system is made was examined.

Blockchain technology is new area of technology and this thesis aimed to broaden the understanding of how it works and why it will revolutionize the future.

Keywords Bitcoin, cryptocurrency, blockchain technology

# SISÄLLYS

TIIVISTELMÄ
ABSTRACT

AVAINSANAT ..... 6
1 TUTKIMUKSEN TAVOITTEET JA JOHDANTO ..... 7
2 MIKÄ ON BITCOIN? ..... 8
2.1 Bitcoinin historiaa ..... 10
2.2 Bitcoinien louhinta ..... 10
2.3 Bitcoin käytännön maksutilanteessa ..... 11
3 LOHKOKETJU ..... 13
3.1 Bitcoin-verkko ..... 14
3.2 Noodit ja noodityypit ..... 14
4 KRYPTOGRAFIA ..... 17
4.1 Yksityisavain ..... 17
4.2 Bitcoin-osoite ..... 18
4.2.1 Base58 ja Base58Check Encoding ..... 20
4.3 Bitcoin-lompakko ..... 21
4.3.1 Laite-lompakko ..... 22
4.3.2 Ohjelmisto-lompakko ..... 22
4.3.3 Paperiset lompakot ..... 23
4.3.4 Epädeterminen lompakko ..... 24
4.3.5 Determiniset jaetut lompakot ..... 25
4.3.6 Hierarkkiset determinoidut lompakot ..... 25
5 SIIRTOJEN ELINKAARI ..... 28
5.1 Siirron luonti ..... 28
5.2 Transaktioiden kuulutukset bitcoin verkossa ..... 29
5.3 Transaktion provisiomaksu ..... 30
6 LOUHINTATEKNOLOGIA ..... 32
6.1 Ryhmälouhinta ..... 33
6.2 Bitcoinin ekonomia ja valuutan luonti ..... 35

6.2.1 Hajautettu yhteisymmärrys ..... 35
7 BITCOIN TIETOTURVA ..... 38
7.1 Turvallisuuden periaatteet ..... 38
7.1.1 Bitcoinin järjestelmän turvallinen kehittäminen ..... 39
7.1.2 Root of Trust ..... 40
7.2 Käyttäjäturvallisuus ..... 41
7.2.1 Riskin tasapainottaminen ..... 42
7.2.2 Multiavaimet ja hallinto ..... 43
8 BITCOINIIN POHJAUTUVAT MUUT VALUUTAT JA TOIMINNOT ..... 45
8.1 Vaihtoehtoisten valuuttojen ja ketjujen luokittelu ..... 45
8.2 Metakolikoiden ohjelmistoalustat ..... 46
8.2.1 Väritetyt kolikot ..... 46
8.2.2 Mastercoin ..... 46
8.3 Vaihtoehtoiset kolikot ..... 47
9 TUTKIMUKSEN TULOKSET ..... 49
LÄHTEET ..... 51

## AVAINSANAT

| | |
|---|---|
| Kryptovaluutta | Kryptovaluutta on kryptografiaan perustuva digitaalinen virtuaalivaluutta |
| BTC/XBT | Lyhenne sekä yksikkömerkki bitcoinille. |
| Peer-to-Peer | Vertaisverkko, eli verkko, jossa käyttäjät ovat vertaisia toisilleen |
| Fiat-raha | Valuutta, jolla ei ole aineellista arvoa, joka on vain valtion määrittämän arvoinen valuutta. |
| Genesis-lohko | Lohkoketjun ensimmäinen lohko, johon kaikki muut lohkot yhdistyvät ketjuna. |
| Kryptografia | Salausmenetelmä, jolla kryptataan dataa. |
| Digitaalinen allekirjoitus | Digitaalinen allekirjoitus on yhdistelmä lähettäjän yksityis- sekä julkisesta avaimesta, johon lisätään myös viesti lähettäjältä. Tämän perusteella syntyy vahvistusalgoritmi, joka toimii digitaalisena allekirjoituksena |
| Noodi | Noodi on käyttäjän tietokone bitcoin verkossa. |
| Julkinen avain | Julkinen avain toimii käyttäjätunnuksena bitcoin verkossa. |
| Yksityinen avain | Yksityinen avain toimii bitcoin lompakkosi niin sanottuna salasanana, jolla pääset käsiksi bitcoin varoihisi. |

# 1 TUTKIMUKSEN TAVOITTEET JA JOHDANTO

Tutkimuksemme tavoite on tutkia ja pohtia bitcoinia sekä lohkoketjuteknolgiaa. Toivomme, että tutkimuksemme jälkeen ymmärrämme paremmin, miten bitcoin ja lohkoketjuteknologia toimivat. Lohkoketjuteknologia on huomattavan uusi käsite, jota ei ole vielä ehditty tutkimaan niin, että se olisi kaikille ymmärrettävä. Tämän lisäksi pyrimme vastaamaan seuraaviin kysymyksiin aiheeseen liittyen:

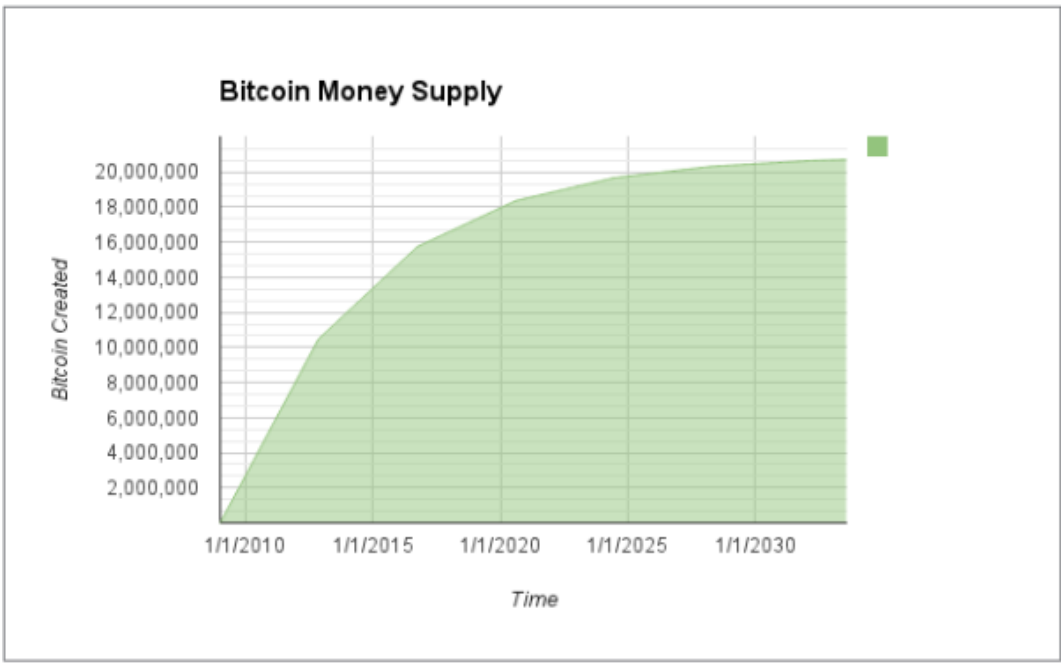
1. Miten lohkoketjuteknologia toimii ja miten sitä hyödynnetään?
   Käydä läpi, miten tämä mullistava teknologia toimii ja miten sitä voidaan hyödyntää muissakin asioissa, kuin kryptovaluutoissa.
2. Miten tietoturva toimii?
   Tietää, miten tämä järjestelmä koetaan turvallisena käyttäjille. Miten tämän tietoturva on luotu, ja miten tämä toimii?
3. Miksi bitcoin luotiin?
   Miten bitcoin osoittaa etuja, verrattuna esimerkiksi muihin valuuttoihin?
4. Tutkimuksen perusteella, mikä on oma näkemyksemme bitcoinin tulevaisuuteen liittyen?
   Tuleeko bitcoin näkemään nopean lopun vai suuren kansainvälisen hyväksymisen ”oikeaksi” kansainväliseksi valuutaksi.

# 2 MIKÄ ON BITCOIN?

Bitcoin on ensimmäinen ja tunnetuin digitaalinen valuutta. Bitcoinin lyhenteinä toimivat BTC ja XBT ja valuutan symbolina käytetään merkkiä ฿.

Bitcoin on avoimeen lähdekoodiin perustuva kryptovaluutta. Avoin lähdekoodi tekee lähdekoodista kaikille avoimen ja sitä voi käyttää maksutta. Linux ja Android käyttöjärjestelmät ovat myös avoimen lähdekoodin tuotteita. Suurin osa internetin infrastruktuurista toimii avoimen lähdekoodin ohjelmistolla. Avoimen lähdekoodin tarkoituksena on tehdä ohjelmistokehityksestä samankaltaista kuin akateemisesta tutkimuksesta, julkaisemalla koodin kaikille tutkittavaksi. Avoin lähdekoodin tarkoitus on nostaa ohjelmiston laatua. (Franco, 2014)

Bitcoin on kokoelma eri konsepteja ja teknologioita, jotka luovat pohjan digitaalisen valuutan ekosysteemille. Bitcoin on täysin digitaalinen valuutta, joten bitcoinia ei saa fyysisenä valuuttana. Bitcoinin arvo perustuu bitcoinien määrään, kysyntään ja tarjontaan. Bitcoineja on rajallinen määrä ja näitä ei voida luoda enempää. Bitcoinien lopullinen määrä tulee olemaan 21 miljoonaa bitcoinia, joita ei ole vielä kaikkia louhittu, eli päästetty kiertoon. Kuvassa 1. näemme bitcoinin lisääntymiskaaren. Bitcoineja voidaan ostaa, myydä tai vaihtaa myös perinteiseen valuuttaan esimerkiksi euroon tai dollariin. Bitcoineja ei säilötä yhdellä palvelimella, vaan bitcoin siirtyy suoraan käyttäjältä käyttäjälle (peer-to-peer). (Antonopoulos, 2015)




Kuva 1. Bitcoinin nykyisestä ja ennustetusta määrästä tulevaisuudessa. (Antonopoulos, 2015, 180)

Yksi bitcoin voidaan jakaa sataan miljoonaan osaan, ja pienin yksikkö on nimeltään Satoshi (0,00000001). Bitcoinin pitää olla jaettavissa pieniin osiin, koska yksittäinen Bitcoin voi olla tuhansia euroja. Bitcoineista käytetään myös muita nimiä kuten esimerkiksi kryptovaluutta, virtuaalivaluutta tai bittiraha. (Bitcoin Wiki)

Bitcoineja säilötään bitcoinlompakossa. Bitcoin-lompakko on sovellus tai ohjelma, jota käytetään bitcoineilla maksettaessa tai vastaanottaessa. Bitcoin-lompakko sisältää käyttäjän digitaalisen avaimen, joka toimii digitaalisena allekirjoituksena. Bitcoin-lompakkoa voidaan käyttää ilman internet yhteyttä koska kylmävarastoitu bitcoin nostetaan offline-lompakosta kertakäyttöisellä yksityisavaimella.

Bitcoineilla on arvoa aivan samalla tavalla kuten muillakin valuutoilla. Bitcoineilla on muiden valuuttojen ominaisuudet kuten esimerkiksi siirrettävyys, jaollisuus ja tunnettavuus. Bitcoinin arvo perustuu sen matemaattisiin ominaisuuksiin, eikä sen fyysisiin ominaisuuksiin kuten kulta tai hopea, eikä myöskään luottamukseen kuten fiat-valuutat. Lyhyesti bitcoinin arvo perustuu vain siihen, moniko bitcoiniin luottaa ja moniko sitä käyttää. (Bitcoin.org)

## 2.1 Bitcoinin historiaa

Bitcoin sai alkunsa 2008 elokuussa, kun bitcoin.org-palvelin, rekisteröitiin verkkoon. Myöhemmin samana vuonna lokakuussa Satoshi Nakamoton artikkeli ”Bitcoin: A Peer-to-Peer Electronic Cash System” julkaistiin. Artikkelissa kerrottiin, kuinka vertaisverkolla voidaan luoda järjestelmä, jossa elektronisia kaupankäyntejä voidaan suorittaa ilman kolmatta osapuolta kuten pankkia.

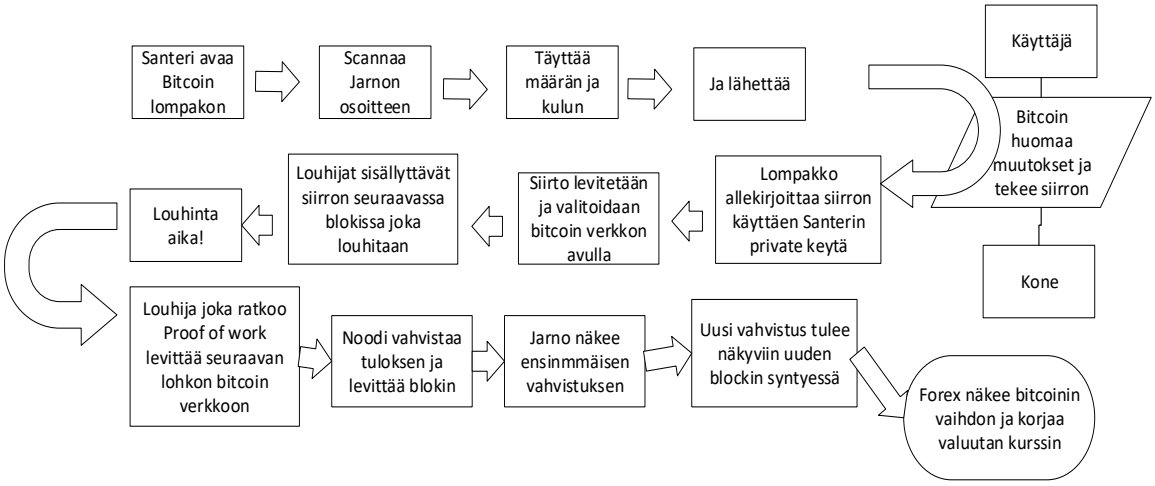
2009 tammikuussa bitcoinverkosto luotiin, ja Satoshi Nakamoto louhi ensimmäisen lohkon bitcoineja. Ensimmäinen bitcoinsiirto tapahtui, kun ensimmäinen jäsen Hal Finney latasi bitcoinsovelluksen, ja Nakamoto lähetti hänelle kymmenen bitcoinia. Myöhemmin Nakamoto antoi bitcoinin johdon Gavin Andresenille, hänestä tuli bitcoin Foundationin johtava kehittäjä.

2010 tehtiin ensimmäinen ostos bitcoineilla, kun Laszlo Hanyecz maksoi kaksi pizzaa arvoltaan 25 Amerikan dollaria käyttäen kymmenen tuhatta bitcoinia. 2011 bitcoin saavutti tärkeän rajapyykin, kun yksi bitcoin oli arvoltaan yhden Amerikan dollarin. (Fiorillo, 2018)

## 2.2 Bitcoinien louhinta

Bitcoineja vapautuu kiertoon ”louhimalla”. Louhiminen teoriassa tarkoittaa, että bitcoin käyttäjä luovuttaa tietokoneensa laskentatehoja lohkoketjun algoritmin ratkaisemiseen, kun tietokoneen laskentatehoa on hyödynnetty algoritmin ratkaisussa, käyttäjä saa tietyn määrän tai osan bitcoineja palkkioksi työstään. Lohkoketjun ratkaiseminen selkokielellä tarkoittaa, että tietokoneesi laskentatehoa hyödynnetään bitcoinien siirron käyttäjältä käyttäjälle vahvistamiseen. Tästä maksetaan louhijalle palkkio bitcoineilla. Bitcoinien louhintapalkkio on laskenut ajan myötä, alussa louhija sai 50 bitcoinia jokaista lohkoketjun ratkaisua kohden. Tämä luku puolittui 2012 marraskuussa, jonka jälkeen louhija sai 25 bitcoinia per lohkoketjun ratkaisu, vuonna 2016 palkkiosta tuli 12.5 bitcoinia. [Bitcoin mining]

Louhinta myös turvaa bitcoinjärjestelmän vääriltä siirroilta, tai ettei sama siirto tapahdu useampaan kertaa, tästä käytetään ”double-spend” nimitystä. [Bitcoin mining] Bitcoinin louhinnan voi karkeasti esittää vertauksena kultakaivoksessa louhimiseen, jossa tietokoneesi laskentateho toimii kaivajana, ja bitcoin toimii kultana. Kuvassa 2. näemme bitcoinsiirron elinkaaren, jossa käydään läpi bitcoinin vaiheita louhinnasta ja käytöstä.




Kuva 2. Kaavio bitcoinin siirtoprosessista sekä louhinnasta.

### 2.3 Bitcoin käytännön maksutilanteessa

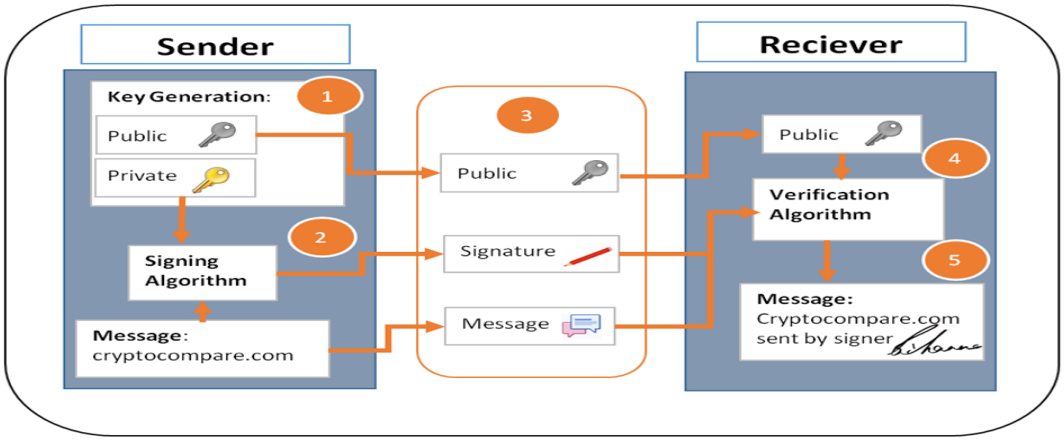
Kuvitellaan tilanne, jossa henkilö A, haluaa ostaa kupin kahvia käyttämällä bitcoineja. Kassaan on merkitty hinnastot euroissa mutta kassalla on mahdollisuus myös maksaa tuotteet bitcoineilla. Henkilö A tilaa kahvin ja työntekijä B syöttää hinnan kassalla. Kassakone kääntää dollarihinnan bitcoin-hinnaksi nykyisen kurssin mukaan ja näyttäen molempien valuuttojen hinnat. Lisäksi kassakoneella on QR-koodi maksupyynnöstä.

Työntekijä B ilmoittaa henkilölle A, että hinta on yksi dollari ja viisikymmentä senttiä tai 0.0150 BTC. Henkilö A käyttää älypuhelintaan skannatakseen QR-koodin näytöllä. Hänen älypuhelimensa näyttää 0.0150 BTC siirron kahvilaan, ja henkilö A painaa lähetä-nappia vahvistaakseen siirron. Parissa sekunnissa, suunnilleen samassa kuin maksaisit pankkikortilla, työntekijä B näkee siirron onnistuneen kassakoneella ja maksu on suoritettu.

Siirto kertoo bitcoinverkolle, että nämä bitcoinit ovat nyt vaihtaneet omistajaa, ja uusi omistaja voi nyt käyttää kyseiset bitcoinit. Tehdessään uuden ostoksen, bitcoinit siirtyvät taas verkossa, luoden lohkoketjun mukaisen omistajuusketjun.

Tällaiset siirrot ovat kuin merkintöjä kaksinkertaisessa kirjanpidossa, eli rahansiirto sisältää yhden tai useamman syötteen, jotka ovat veloituksia maksavalta bitcoinkäyttäjältä. Toisella puolella siirtoa on yksi tai useampi tuloste, jossa bitcoinit annetaan bitcoin käyttäjälle.

Jokainen bitcoinsiirto luo lohkon, joka on julkinen ja sisältää siirtoon liittyvää tietoa. Lohkossa on kaikille julkinen digitaalinen allekirjoitus omistajuudesta, jonka avulla kuka tahansa käyttäjä voi varmentaa siirron aitouden. Kuvassa 3. näemme, kuinka tämä digitaalinen allekirjoitus luodaan avainparin, nimimerkin ja viitekoodin yhdistelmästä. Bitcoin termeissä ostotoiminta toimii allekirjoituksena, joka siirtää arvoa seuraavalle omistajalle ja siirto siirtyy lohkoketjuun. (Antonopoulos, 2015)



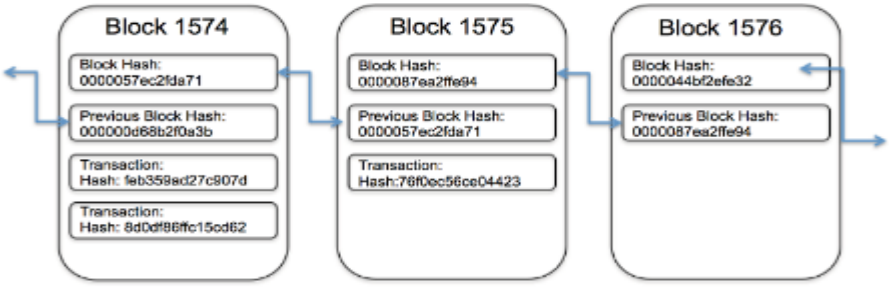

Kuva 3.Kuinka digitaalinen allikirjoitus luodaan. (CryptoCompare 2015)

# 3 LOHKOKETJU

Lohkoketjun nimi tulee tämän tavasta tallentaa transaktioiden tietoa. Lohkoketjussa transaktiot kuvastetaan lohkoina, jotka on linkitetty toisiinsa ketjuina. (Tätä havainnollistetaan kuvassa 4) Kun transaktioiden määrä kasvaa, niin myös lohkoketju kasvaa pituutta. Lohkot tallentavat sisälleen transaktioiden ajankohdan sekä siirron tiedot, jotka sitten liitetään julkiseen lohkoketjuun, jota verkon jäsenet voivat tarkastella.

Jokainen lohko sisältää tiedoissaan tiivisteen, joka toimii digitaalisena sormenjälkenä, onnistuneen transaktioerän aikaleimauksen sekä edellisen lohkon tiivisteen. Aiemman lohkon tiiviste linkittää lohkot yhteen ja estää muiden lohkojen muuttumisen tai toisen lohkon päätymisen uuden ja aiemman lohkon väliin. Näin jokainen peräkkäinen lohko vahvistaa aiemman lohkon varmennusprosessia ja myös koko lohkoketjua. Tämän takia lohkoketjua on todella vaikea sabotoida, koska jokainen lohko lisää lohkoon varmenteita ja turvaa.

Mutta vaikka lohkoketju pitää sisällään transaktioiden tietoja, tämä ei ole korvaava tekniikka esimerkiksi tietokannalle, viestinnälle tai transaktioiden prosessoinnille. Lohkoketju toimii periaatteessa tietokantana, joka tallentaa siirtojen tietoja. Lohkoketju luo tietokantaan verrattuna ominaisuuksia, jotka varmistavat tiedon oikeellisuuden. (Gupta, 2018)




Kuva 4. Lohkoketju ja lohkojen tiedot. (Gupta, 2018, 14)

Lohkoketju on vertaisverkko, jossa ei ole keskitettyä kolmatta toimijaa valvomassa tiedon kulkua. Tehokkain tapa poistaa keskitettyä valvontaa uhraamatta järjestelmän tietoturvaa ja koskemattomuutta, on ylläpitää suurta hajautettua verkkoa yksityisten käyttäjien ylläpitämänä. Tämä tarkoittaa sitä, että hajautetun verkon tietokoneet, ylläpitävät verkkoa. Näitä tietokoneita kutsutaan täysnoodeiksi.

Lohkoketjut tunnistetaan tietotekniikan ”viidentenä evoluutiona”, eli internetin luottamuksen kerroksena. Tämän takia monet asiantuntijat ovat kiinnostuneet tästä teknologiasta. Lohkoketjut voivat luoda luottamuksen verkon käyttäjien välille. Kun tieto on kerran kirjoitettu lohkoketjuverkkoon, sitä on käytännössä mahdotonta muokata tai poistaa. Vastaavaa teknologiaa ei ole ennen tätä vielä keksitty.

Kun tieto on pysyvää ja luotettavaa digitaalisessa muodossa, voidaan tätä hyödyntää laajasti esimerkiksi verkkokaupoissa. Rahansiirtoja, pankkitoimintoja ja muita sovittuja maksuja voidaan tehdä ilman pankkeja reaaliajassa odottamatta pankkipäivien kulkua.

Lohkoketju on tehokas työkalu, jolla voidaan rakentaa luottamusjärjestelmä, joka poistaa tarpeen kolmannelle osapuolelle rahansiirtotilanteissa tai sopimuksia luodessa. Sääntöjä voidaan vahvistaa algoritmeilla eikä kolmannella valvovalla osapuolella. (Laurence, 2017)

### 3.1 Bitcoin-verkko

Bitcoin-verkko on vertaisverkkorakenne, joka toimii internetissä. Termillä vertaisverkko tarkoitetaan järjestelmää, jossa verkon tietokoneet, ovat tasa-arvoisia keskenään. Tämä tarkoittaa, että verkossa ei ole palvelinta tai keskitettyjä palveluita. Noodit vertaisverkossa tarjoavat ja kuluttavat vertaisverkon palveluita samanaikaisesti. Vertaisverkot ovat luonteeltaan joustavia, hajautettuja ja avoimia kaikille.

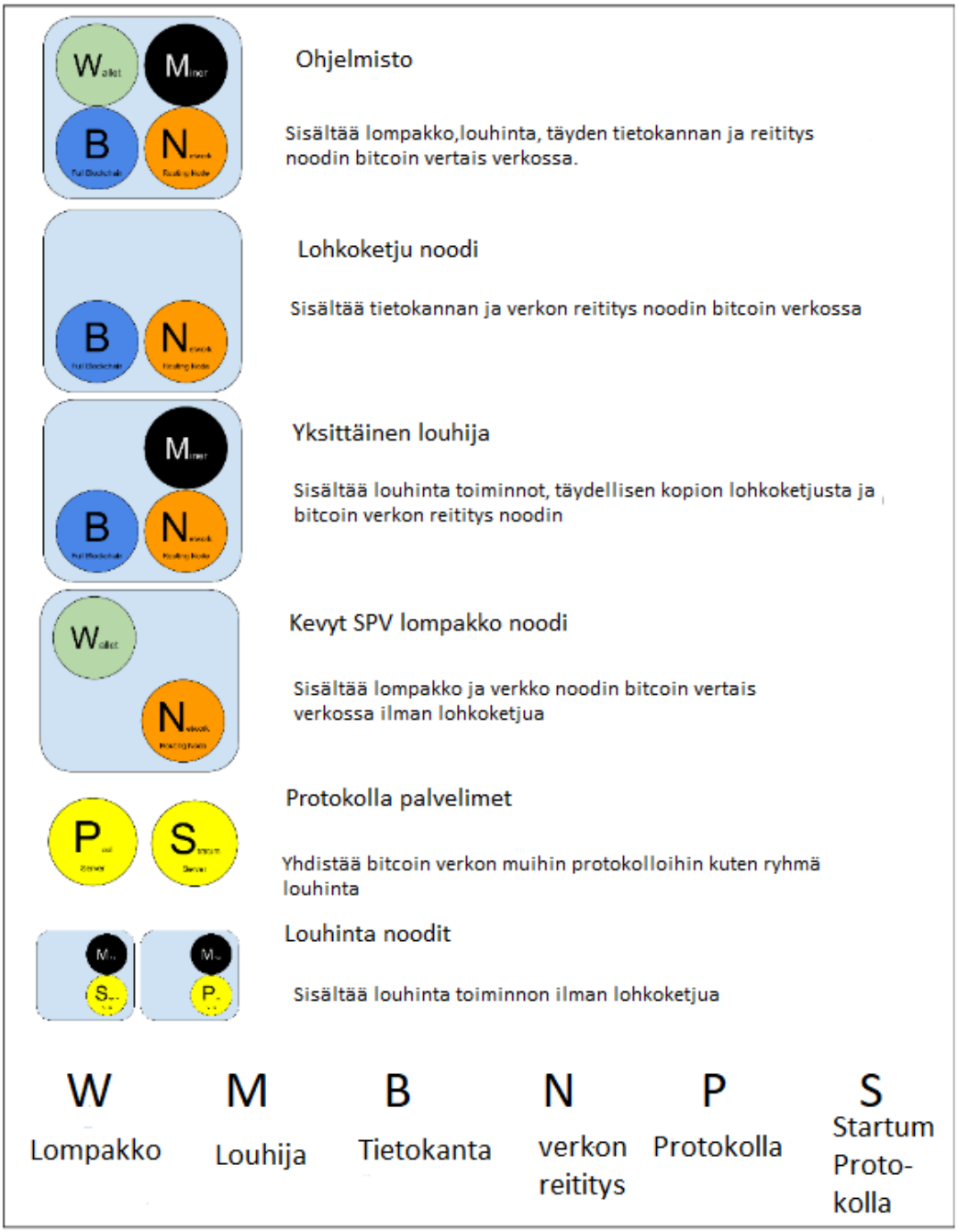
### 3.2 Noodit ja noodityypit

Vaikka noodit ovat tasa-arvoisia bitcoinverkossa, niillä voi olla väliaikaisesti ”rooleja”, tehdäkseen eri toimintoja. Bitcoin noodi on kooste seuraavista toiminnoista:

reititys, tietokanta, louhinta ja lompakkopalvelut. Kaikki noodit joutuvat osallistumaan reititykseen osallistuakseen verkostoon ja voivat myös tehdä muita toimintoja. Kaikki noodit varmistavat ja propagoivat transaktioita ja lohkotietoja.

Osa noodeista on täysiä noodeja, jotka ylläpitävät täydellistä ja päivitettyä kopiota lohkoketjusta. Tämä tarkoittaa, että tällä noodilla on täydellinen kuva koko lohkoketjusta, eli aina ensimmäisestä genesislohkosta juuri hetki sitten tapahtuneeseen siirtoon. Täydet noodit voivat autonomisesti vahvistaa transaktioita ilman muiden noodien tarkistusta. Jotkut noodit pitävät kopioita vajaista lohkoketjuista ja voivat vahvistaa transaktioita käyttämällä ”Simplified Payment Verification” metodia, joka muiden noodien pitää kuitenkin tarkistaa. Nämä noodit tunnetaan SPV tai kevytsarja noodeina.

Louhintanoodit kilpailevat uusien lohkojen luonnissa, pyörittämällä louhintaan erityisesti tarkoitettua tietokonetta. Jotkut louhintanoodit ovat myös täysnoodeja tai SPV-noodeja. Lompakkosovellukset voivat olla osana täyttä noodia, ja tämä on usein totta tietokonekäyttäjien parissa. Useimmiten puhelinkäyttäjät ovat SPV-noodeja. Kuva 5. kuvastaa eri noodityyppejä. Näiden tyyppien välillä ei ole loppujen lopuksi paljon eroja, mutta kuitenkin tarpeeksi ollakseen oma noodityyppinsä. (Antonopoulos, 2015)




Kuva 5. Kuva yleisimmistä noodityypeistä. (Antonopoulos, 2015, 142)

# 4 KRYPTOGRAFIA

Bitcoinin omistajuus pohjautuu digitaalisiin avaimiin, bitcoin osoitteisiin ja digitaalisiin allekirjoituksiin. Digitaalisia avaimia ei tallenneta verkkoon, vaan ne säilytetään käyttäjän koneella olevassa bitcoinlompakossa. Digitaaliset avaimet käyttäjän lompakossa ovat täysin itsenäisiä bitcoin protokollasta. Niitä ei voi generoida tai hallita käyttäjän lompakkosovelluksella ilman viitettä lohkoketjuun tai pääsyä internettiin. (Antonopoulos, 2015)

Digitaalista allekirjoitusta käytetään bitcoin siirron varmistamisessa. Sillä varmistettaan mistä varat on lähetetty. Digitaalinen allekirjoitus generoituu lähettäjän yksityisavaimesta digitaalisen allekirjoitus algoritmin kautta. Jokaisella siirrolla on oma digitaalinen allekirjoitus. (Lipovyanov, 2019)

Kaikki bitcoinsiirrot vaativat pätevän, eli louhitun ja lohkoketjuun hyväksytyn lohkon. Tämä voidaan generoida vain pätevillä digitaalisilla avaimilla. Avaimet koostuvat yksityisestä ja julkisesta avaimesta. Julkisen avaimen voi kuvitella kuin pankkitilin tilinumerona ja yksityisavaimen pankkitilin PIN-koodina, joka antaa käyttöoikeuden tilille. Bitcoinin käyttäjä ei näe näitä avaimia, koska niitä säilötään bitcoin lompakkosovelluksen tiedostoissa ja sama sovellus hallitsee niitä.

Bitcoinin maksuosiossa vastaanottajan julkinen avain esitetään digitaalisena sormenjälkenä, jota kutsutaan bitcoinosoitteeksi. Osoitetta käytetään kuin saajan nimeä sekissä. Bitcoin-osoite generoituu ja vastaa julkista avainta. Bitcoin-osoitteet eivät ole kuitenkaan sitovia, vaan vastaanottaja voi vaihtua, kuten paperi sekissä. Bitcoin osoite on ainoa näyttö avaimista, jonka muut käyttäjät näkevät, koska vain tämä osa jaetaan julkisesti kaikille. (Antonopoulos, 2015)

## 4.1 Yksityisavain

Bitcoin-lompakko sisältää kokoelman avainpareista, joista jokainen koostuu yksityisavaimesta ja julkisesta avaimesta. Yksityisavain on numero, joka yleensä valitaan satunnaisesti. Yksityisavaimesta generoidaan yksisuuntaisen funktion avulla

julkinen avain. Julkisesta avaimesta käytämme yksisuuntaista kryptografiaa eli hash-funktiota generoidaksemme bitcoinosoitteen.

Kuten aiemmin mainitsimme, yksityinen avain luodaan satunnaisesti kaavalla. Omistusoikeus ja yksityisen avaimen hallinta ovat käyttäjän valvonnan perusta kaikkien vastaavien bitcoinosoitteiden varoihin. Yksityisavainta käytetään digitaalisten allekirjoitusten luomisessa, joita vaaditaan bitcoineja käytettäessä. Tällä vahvistetaan siirrossa käytettyjen varojen omistajuus. Yksityisavaimen tulee pysyä salattuna, sillä yksityisavaimella voidaan varastaa tämän yksityisavaimen omistajan bitcoin varat. Yksityisavain tulee myös varmuuskopioida ja suojella mahdolliselta katoamiselta. Jos yksityisavaimen unohtaa tai hävittää, sitä ei voida palauttaa ja tämän avaimen varat on menetetty pysyvästi.

Bitcoinin avaimen luonti on periaatteessa sama kuin numeron valinta väliltä $1\text{-}2^{256}$. Valitsemismenetelmällä ei ole väliä niin kauan, kun se ei ole arvattava tai toistettavissa. Bitcoin ohjelma käyttää käyttöjärjestelmän satunnaisen numeron generointia luodakseen 256-bittisen sarjan satunnaisista numeroista. Yleensä käyttöjärjestelmä tarvitsee ihmisen apua luomaan satunnaisuutta, esimerkiksi pyytämällä liikuttamaan hiirtä muutama sekuntia. (Antonopoulos, 2015)

### 4.2 Bitcoin-osoite

Bitcoin-osoite on merkkijono kirjaimia ja numeroita, joita voidaan jakaa kaikille, jotka haluavat lähettää bitcoineja. Julkisesta avaimesta luodut osoitteet koostuvat luvulla 1 alkavasta merkkijonosta, jossa on numeroita ja kirjaimia.

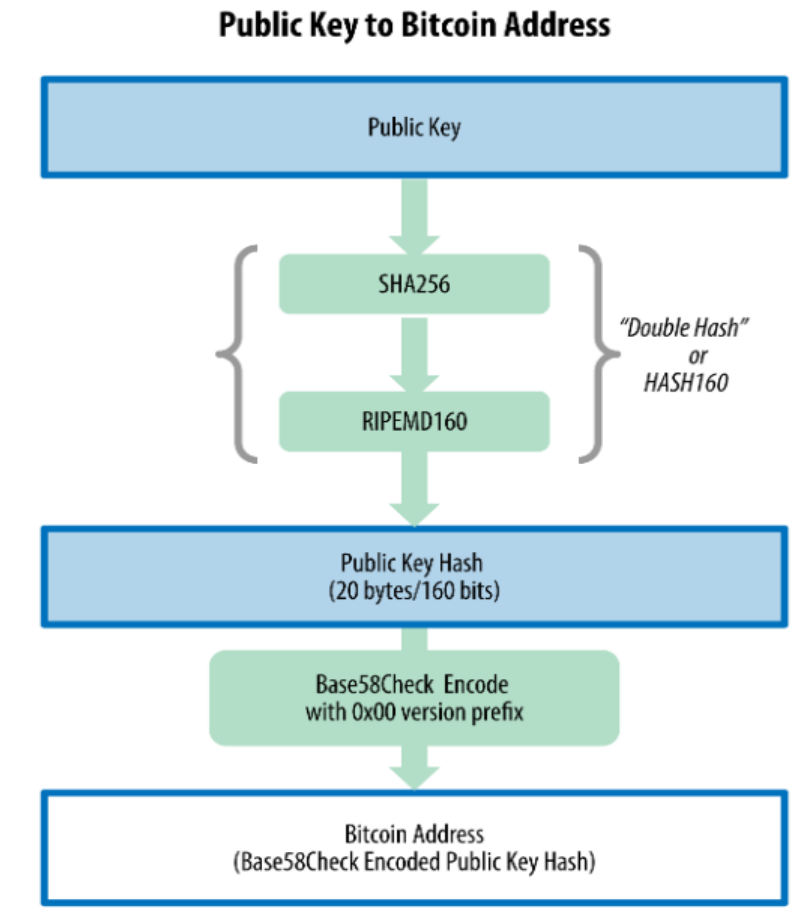
Esimerkki bitcoin osoitteesta:”1J7mdg5rpQyUHENYdx39WVWK7fsLpEoXZy ”

Bitcoin osoite on nähtävissä varoja siirrettäessä, koska bitcoin osoitetta käytetään vastaanottajan tunnistuskeinoa. Jos vertaisimme bitcoin siirtoa paperiseen sekkiin, bitcoin osoite olisi sekin vastaanottaja. Paperi-sekillä vastaanottaja voi olla myös pankki, jota vastaanottaja käyttää, mutta voi myös olla korporaatio tai instituutio. Paperi-sekit eivät tarvitse tarkkaa tiliä. Ne voidaan kirjoittaa pelkällä vastaanottajan

abstraktilla nimellä, tämä tekee paperisekeistä hyvin joustavia. Bitcoin-siirrot käyttävät samanlaista abstraktista kohdetta, bitcoinosoitetta, joka tekee myös bitcoin siirroista hyvin joustavia.

Bitcoin-osoite saadaan julkisesta avaimesta käyttämällä yksisuuntaista tiivistealgoritmia. Tiivistealgoritmi on vain yksisuuntainen keino luoda ”sormenjälki” eli tarkiste satunnaisen kokoisesta syötteestä. Tiivistealgoritmia käytetään laajasti bitcoinissa, bitcoin osoitteissa, ohjelmisto osoitteissa ja louhinta työtodistuksen algoritmissa. Algoritmeja, joita käytetään bitcoin osoitteen luontiprosessissa ovat SHA256 ja RIPEMD160.

Bitcoin-osoitteet on lähes aina esitelty käyttäjille koodattuna ”Base58Check”koodilla. Kuvassa 6. käydään läpi bitcoinosoitteen luonnin vaiheet. Aluksi meillä on vain julkinen avain, joka käännetään SHA256:lla julkisen avaimen tiivisteeksi. Tämän jälkeen Base58Check-toiminnolla tarkistetaan tiivisteen tarkistussumma. (Antonopoulos, 2015)




Kuva 6. Havainnollistava kaava kyseisestä muunnoksesta. (Antonopoulos, 2015, 72)

### 4.2.1 Base58 ja Base58Check Encoding

Normaali desimaali järjestelmä käyttää kymmentä numeroa nollasta yhdeksään, heksadesimaalijärjestelmä käyttää kuuttatoista, jossa on myös kirjaimet A-F ovat käytössä lisämerkkeinä. Numero esitettynä heksadesimaaleina on lyhyempi kuin sama desimaaleina esitettynä.

Base-64 on järjestelmä, joka käyttää kahtakymmentä kuutta pientä kirjainta, kahtakymmentä kuutta isoa kirjainta, kymmentä numeroa ja myös ”+” ja ”/” merkkiä lähettääkseen binaarista tietoa tekstin muodossa. Base-64 on useimmiten käytetty, kun lisätään binaarisia liitteitä sähköpostissa. Base-58 on tekstipohjainen binaariesitysformaatti, joka on käytössä bitcoinien ja muiden kryptovaluuttojen koodauksessa. Base58 on osajoukko Base64:sta, joka käyttää pieniä ja isoja kirjaimia

ja numeroita jättäen pois joitain merkkejä, jotka useimmiten sekoitetaan toisiinsa. Base58 on Base64 ilman numeroa nolla, kirjainta O:ta, numeroa 1 ja kirjainta I:ta, sekä symboleja ”\”, ”+” ja ”/”.

Base58 koodissa käytetyt merkit ovat

```
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
```

Base58Check on Base58:sen koodaus formaatti, jota käytetään usein bitcoinissa, tämä sisältää virheentunnistuskoodin. Tarkistussumma on lisätyt neljä tavua, jotka lisätään tiedon loppuun, jota tiivistetään. Tarkistussumma on johdettu salatun tiedon tarkisteesta, jota voidaan täten käyttää siirto- ja kirjoitusvirheiden ehkäisyssä. Kun tarkistusohjelma saa tarkistettavakseen Base58Check koodin, tarkistusohjelma voi laskea koodin tarkistussumman ja verrata sitä laskemaansa tarkistussummaan. Jos tarkistussummat eivät täsmää, tämä viittaa siihen, että on tapahtunut virhe ja Base58Check tieto on väärin. Tämä esimerkiksi estää väärinkirjoitetun bitcoin osoitteen hyväksymisen oikeaksi bitcoin lompakossa ja lompakko ilmoittaa väärästä bitcoin osoitteesta. Ilman tätä tarkistusmenetelmää bitcoinit olisivat kadonneet bittiavaruuteen, koska siirto olisi tehty vialliseen bitcoin osoitteeseen jota ei ole olemassa. (Antonopoulos, 2015)

### 4.3 Bitcoin-lompakko

Bitcoin-lompakko on ohjelma, jossa bitcoinin käyttäjät varastoivat bitcoin-avainparejaan. Bitcoin-avainpareja tarvitaan varojen säilömiseen, käyttöön ja siirtoihin. Yksityinen avain toimii bitcoin lompakon salasanana, ja näitä voi olla lompakossa useampi, mikäli varat varastoidaan hajautetusti. Jokaisella yksityisavaimella voi olla eri varoja varastoituna. (Antonopoulos, 2015)

Lompakko sovellukset toimivat mobiilissa, työpöytä ohjelmana tai sitten erillisellä laite lompakolla. Mobiili ja työpöytä sovellukset tallentavat avaimet lokaalisti. Joten niiden turvallisuudesta vastaa käyttäjä itse. Jos tietokoneen kovalevy hajoaa avaimet menevät siinä samalla, jos niistä ei ole varmuuskopiota. Erillinen laite lompakko on laite, johon tallennetaan yksityisavain. (Hill, Chopra, Valencourt, Prusty, 2018)

### 4.3.1 Laite-lompakko

Lompakko sovelluksia on monenlaisia ja niitä tulee erilaisissa formaateissa ja ne on suunniteltu erilaisille alustoille.

Laitelompakko on erillinen laite, joka tarjoaa lisä suojausta kylmille varastoille. Laitteessa on suojaus siru, jonka avulla käyttäjän ei tarvitse syöttää salaista avainta tietokoneelle varoja siirrettäessä. Avain on säilössä itse laitteessa. Jos laite hajoaa tai katoaa, avaimet saadaan takaisin uudella laitteella ”seed word”:in avulla, joka tulee laitteen mukana. ”Seed word” on vaihtoehto numerolliselle PIN-koodille, jolla bitcoinlompakko voidaan palauttaa yksityisavaimen katoamistilanteessa ja tämä on helpompi muistaa, kuin sarja satunnaisia numeroita. Usein seed word on sarja satunnaisia sanoja. Tunnettuja laite lompakkoja ovat Trezor ja Ledger nano. (Oliver Dale 2018)

Seed word on 12-24 englanninkielistä sanaa, jotka laite generoi ja ne ovat uniikkeja. Näiden avulla voidaan palauttaa lomapakon sisältö. Sanat tulee syöttää annetussa järjestyksessä ja sama sana saattaa toistua. (SatoshiLabs 2018)

### 4.3.2 Ohjelmisto-lompakko

Ohjelmisto-lompakot ovat tietokone ohjelmia, jotka toimivat tietokoneella, mobiililaitteella tai verkossa.

Tietokoneella toimivat lompakot ovat tietokone ohjelmia, jotka tallentavat varat lokaalisti tietokoneelle. Lompakko antaa käyttäjälle täyden kontrollin lompakon varoihin, joka on yksi lompakon eduista. Eikä sen tarvitse turvautua kolmannen osapuolen käyttöliittymään. Käyttäjä joutuu itse vastaamaan turvallisuudesta. Jos tietokone, jolla lompakko on asennettuna, hakkeroidaan tai koneen kovalevy hajoaa, menetetään lompakolla olevat varat. Varoja voidaan säilöä koneella, jolla ei ole pääsyä verkkoon ja on näin turvassa hakkerointi yrityksiltä.

Mobiili-lompakko on mobiili appi. Mobiili-lompakon käyttö on nopeaa ja helppoa kaupan maksutilanteissa. Mobiili-lompakoita on kahdenlaisia: applikaatio, joka tallentaa varat paikallisesti puhelimelle ja applikaatio, joka käyttää varoja verkkolompakosta.

Verkossa toimivaan lompakkoon pääsee käsiksi verkon välityksellä mistä vain. Verkko-lompakkoa pystyy käyttämään millä laitteella vain ja ne voidaan linkittää mobiili- ja tietokonelompakkoon. Verkkosivun omistajalla on hallussaan käyttäjän yksityisavain mikä on yksi lompakon haitoista. Käyttäjä joutuu luottamaan verkkosivun omistajaan ja sen turvallisuuteen. Muutamia ohjelmistolompakoita Jaxx, Exodus, Electrum, Atomic Wallet. (Oliver Dale 2018)

### 4.3.3 Paperiset lompakot

Paperilompakko on yksityisavain tulostettuna paperille QR-koodin muodossa. Yleensä paperiset lompakot myös sisältävät tätä vastaavan bitcoin osoitteen kätevyyden takia. Paperiset lompakot ovat tehokas tapa varmuuskopioida tai säilöä bitcoineja verkottomassa varastossa eli kylmävarastossa. Varmuuskopio-mekanismina paperilompakot luovat turvaa hävitettyjä avaimia vastaan. Kuvassa 7. on esimerkki paperisesta lompakosta.

Paperilompakon huono puoli on luonnollisesti fyysisen varkauden uhka. Varas, jolla on pääsy paperilompakkoon voi joko varastaa tai ottaa valokuvan avaimista ja saada bitcoineja käyttöön. Parempi tapa säilöä paperisia lompakoita on käyttää BIP0038 kryptausta yksityisavaimiin. Avaimet, jotka on tulostettu paperilompakolle, suojataan salasanalla, jonka vain haltija muistaa. Ilman kyseistä salasanaa salatut avaimet ovat hyödyttömiä. Paperiset salasanasuojatut lompakot ovat turvallisempia, koska avaimet eivät ole koskaan olleet internetissä ja ne täytyy fyysisesti hankkia tallelokerosta tai muusta fyysisesti turvallisesta kohteesta.


Kuva 7. Esimerkki kryptatusta paperisesta lompakosta. (Antonopoulos, 2015, 107)

Paperilompakkoon voidaan turvallisesti siirtää varoja, mutta paperilompakon varat on turvallisuussyistä hyvä tuhlata tai nostaa kaikki yhdellä kerralla. Tämä johtuu siitä, että käyttötilanteessa joudutaan käyttämään yksityistä avainta ja paperilompakon yksityisavainta ei voi vaihtaa. Yksi keino käyttää vain osa paperilompakon varoista, on siirtää lompakkoon jäävät varat uudelle paperilompakolle.

Paperisia lompakoita on eri muotoisina ja kokoisina, joilla kaikilla on oma tarkoituksensa. Osa paperilompakoista on tarkoitettu henkilökohtaiseen käyttöön, osa esimerkiksi lahjakortin muodossa tai pankkiholvissa säilöttävinä arvopapereina (Antonopoulos, 2015)

### 4.3.4 Epädeterminen lompakko

Ensimmäinen bitcoin lompakko oli yksinkertainen kokoelma satunnaisesti generoituja yksityisavaimia. Tämän tyyppistä lompakkoa kutsutaan ”Type-0 epädeterministiseksi lompakoksi”. Esimerkkinä ”Bitcoin Core” lompakkosovellus generoi 100 satunnaista yksityisavainta ohjelman ensimmäisellä avauskerralla ja generoi avaimia lisää jatkuvasti, vaikka uusille avaimille ei olisi tarvetta, eli epädeterminoidusti. Tämän ennakkoon generoivan lompakon lempinimi verkossa on ”Just a Bunch Of Keys” tai lyhennettynä JBOK. Nämä lompakot pyritään korvaamaan deterministisillä lompakoilla, koska näitä on vaivalloista hallita ja varmuuskopioida turhien avainten määrän takia.

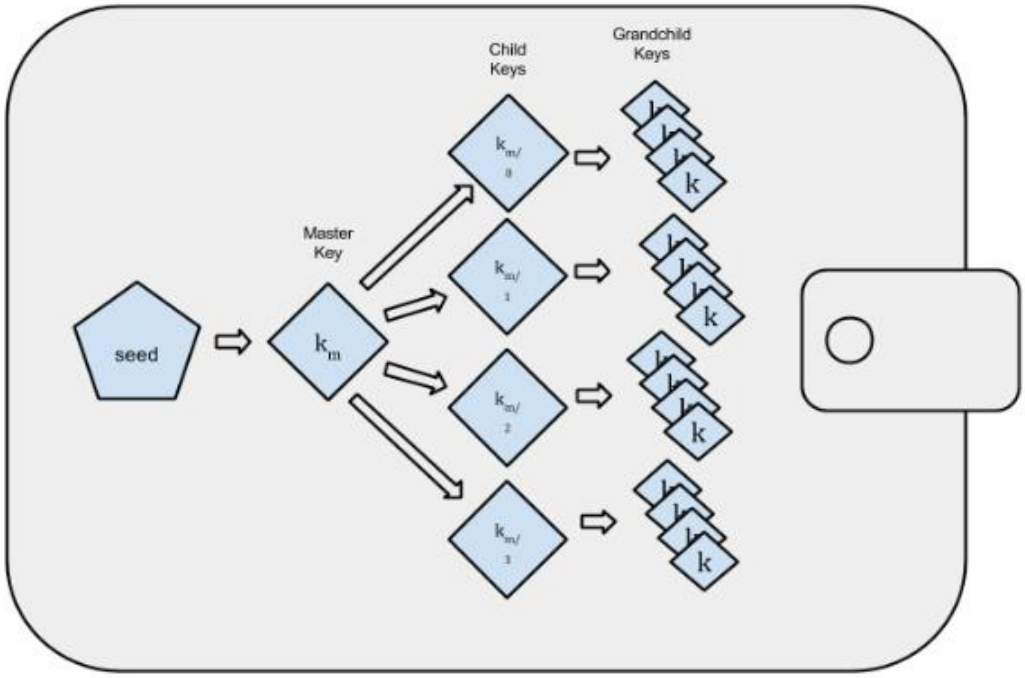
Liian monen satunnaisesti luodun avaimen haittapuoli on, että näitä käytettäessä, käyttäjän tulee tallentaa kopiot kaikista käytetyistä avaimista. Avaimen kadotessa, tällä avaimella olevat varat ovat peruuttamattomasti kadotettu bittiavaruuteen. Type-0 epädeterministinen lompakko on huono vaihtoehto lompakkosovellukseksi erityisesti, kun halutaan välttää osoitteen uudelleenkäyttöä. Tämä tarkoittaa usean avaimen hallintaa, joka luo tarpeen jatkuvalle varmuuskopioinnille. Vaikka Bitcoin Core sisältää Type-0 lompakkosovelluksen, ohjelmiston kehittäjät eivät suosittele tämän lompakon käyttöä lukuisien ongelmiensa vuoksi. (Antonopoulos, 2015)

### 4.3.5 Determiniset jaetut lompakot

Determiniset, tai jaetut lompakot ovat lompakkoja, jotka sisältävät yksityisiä avaimia, jotka on luotu yhdestä lähteestä yksisuuntaista tiivistefunktiota hyödyntäen. Lähde näille avaimille luodaan satunnaisesti hyödyntäen muuta dataa, kuten indeksinumeroa tai sarjakoodia avaimien johtamiseen. Deterministisessä lompakossa tämä äsken mainittu indeksinumero riittää palauttamaan kaikki lompakon luomat avaimet. Näin yksi varmuuskopio riittää avainten palauttamiseen. Lähdeavain eli indeksinumero on myös riittävä lompakon tietojen tuonnissa ja viennissä, mahdollistaen helpon käyttäjän avaimien siirron lompakkosovelluksen vaihtotilanteessa. Ero deterministisen ja epädeterministisen lompakon välillä on, että deterministinen lompakko ei luo satunnaisesti uusia avaimia, vaan vain silloin, kun uusille avaimille on tarvetta. (Antonopoulos, 2015)

### 4.3.6 Hierarkkiset determinoidut lompakot

Hierakkinen determinoitu lompakko on sama kuin determinoitu lompakko, mutta generoidut avaimet ovat arvojärjestyksessä. Kuvassa 8. esitetään miten avaimet ovat arvojärjestyksessä puunoksamaisesti. Vasemmalla laidalla on lähdeavain, josta lähdetään haarautumaan hierarkiassa alempiin avaimiin. Esimerkkikuvassa master key riittää palauttamaan lompakon child keyt sekä grandchild keyt katoamistilanteessa.




Kuva 8. Kuva hierarkkisista determinoiduista lompakoista. (Antonopoulos, 2015, 88)

HD lompakot (hierarkkiset determinismiset lompakot) tarjoavat kaksi etua verrattuna epädeterministisiin lompakoihin. Ensimmäinen etu on puurakenne. Jota voidaan käyttää edustamaan organisaationaalista tarkoitusta, kuten tiettyä haaraa aliavaimista, jota käytetään varoja vastaanottaessa ja toista haaraa voidaan käyttää maksettaessa. Haarojen avaimia voidaan myös käyttää yritysmaailmassa, kun haaroja allokoidaan yrityksen eri osastoille, tytäryhtiöille sekä tiettyjen toimintojen tai kirjanpidon kategorioihin. Kuvitellaan yritys, joka on jakanut bitcoin varojaan usealle osastolle. Näiden osastojen esimies omistaisi Master Keyn, jolla hän voi jakaa child avaimia eri osastoille, mutta hän itse voi kuitenkin palauttaa itselleen alaistensa avaimet.

Toinen etu HD lompakoilla on, että käyttäjä voi luoda sarjan julkisia avaimia ilman tarvetta näiden yksityisavaimille, eli luoda vastaanottoavaimia. Tämä sallii HD lompakoiden käytön myös suojaamattomilla palvelimilla ja mahdollistaa bitcoinien vastaanoton yhteen lompakkoon, useammalla julkisella avaimella. Julkisia avaimia ei tarvitse ladata ennakkoon eikä johdattaa ennakkoon lähteeseen, eikä palvelimella

tarvitse olla yksityistä avainta varojen käyttämiseen. Voimme kuvitella tästä esimerkkinä tilinumeron, jonka käyttäjä voi antaa asiakkaille, joilta käyttäjä odottaa maksua. Näissä kuitenkin on aina eri tilinumero, johon kuitenkin kirjaudut käyttämällä samaa salasanaa. Näin maksajat eivät osaa liittää käyttäjää toisiin annettuihin julkisiin avaimiin, parantaen anonymiteettiä, kun käyttäjät eivät tiedä maksavansa samalle henkilölle, eri julkisen avaimen takia. (Antonopoulos, 2015)

# 5 SIIRTOJEN ELINKAARI

Bitcoin siirron elinkaari alkaa siirron luonnista. Siirto on tämän jälkeen allekirjoitettu avaimella, mikäli kyseessä on esimerkiksi yritys, jossa useamman käyttäjän tulee allekirjoittaa siirto. Tämän jälkeen siirto kuulutetaan bitcoin verkossa, jossa jokainen verkkonoodi eli kuulutuksen vastaanottaja vahvistaa ja levittää siirtokuulutusta, kunnes uutinen on saavuttanut lähes kaikki verkkonoodit. Viimeisenä varmistuskeinona toimii louhintanoodi ja siirto sisällytetään uuteen siirtolohkoon, joka sijoitetaan lohkoketjuun.

Kun siirto on osana lohkoketjua ja tämän lohkon aiempi ja jälkeinen lohko kykenevät varmistamaan siirron aitouden, lohkosta tulee pysyvä osa bitcoin tilikirjaa. Tämän jälkeen siirto näkyy kaikille käyttäjille hyväksyttynä. Siirrettävät varat valtuutetaan uudelle vastaanottajalle, joka on nyt vapaa käyttämään varoja haluamallaan tavalla, ja näin alkaa siirron elinkaari uudelleen. (Antonopoulos, 2015)

## 5.1 Siirron luonti

Bitcoin transaktion voidaan kuvitella paperisen sekin siirtona. Kuten sekki, siirto on instrumentti, joka ilmaisee aikomusta siirtää rahaa ja ei ole näkyvä maksujärjestelmälle ennen kuin se on toimitettu nostettavaksi.

Transaktion voi luoda kuka vain verkossa tai verkon ulkopuolella, vaikka transaktion luoja ei olisikaan valtuutettu henkilö käyttäjätilillä. Esimerkiksi kirjanpitäjä saattaa käsitellä yrityksen toimitusjohtajan sekkejä. Vastaavasti käyttäjän kirjanpitäjä voi luoda bitcoin transaktioita ja tämän jälkeen pyytää toimitusjohtajaa lisäämään siirtoihin digitaalisen allekirjoituksensa, joka tekee siirroista lopullisia. Sekeissä yleensä lukee maksajan tili, kun taas bitcoin transaktiossa lukee edellisen transaktion lähde, eikä varsinaisesti siirtäjän käyttötiliä.

Kun siirto on luotu, varojen omistaja allekirjoittaa siirron. Jos tämä luotiin oikein ja allekirjoitettiin, allekirjoitettu transaktio on nyt voimassa ja sisältää kaiken tarvittavan tiedon siirron mahdollistamiseen. Viimeisenä, siirto julkistetaan bitcoin verkossa ja tietoa levitetään tietokoneelta tietokoneelle, kunnes louhija ratkaisee

yhtälön ja luo tästä uuden lohkon lohkoketjuun eli julkiseen tilikirjaan. (Antonopoulos, 2015)

### 5.2 Transaktioiden kuulutukset bitcoin verkossa

Ensin transaktio pitää toimittaa bitcoin verkkoon, josta se voidaan propagoida ja liittää lohkoketjuun. Yksinkertaistettuna bitcoin transaktio on vain 300-400 tavua dataa ja tämän tulee saavuttaa yksi kymmenistä tuhansista bitcoin noodeista. Lähettäjän ei tarvitse luottaa noodeihin, joita hän käyttää transaktion kuuluttamiseen, kunhan lähettäjä lähettää tiedon useammalle kuin yhdelle noodille. Noodien ei myöskään tarvitse luottaa lähettäjään tai vahvistaa lähettäjän henkilöllisyyttä, koska transaktio on allekirjoitettu eikä sisällä luottamuksellista tietoa, yksityisiä avaimia eikä pääsytietoja. Transaktiota voidaan julkisesti kuuluttaa käyttäen mitä vain järjestelmään sisäänrakennettuja tiedotusväyliä. Kunnes tiedot transaktiosta saapuvat yhdelle noodille. Noodi propagoi sen eteenpäin muille noodeille, järjestelmässä ei ole väliä, kuinka tieto saapuu ensimmäiselle noodille.

Bitcoin transaktiot voidaan välittää bitcoinverkossa turvaamattomalla kaistalla kuten WiFi:lla, Bluetoothilla, NFC:lla, Chirpillä (radioaalloilla), viivakoodeilla tai yksinkertaisesti kopioimalla verkkolomakkeelle. Bitcoin transaktio voidaan jopa salata käyttämällä hymiöitä ja siirtää julkiselle foorumille. Bitcoin on muuttanut valuutan tietorakenteeksi. (Antonopoulos, 2015)

Kun bitcoin transaktio on lähetetty yhdelle noodille, joka on osana bitcoin verkostoa, noodi vahvistaa siirron. Jos noodi toteaa transaktion oikeaksi, alkaa noodi kuuluttaa tietoja transaktiosta eteenpäin verkossa. Noodi vastaa transaktion lähettäjälle viestillä, jos transaktio oli validi. Jos siirto ei ole validi, noodi kieltäytyy näistä tiedoista ja lähettää kielteisen viestin lähettäjälle.

Bitcoin verkko on vertaisverkko, joka tarkoittaa, että jokainen bitcoin noodi, eli käyttäjän laite on yhdistetty useaan eri bitcoin noodiin, jotka verkko havaitsee noodien käynnistysprosessin aikana vertaisverkon protokollan avulla. Koko bitcoin verkko on löyhästi yhteydessä ilman varsinaista hierarkiaa, joten verkon kaikki rakenteet ovat keskenään tasa-arvoisia. Viestit, jotka sisältävät transaktiot ja lohkot,

propagoidaan jokaisesta noodista verkon muille käyttäjille, jotka on yhdistetty kyseiseen noodiin. Uusi validoitu transaktio, joka lähetetään noodiin, lähetetään eteenpäin kolmesta neljään viereiseen noodiin. Tämä jatkuu, kunnes kaikki noodit ovat vastaanottaneet tiedon siirrosta.

Bitcoin verkosto on suunniteltu propagoimaan transaktioita ja lohkoja kaikille noodeille tehokkaasti ja joustavasti mutta samalla turvallisesti. Estääkseen spämmiä, palvelunesto hyökkäyksiä ja muita rasitteita bitcoin järjestelmässä, kaikki noodit itsenäisesti validoivat kaikki transaktiot ennen sen propagoimista eteenpäin. (Antonopoulos, 2015)

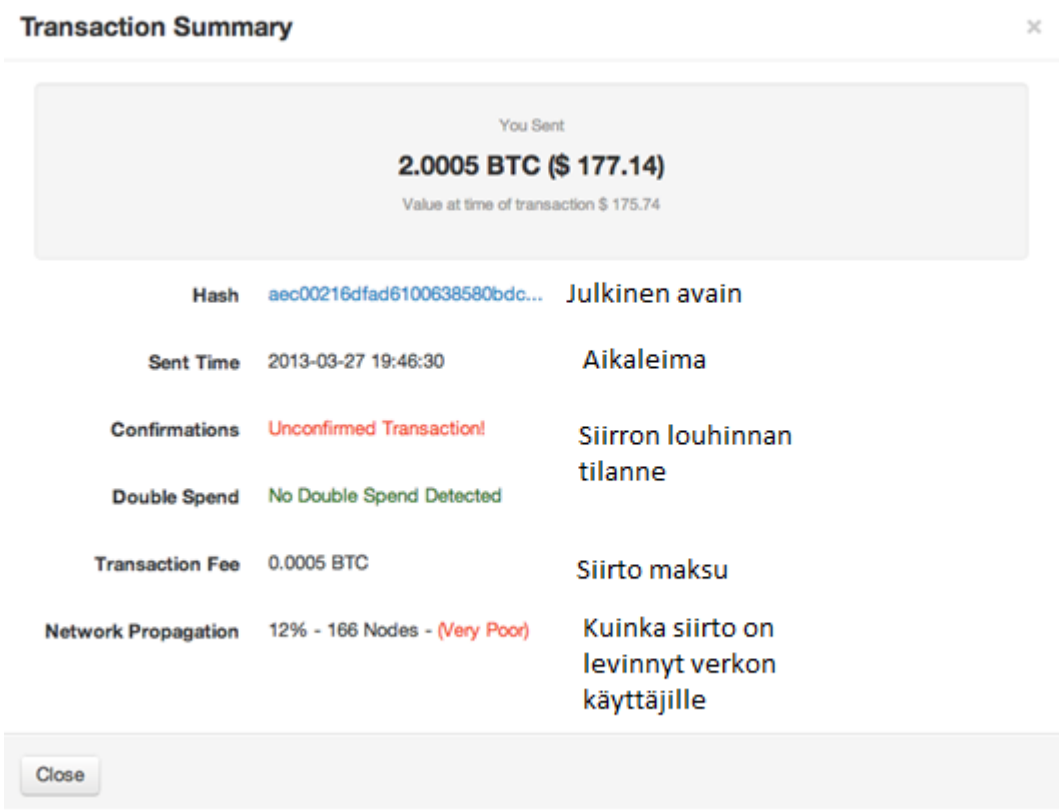
### 5.3 Transaktion provisiomaksu

Useimmat siirrot sisältävät transaktiomaksun, joka kompensoi bitcoin louhijoita verkoston turvaamisesta. Suurin osa lompakkosovelluksista laskee ja sisällyttää transaktioprovisiot automaattisesti.

Transaktiomaksut luovat kannusteen louhia transaktioita lohkoketjuun. Louhija kerää transaktiokulut talteen palkkiona lohkoketjun ylläpidosta.

Transaktiokulut lasketaan perustuen siirron kokoon kilotavuina, ei transaktion varsinaiseen rahalliseen arvoon. Kaiken kaikkiaan transaktiokulut perustuvat markkinointivoimaan bitcoin verkostossa. Louhijat priorisoivat siirrot perustuen useaan eri kriteeriin ja voivat jopa prosessoida transaktioita ilmaiseksi tietyissä tilanteissa. Transaktiokulut vaikuttavat käsittelyprioriteettiin. Suuremman palkkion sisältävät transaktiot käsitellään yleensä pienempipalkintoisia transaktioita nopeammin. Transaktioita voidaan tehdä myös ilman transaktiomaksua. Tämä kuitenkin hidastaa käsittelyä, mutta kaikki transaktiot käydään lopulta läpi.

Ajan myötä transaktiopalkkiot ja näiden vaikutus verkostoon muuttuu. Alussa transaktiomaksut oli vakioitu mutta verkoston laajentuessa maksuja on kuitenkin lievennetty. Rakenteen vapauttaminen on tehty lisäämään markkinavoimaa verkostossa, jonka voima määrittyy verkoston kapasiteetin ja transaktioiden suuruuden perusteella. Kuvassa 9. näemme julkiseen tarkoitukseen luodun tietoruudun siirrosta. Tämä ikkuna sisältää bitcoin siirron tiedot. (Antonopoulos, 2015)




Kuva 9. Kuva bitcoin transaktion tiedoista.

# 6 LOUHINTATEKNOLOGIA

Louhinta on prosessi, jossa uusia bitcoineja lisätään bitcoin verkkoon mutta tämä ei ole sen päätarkoitus. Louhinta myös turvaa bitcoin järjestelmää haittatekijöiltä ja varmistaa, että siirrot siirtävät varat vain kerran. Louhijat luovuttavat prosessointivoimaa bitcoin verkolle ja saavat vastineeksi palkkioita bitcoineina.

Louhijat validoivat bitcoin siirtoja ja tallentavat nämä tilikirjoille. Uusi lohko, joka sisältää siirron tiedot liitetään aiempaan lohkoon jatkaen lohkoketjua. Siirrot, jotka tulevat osaksi lohkoketjua uutena lohkona, ovat validoituja lohkoja, joka oikeuttaa bitcoin siirron vastaanottajan käyttämään vastaanottamansa bitcoinit seuraavassa siirrossaan.

Siirtojen louhijoille on olemassa kahdenlaisia palkintoja: joko he saavat täysin uudesti luotuja bitcoineja, jotka syntyvät uuden lohkon valmistuessa, tai heille maksetaan transaktiomaksu siirron tapahtuessa. Saadakseen tämän palkkion, louhijat kilpailevat keskenään ratkaistakseen matemaattisen algoritmin, joka perustuu kryptografiseen tunnistealgoritmiin. Ongelman ratkaisusta myönnetään työtodistus, joka on sisällytetty juuri syntyneeseen lohkoon. Tämä toimii todisteena, että louhija on käyttänyt riittävästi tietokoneen prosessointikykyä ongelmanratkaisuun. Kilpailu louhijoiden välillä luo perustan bitcoinin lohkoketjuteknologian tietoturvalle.

Uusien kolikoiden generointia kutsutaan louhimiseksi. Louhintaa voidaan verrata kultakaivokseen, joskus louhija löytää kultaa, ja joskus kaivoksen kulta loppuu, joten ajan myötä kultaa löytyy vähemmän. Bitcoin verkoston rahan määrä määräytyy louhinnan määrällä, aivan kuten keskuspankki painattaa lisää rahaa. Neljän vuoden välein bitcoin palkkio louhinnasta laskee.

Bitcoin louhijat saavat myös palkkioita transaktiomaksuina. Aina kun käyttäjä siirtää bitcoineja toiselle käyttäjälle, hän maksaa pienen provision louhijalle, joka lisäsi tämän siirron lohkoketjuun. Tämä transaktio on yleisesti 0.5% siirron suuruudesta. Ennusteen mukaan, ainoa tulonlähde louhijoille on transaktiomaksu vuonna 2140 kun kaikki bitcoinit on louhittu ja uusia ei voida enää luoda.

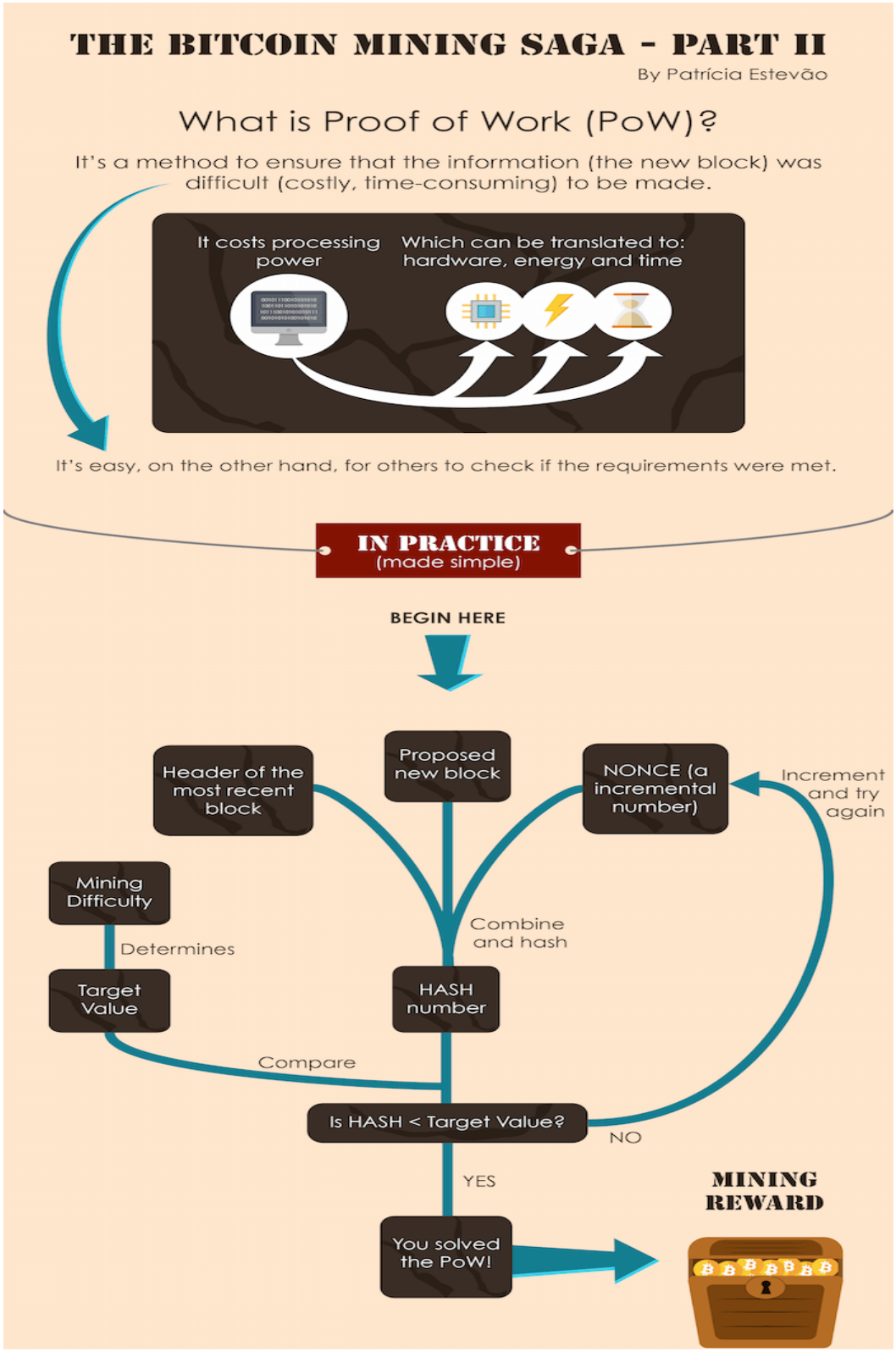
Louhinta terminä on kuitenkin harhaanjohtava. Louhinnan tarkoituksena ei ole luoda uusia bitcoineja ja tuottaa rahaa, vaan toimia kannusteena käyttäjille ratkoa bitcoin siirtoja. Louhinta on keino pitää bitcoin verkko turvallisena ja varmistaa rahan liikkuvuus. Tätä kutsutaan hajautetuksi tietoturvaksi. Verkostoa ei turvaa yksittäinen palvelu vaan koko bitcoin verkko varmistamalla jokaisen siirron laillisuuden, täsmällisyyden ja toimivuuden.

Louhinta on keksintö, joka tekee bitcoinista uniikin tekemällä tämän tietoturvasta täysin hajautetun. Tämän tarkoitus on luoda järjestelmä, jossa ostaja ja myyjä eivät tarvitse pankkia välikädeksi siirtoja luodessaan vaan siirrot ovat täysin käyttäjien hallitsemia ja turvaamia. (Antonopoulos, 2015)

### 6.1 Ryhmälouhinta

Ryhmälouhinta muodostuu, kun ryhmä louhijoita työskentelevät yhdessä ratkaistakseen matemaattisen ongelman. Ryhmän johtaja saa palkkion, jos ryhmä saa ongelman ratkaistua. Johtajan vastuulla on jakaa palkkio ryhmän jäsenille, jotka ovat osallistuneet louhintaan. Tämä on tuottoisampaa kuin yksin louhiminen, missä vain yksi louhija yrittää ratkaista ongelma. On olemassa monenlaisia malleja, jolla ryhmän johtaja voi maksaa louhijoille. Pay Per Share (PPS) malli millä johtaja maksaa saman summan jokaiselle, joka on osallistunut louhintaan. Ehdotettu malli, joka laskee palkkion kuinka paljon laskutehoa, on luovutettu ongelman ratkaisuun. On olemassa monenlaisia kaupallisia yrityksiä, jotka tarjoavat sopimuksia verkon välityksellä. (Bashir 2018)

Kuvassa 10. näemme kuinka louhinta alkaa kuvan yläosasta, kun lohkoketjuun ehdotetaan uutta lohkoa. Tämä lohko saa tiivistenumeron louhinnan tuloksena (HASH number), ja seuraavaksi tiivisteen arvo tarkistetaan (is HAS < Target value?). Mikäli tiiviste ei ole oikea, se menee uudelleen louhittavaksi. Tiivisteen vertailun kohteena toimii edellisen lohkon tiiviste, louhinnan vaikeus sekä kohdearvo. Kun tiivisteen arvo on oikea, liitetään lohko lohkoketjuun ja louhinnan tekijä saa työtodistuksen sekä bitcoineja.




Kuva 10. Havainnollistava kuva, kuinka bitcoinin työtodistus luodaan. (Patricia Estavâo 2013)

### 6.2 Bitcoinin ekonomia ja valuutan luonti

Bitcoinit ”lyödään” aina kun uusi lohko on korjattu ja tarkistettu sekä liitetty lohkoketjuun. Uusia lohkoja generoituu noin kymmenen minuutin välein, luoden täysin uusia bitcoineja.

```
# Original block reward for miners was 50 BTC
start_block_reward = 50
# 210000 is around every 4 years with a 10 minute block interval
reward_interval = 210000

def max_money():
    # 50 BTC = 50 0000 0000 Satoshis
    current_reward = 50 * 10**8
    total = 0
    while current_reward > 0:
        total += reward_interval * current_reward
        current_reward /= 2
    return total

print "Total BTC to ever be created:", max_money(), "Satoshis"
```

Yllä näemme kaavan, jonka perusteella lasketaan bitcoinien lopullinen määrä. Koodin alussa huomaamme louhinnan palkkion olevan 50 bitcoinia ja tätä alempana koodi, joka kuvastaa kaavan maksimimäärälle bitcoineja, ja miten palkkio pienenee bitcoinien lisääntyessä, kunnes kaava saavuttaa huippuintervallinsa, eli 21 000 000 bitcoinia. (Antonopoulos, 2015)

Bitcoinit katoavat kierrosta, kun niiden omistaja menettää lompakon hallintaan tarvittavan yksityisavaimen. Avaimia voidaan menettää jo pelkän huolimattomuuden takia. Hävinnyttä salausavainta ei voi palauttaa bitcoinin hajautetun järjestelmän takia. Uskotaan että bitcoineja on kateissa noin 4 miljoonaa kappaletta. (Teemu Laitila 2017)

#### 6.2.1 Hajautettu yhteisymmärrys

Hajautettu järjestelmä kuulostaa vaikeasti hallittavalta ja herättää kysymyksen, miten bitcoin ylläpitää luottamusta ja määrää kuka omistaa bitcoineja. Kaikki aikaisemmat maksujärjestelmät perustuivat luottamusjärjestelmään, jossa on keskitetty

valta yhdelle ulkopuoliselle tekijälle kuten pankille. Bitcoinverkossa ei ole keskitettyä hallinnoijaa kuten pankeissa, mutta bitcoin kuitenkin tarjoaa kaikille tietonoodeille julkisen tiedon tapahtuneista transaktioista. Lohkoketjuteknologia ei ole yhden hallitsevan organisaation ylläpitämä, vaan kaikkien järjestelmän käyttäjien yhteinen aikaansaannos. Kaikki bitcoin noodit sisältävät saman tiedon, joka täsmää muiden noodien tietoihin.

Satoshi Nakamoton alkuperäinen keksintö oli hajautettu järjestelmä, jota ylläpidetään kehittyvällä yhteisymmärryksellä. Kehittyvällä, koska yhteisymmärrystä ei saavuteta ikinä lopullisesti, järjestelmällä ei ole olemassa äänestystä tai tarkkaa hetkeä, jolloin yhteisymmärrys tapahtuisi suoranaisesti. Tämän sijaan, bitcoin järjestelmän yhteisymmärrys on tuhansien epäsynkronisten vuorovaikutusten tuote itsenäisten bitcoinnoodien eli käyttäjien välillä, jotka kaikki noudattavat järjestelmän sääntöjä. Kaikki bitcoinin ominaisuudet, kuten valuutta, transaktiot, maksut ja tietoturvamallit eivät ole missään keskitetyn vallan tai luottamuksen varassa.

Bitcoinin hajautettu yhteisymmärrys pyörii neljän prosessin ympärillä, jotka tapahtuvat jatkuvasti ja itsenäisesti kaikissa bitcoin verkoston noodeissa eli käyttäjien laitteissa:

- Noodien itsenäinen transaktion vahvistus, eli louhinta, joka käy läpi transaktion hyväksymiskriteerit.
- Transaktioiden yhdistäminen aiempiin lohkoihin lohkoketjussa louhinnan tuloksena, jonka tulokset näemme louhijoiden työtodistuksina.
- Uusien lohkojen tarkistus.
- Lohkoketjun jokaisen lohkon ratkaisu, jonka kumulatiivinen laskenta on varmistettu työtodistuksen perusteella.

Nämä neljä prosessia sisältävät seuraavat tarkistusmenetelmät, varmistaakseen transaktion aitouden ja virheettömyyden:

- Transaktion syntaksiarvo sekä tietorakenne tulee olla oikea.
- Vastaanottajakenttä ja lähettäjäkenttä tulee olla täytettynä.
- Transaktion tavumäärä tulee olla maksimiarvon alapuolella.

- Syöttöarvon täytyy olla mahdollinen määrä, eli vähemmän kuin 21 miljoonaa ja enemmän kuin 0.
- Siirrettävät varat pitää löytyä lohkoketjun aiemmista lohkoista.
- Siirrossa käytettäviä varoja ei ole samanaikaisesti muussa transaktiossa.
- Peruuttaa siirto, jos transaktiomaksu on liian pieni.

(Antonopoulos, 2015)

# 7 BITCOIN TIETOTURVA

Bitcoinin turvaaminen on haastavaa koska bitcoin ei ole abstrakti viittaus arvoon kuten pankkitilin saldo. Bitcoin on enemmän kuin digitaalinen valuutta tai digitaalinen kulta. Avaimien hallussapito avaa bitcoin tilin, joka vastaa rahan tai arvometallin hallussapitoa. Sen voi hävittää, se voidaan varastaa tai voidaan vahingossa antaa väärä summa siirrossa. Missään näissä tapauksissa, käyttäjä ei saa korvauksia, vastaavasti jos pudottaa rahaa julkiselle jalkakäytävälle.

Bitcoinilla on kuitenkin ominaisuuksia, joita rahalla, kullalla tai pankkitilillä ei ole. Bitcoin lompakko, joka sisältää käyttäjän avaimet voidaan varmuuskopioida aivan kuten muutkin tiedostot. Se voidaan varastoida useampana kopiona tai jopa tulostettuna paperille fyysiseksi varmuuskopioksi. Käyttäjä ei voi varmuuskopioida kultaa, rahaa tai pankkitilejä. Bitcoin eroaa aiemmista tuntemistamme valuutoista ja sen turvallisuutta pitää miettiä uudella tavalla. (Antonopoulos, 2015)

## 7.1 Turvallisuuden periaatteet

Bitcoinin pääperiaate on sen hajautettu luonne ja se tarjoaa bitcoinille yksilöllisiä keinoja luoda turvaa. Keskitetty malli, kuten perinteinen pankki vaatii paljon kolmannen tahon hallintaa, jotta järjestelmä voidaan pitää turvallisena. Kun vertailemme hajautettua ja keskitettyä järjestelmää, hajautetun järjestelmän vastuu siirtyy bitcoinin käyttäjille. Koska tietoverkon turvallisuus perustuu louhijoiden työtodistuksiin eikä verkoston hallintaan, verkosto voidaan pitää julkisena ja ylimääräistä salausta ei tarvita bitcoin liikenteen seurantaan.

Perinteisessä pankkimaksuverkossa, kuten luottokorttijärjestelmässä maksu on hyvin avoin koska se sisältää käyttäjän yksityistunnisteen eli luottokorttinumeron. Ensimmäisen ostokerran jälkeen kaikki, joilla on nämä kyseiset tunnistetiedot, voi laskuttaa käyttäjää uudestaan ja uudestaan. Tämän vuoksi maksuväylän pitää pysyä salattuna alusta loppuun ja täytyy varmistaa, ettei siirron ulkopuolinen käyttäjä voi sabotoida maksuväylää siirrossa tai pankkitilillä. Jos ulkopuolinen käyttäjä pääsee käsiksi järjestelmään, he voivat murtaa siirtojen tiedot, ja hyödyntää näitä tietoja

uusien maksujen luonnissa eli käyttää toisen käyttäjän bitcoinlompakkoa. Tätä vakavampana ongelmana on käyttäjien tietojen vuotaminen.

Bitcoin siirto auktorisoi vain tietyn arvon tietylle vastaanottajalle, eikä tätä voida väärentää tai muokata. Se ei paljasta yhtäkään yksityistä tietoa, kuten siirron osapuolia eikä se voi auktorisoida ylimääräisiä rahansiirtoja. Bitcoin maksuverkostoa ei ole tarpeellista kryptata. Kaikki bitcoin siirrot ilmoitetaan julkisesti verkossa kaikille ilman mitään tietoturvariskejä.

Bitcoinin hajautettu turvallisuusmalli tuo paljon vastuuta päätekäyttäjälle. Tämä vastuu tarkoittaa pääasiassa henkilökohtaisten avaimien salaamista ja varmuuskopiointia. Useimmille käyttäjistä se ei ole helppoa, erityisesti niille käyttäjille, jotka käyttävät julkisessa käytössä olevia tietokoneita. Bitcoinin hajautettu malli estää tietomurtojen aiheuttamat suuret tietovuodot mutta aiheuttaa enemmän vastuuta ja riskejä yksilökäyttäjiä kohtaan, jotka ovat vastuussa omista tiedoistaan. (Antonopoulos, 2015)

### 7.1.1 Bitcoinin järjestelmän turvallinen kehittäminen

Tärkein periaate bitcoin kehittäjille on hajauttaminen. Useimmat kehittäjät ovat tutustuneet jo keskitettyihin turvallisuusmalleihin ja ovat yrittäneet soveltaa näitä bitcoin sovelluksiinsa tuhoisin tuloksin.

Bitcoinin turvallisuus riippuu täysin sen hajautetuista avaimista ja itsenäisistä louhijoiden validoinneista. Jos käyttäjä haluaa kehittää bitcoinin tietoturvaa, käyttäjän tulee varmistua, että hän noudattaa bitcoinin tietoturvaregulaatioita.

Yleinen esimerkki ajatusmalli, joka monella bitcoinia kehittävällä käyttäjällä on, on vähentää bitcoinin hajautusta ja keskittää enemmän valtaa yhdelle palvelimelle. Esimerkiksi poistaa lohkoketjujen varmuuskopioinnit käyttäjiltä, ja varastoida kaikki lohkoketjukaaviot yhdelle palvelimelle. Tämä poistaa hajautetun järjestelmän tietoturvan verkon kaatumista vastaan. Jos hajautettu verkko kaatuu, löytyy

varmuuskopio tuhansilta eri noodeilta. Keskitetyssä verkossa palvelimen kaatuminen voi johtaa jopa koko lohkoketjun katoamiseen.

Toinen yleinen virhe on luoda siirtoja lohkoketjun ulkopuolella, kun tarkoituksellisesti yritetään vähentää transaktiomaksuja ja nopeuttaa transaktion käsittelyä. Lohkoketjun ulkopuolella tarkoitamme bitcoinin ulkoista järjestelmää, joka tekisi transaktiot käyttäjien sijasta. Järjestelmä, joka tekee transaktion lohkoketjun ulkopuolella, tallentaa siirrot sisäiseen ja keskitettyyn tilikirjaan ja vain satunnaisesti synkronoi nämä bitcoinin lohkoketjuun. Kun siirrot tehdään lohkoketjun ulkopuolella, väärin turvatut keskitetyt tilikirjat voidaan väärentää, siirtäen varoja ja tyhjentämällä tilejä kenenkään huomaamatta. (Antonopoulos, 2015)

### 7.1.2 Root of Trust

Perinteinen tietoturva-arkkitehtuuri perustuu konseptiin, jota kutsutaan luottamuksen juureksi, eli toiminnot järjestelmän juuressa, joita järjestelmä voi aina hyödyntää luottamuksella. Tietoturva arkkitehtuuri kehitetään luottamuksen juuren ympärille samankeskisten ympyröiden sarjana, vähän kuin sipulinkuoret, jotka ulottuvat kerroksina ulospäin juuresta. Jokainen kerros rakentaa aiemman kerroksen päälle lisää turvaa käyttäen hallintotyökaluja, digitaalisia allekirjoituksia, kryptauksia ja muita turvallisuusmenetelmiä. Kun ohjelmiston järjestelmät kehittyvät enemmän komplekseiksi, alkavat nämä rakenteet todennäköisemmin sisältämään enemmän virheitä koodissa. Tämän tuloksena mitä monimutkaisemmaksi ohjelmiston järjestelmä muuttuu, sitä vaikeampi tätä on suojella. Luottamuksen juuren tarkoitus on konseptina varmistaa, että suurin osa luottamuksesta annetaan järjestelmän vähiten monimutkaiselle osiolle ja täten myös vähiten haavoittuvaiselle osalle järjestelmää, jonka ympärille asetetaan monimutkainen järjestelmä, jotta tärkeimmät osat järjestelmää pysyy toiminnallisena. Turvallisuusarkkitehtuuri toistetaan eri koossa, ensin luodaan juuri laitteiston yksittäiselle järjestelmälle, tämän jälkeen laajennetaan juurta hallintojärjestelmän läpi korkeammalle järjestelmän tasolle ja viimeiseksi monen saman keskeisen ympyrän läpi.

Bitcoinin tietoturva arkkitehtuuri on erilainen. Bitcoinin yhteisymmärrysjärjestelmä, eli tämän hajautettu luonne, luo luottamuksesta julkisen tilikirjan, joka on

täysin hajautettu. Oikein validoitu lohkoketju käyttää genesislohkoa eli lohkoketjun ensimmäistä lohkoa luottamuksen juurena, josta luottamus jatkuu aina uusimpaan lohkoon. Bitcoin järjestelmä voi ja tulisi käyttää lohkoketjua luottamuksen juurenaan. Kun suunnitellaan monimutkaista bitcoin sovellusta, joka sisältää palvelun monella eri järjestelmällä, kehittäjän tulisi tarkasti tutkia turvallisuusarkkitehtuuria määritelläkseen mistä järjestelmän luottamus on peräisin.

Lopullisesti ainut kohde, johon tulisi luottaa täysin, on validoitu lohkoketju. Jos kehittäjän ohjelmisto suorasti tai epäsuorasti asettaa luottamusta ulkoistettuun järjestelmään, eli muuhun kuin hajautettuun lohkoketjuun, syntyy tästä huolenaihe koska tämä luo haavoittuvaisuuden järjestelmään. Hyvä keino arvioida sovelluksen tietoturva-arkkitehtuuria on tutkia yksittäistä osaa tästä, ja arvioida hypoteettinen tapahtuma, jossa tämä osa on kokonaan murrettu ja ulkopuolisen tekijän hallussa, että miten tämä tilanne vaikuttaa verkkoon kokonaisuutena. Kehittäjän tulee tutkia jokaista osaa sovelluksesta ja arvioida tämän osuutta kokonaisuudessaan osana koko järjestelmän turvallisuutta. Jos sovellus ei ole enää turvallinen, kun tämä yksi osa on murrettu, on järjestelmässä asetettu liikaa luottoa tähän yhteen osaan järjestelmää, ja järjestelmää tulisi hajauttaa, ettei järjestelmä pyöri yhden osan ympärillä. Bitcoin sovelluksen tulisi olla haavoittuvainen vain tämän järjestelmän yhteisymmärrysmekanismille, tarkoittaen että tämän luottamus on asetettu bitcoinin turvallisimpaan osioon. Vaikka keskitetyt ratkaisut olisivatkin asettaneet luottamusta pois hajautetusta järjestelmästä keskitettyyn järjestelmään, kuten yksityiselle palvelimelle. (Antonopoulos, 2015)

### 7.2 Käyttäjäturvallisuus

Meidän kokemuksemme digitaalisesta turvallisuudesta ovat alle viideltäkymmeneltä vuodelta. Modernit käyttöliittymät eivät ole turvallisia, eivätkä sovi säilömään digitaalista rahaa. Tietokoneet ovat jatkuvasti alttiita ulkoisille uhille, aina päällä olevan internetyhteyden takia. Tietokoneet pyörittävät tuhansia ohjelmistoja, joita käyttävät sadat käyttäjät, jotka usein myös omaavat pääsyn käyttäjän tiedostoihin.

Yksi haittaohjelma monien tietokoneelle asennettujen ohjelmien joukossa voi vaarantaa tietokoneen turvallisuuden ja varastaa bitcoinit, jotka ovat tallennettu lompakkosovelluksiin.

Huolimatta vuosikymmenien tutkimuksista tietoturvan kehityksen aloilta, digitaaliset omaisuudet ovat silti haavoittuvaisia uhille. Kaikkein korkeimmin vartioidut ja rajoitetut järjestelmät esimerkiksi talouspalveluissa, turvallisuuspalveluissa ja puolustusvarusteurakoitsijoilla, ollaan lopulta onnistuttu murtamaan. Bitcoin luo digitaalisen omaisuuden, koska tällä on olennainen arvo ja tämä arvo voidaan varastaa ja kääntää uusille omistajille välittömästi ja peruuttamattomasti. Tämä luo suuren virikkeen hakkereille. Tähän saakka hakkerin piti vaihtaa henkilöllisyystiedot, tilipoletit, luottokortit, pankkitilit ja muut vastaavat rahaksi sen murtamisen jälkeen eli niin sanotusti pestä rahat. Huolimatta rahanpesun vaikeudesta, on tämä silti nähty kasvavana ilmiönä. Bitcoin edistää tätä ongelmaa, sillä bitcoinia ei tarvitse välittää tai pestä koska rahan liikkuvuutta on vaikea tarkkailla. Bitcoinin arvo perustuu tämän digitaalisiin ominaisuuksiin, ja bitcoin on hyvin anonyymi valuuttana, jota verovirastojen on vaikea tarkkailla.

Bitcoin luo myös kannusteen kehittää tietoturvaa. Kun aikanaan tietokoneen murtamisen riskit eivät olleet suoria ja epämääräisiä, bitcoin tekee niistä selkeitä. Pitämällä bitcoineja tietokoneella käyttäjän tulee parantaa tietokoneen turvallisuutta jatkuvasti. Kryptovaluuttojen käytön lisääntymisen myötä näemme erilaisia uusia hakkerointitekniikoita ja turvallisuustekniikoiden käytön kasvavan. Hakkereilla on mehukkaita kohteita ja käyttäjillä on selvä peruste puolustaa itseään. (Antonopoulos, 2015)

### 7.2.1 Riskin tasapainottaminen

Useimmat käyttäjät ovat oikeutetusti huolestuneita riskeistä. Tiedostoja katoaa jatkuvasti mutta jos tiedostot sisältävät bitcoineja on rahallinen menetys paljon suurempi. Suojatakseen bitcoin lompakoitaan, käyttäjien tulee olla varovaisia, etteivät he mene liiallisuuksiin varastoimalla liikaa bitcoineja yhteen lompakkoon, vaan jakavat riskin useammalle eri lompakolle. Keinona estää bitcoin varkauksia, käyttäjät ottavat käyttöön todella monipuolisia kryptauskeinoja luodessaan varmuuskopioita.

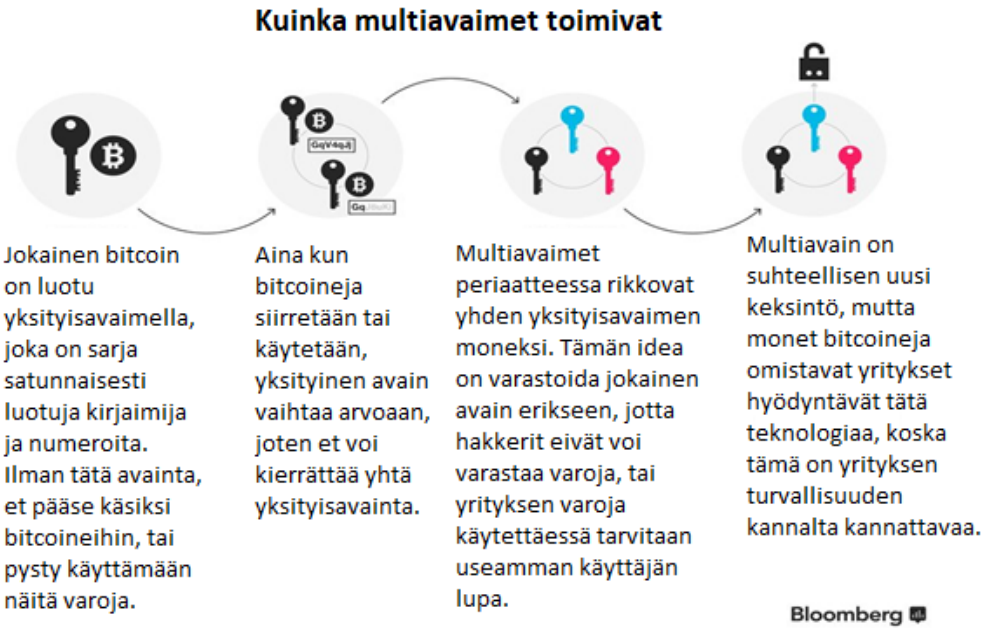
Lopulta he hävittivät kryptauksen purkuavaimet, joka teki varmuuskopioista turhia koska näitä ei voitu enää avata. Tätä voisi verrata kuin kätkisi rahaa hautaamalla ne aavikolle ja unohtamalla mihin ne kätkit.

Tuskin kukaan kantaa koko omaisuuttaan omassa lompakossa, ja samoin bitcoin käyttäjien tulisi jakaa bitcoinit usealle eri lompakolle. Silti käyttäjät tilastollisesti pitävät koko omaisuuttaan yhdellä lompakolla. (Antonopoulos, 2015)

### 7.2.2 Multiavaimet ja hallinto

Kun yritykset säilyttävät suuria määriä bitcoineja, tulisi heidän hyödyntää multiavainteknologiaa. Multiavainteknologia turvaa varoja vaatimalla useamman kuin yhden avaimen siirtoja luodessa. Kun tätä teknologiaa käytetään, tulisi avaimia säilöä useassa eri kohteissa ja eri henkilöiden hallussa. Yritysympäristössä tulisi bitcoinien olla aina useamman henkilön vastuulla, jotta yksittäinen henkilö ei voi hyödyntää varoja.

Bitcoin sisältää myös riskin, käyttäjän kuolema tai muut toimintakykyyn vaikuttavat sairaudet saattavat lukita bitcoinit lompakkoon. Tilanteessa, jossa esimerkiksi lompakon haltija kuolee, omaisen perhe ei välttämättä edes tiedä bitcoin varojen olemassaolosta, tai jos he ovat tästä tietoisia, he eivät yleisesti tiedä bitcoinien avaimien tietoja. Näitä tilanteita tulee ennaltaehkäistä antamalla avaimien avaustiedot perheen tai yrityksen asianajajalle. Kuvassa 11. selkeytämme multiavaimien toimintaa ja käyttötarkoitusta. (Antonopoulos, 2015)




Kuva 11. Havainnollistava kuva, kuinka multiavaimet toimivat ja luovat lisää tietoturvaa yrityksissä.

(Bloomberg News August 15, 2016)

# 8 BITCOINIIN POHJAUTUVAT MUUT VALUUTAT JA TOIMINNOT

Bitcoin on kahdenkymmenen vuoden kehityksen ja tutkimuksen tulos, joka loi mullistavaa uutta teknologiaa, kuten hajautettu yhteisymmärrysmekaniikka, joka pohjautuu louhinnan työtodistuksiin. Tämä keksintö on osa bitcoinin ydintoimintaa ja luo aallon innovaatioille valuuttojen, talouden ekonomian ja sopimusten alalta. Uusia kryptovaluuttoja on jo luotu useita kymmeniä. Nämä ovat saaneet alkunsa bitcoinin käyttäjien toimista. (Antonopoulos, 2015)

## 8.1 Vaihtoehtoisten valuuttojen ja ketjujen luokittelu

Bitcoin perustuu avoimeen lähdekoodiin ja tätä koodia on hyödynnetty pohjaratkaisuna myös monille muille ohjelmistoprojekteille. Yleisin muoto, jota bitcoinin pohjalta on luotu, ovat muut hajautetut valuutat, jotka hyödyntävät samaa lohkoketjuteknologiaa kehittääkseen kryptovaluuttojaan.

On monia muita protokollatasoja, jotka on kehitetty bitcoinin lohkoketjun ympärille. Nämä niin sanotut ”metakolikot”, ”metaketjut” ja lohkoketjuohjelmistot käyttävät lohkoketjuteknologiaa ohjelmiston perustana ja laajentavat nykyistä bitcoinin protokollaa. Esimerkkejä tästä ovat Väritetyt kolikot, Mastercoin ja Counterparty. Tunnetuimmat vaihtoehdot bitcoinille ovat esimerkiksi Litecoin, Dogecoin, Freicoin, Primecoin, Peercoin, Darkcoin ja Zerocoin.

Vaihtoehtovaluutan lisäksi on olemassa monia muita lohkoketju implementaatioita, jotka eivät ole ”kolikoita”, joita kutsutaan aliketjuiksi. Nämä aliketjut ovat omia lohkoketjuja ja käyttävät yhteisymmärrysalgoritmia ja julkista tilikirjaa pohjana sopimuksille, nimirekisteröinnille tai muille ohjelmistoille. Aliketjut käyttävät samaa perustaa lohkojen rakenteille ja saattavat myös käyttää valuuttoja tai tokeneita maksumekanismeina, mutta näiden tarkoitus ei ole olla valuuttoja. Näihin voidaan luetella tunnettuja ratkaisuja kuten Namecoin, Ethereum ja NXT. (Antonopoulos, 2015)

## 8.2 Metakolikoiden ohjelmistoalustat

Metakolikot ja metaketjut ovat ohjelmistokerroksia, jotka on kehitetty bitcoinin rakenteesta, joko kehittämällä valuutan toisen valuutan sisälle tai ohjelmistoalusta protokollana, joka toimii bitcoinjärjestelmän ulkopuolella. Nämä toimintokerrokset laajentavat bitcoinin ydinprotokollaa ja lisäävät ominaisuuksia ja joustavuutta lisäämällä tietoa bitcoin transaktioihin ja bitcoindataan sekä osoitteisiin. (Antonopoulos, 2015)

### 8.2.1 Väritetyt kolikot

Väritetyt kolikot ovat metaprotokolla, jotka lisäävät pieniä uusia ominaisuuksia kryptovaluutoille. ”Väritetyt” kolikot ovat kryptovaluuttaa, jotka on uudelleenmääritetty edustamaan toista arvoa lisäämällä uusia tietoja jokaiselle kolikolle. Kuvitellaan esimerkkinä, jos voisimme lisätä viiden euron seteliin postimerkin, jossa lukee ”tämä on todistus yhden osakkeen omistuksesta Santeri osakeyhtiössä.”. Nyt tämä euroseteli omistaa kaksi tarkoitusta: se on valuutta ja myös todiste osakeomistuksesta. Nyt seteli on myös osake ja käyttäjä ei halua käyttää tätä enää ostotarkoituksiin koska se on arvokkaampi osakkeena. Väritetyt kolikot toimivat juuri näin lisäämällä bitcoineihin tunnisteita, jotta nämä toimivat osakkeina. Tämä toiminto selittää termin väritetyt kolikot. Palvelu ”värittää” valuutalle uusia attribuutteja. Käyttäjä voi itse värittää bitcoininsa itselleen parhaisiin käyttötarkoituksiin, lisäämällä kolikoihin metadataa. Bitcoinien väritys voidaan myös poistaa, tulostamalla lisätty arvo pois kolikosta. (Antonopoulos, 2015)

### 8.2.2 Mastercoin

Mastercoin on protokolla, joka on johdatettu bitcoin ratkaisusta. Mastercoin käyttää valuuttanaan Mastercoin tokeneja, joilla suoritetaan Mastercoin transaktioita. Mutta Mastercoin ei ole pohjimmiltaan käytössä valuuttana. Mastercoin on enemmänkin ratkaisu, josta voidaan rakentaa muita käyttäjävaluuttoja, pieniä omaisuustokeneita, hajautettujen valuuttojen muuttokursseja sekä sopimuksia. Mastercoin on ohjelmistokerrosprotokolla, joka toimii bitcoinin rahallisessa transaktiossa siirtokerroksena, aivan kuten http toimii TCP:n päällä.

Mastercoin operoi pääasiallisesti transaktioiden kautta, jotka lähetetään ja vastaanotetaan bitcoinosoitteista, joita kutsutaan ”exodus-osoitteiksi”. Aivan kuten HTTP hyödyntää tiettyä TCP-porttia (port 80) erotellakseen liikennettä muusta TCP liikenteestä. (Antonopoulos, 2015)

### 8.3 Vaihtoehtoiset kolikot

Suurin osa vaihtoehtoisista kolikoista eli alt-coineista ovat alkujaan bitcoinin lähdekoodia, jotka tunnetaan koodin haarautumina. Vaihtoehtoiset kolikot ja vaihtoehtoiset ketjut eli alt-chainit ovat molemmat erillisiä bitcoinista kehitettyjä ratkaisuja, jotka soveltavat bitcoinin lohkoketjuteknologiaa ja molemmat käyttävät omaa lohkoketjuaan. Ero vaihtoehtoisten kolikoiden ja lohkojen välillä on, että kolikoita käytetään valuuttoina, kun taas ali ketjuja käytetään muihin tarkoituksiin mutta ei pääasiallisesti valuuttoina.

Esimerkkinä alt-coineista on litecoin, joka käyttää ”scrypt:iä” työtodistusalgoritminaan, mutta myös implementoi nopeamman lohkojen generointiajan, joka tähtää bitcoinien luonnin tapahtuvan 2.5 minuutin välein eikä bitcoinin 10 minuutin välein. Tämän tuloksena syntyi niin sanottu hopea bitcoinin kullalle, ja litecoinin tarkoitus on toimia pienempänä ja arvottomampana valuuttana bitcoinin rinnalla. Monet uskovat Litecoinin olevan järkevämpi ratkaisu realistiseen arkikäyttöön kuin bitcoin, jonka nykyiset arvot ovat huipussaan useita tuhansia euroja.

Alt-coinit jatkoivat oman paikkansa etsintää 2011 ja 2012 välillä, joko pohjautuen bitcoiniin tai litecoiniin. 2013 alussa oli jo 20 alt-coinia, jotka kilpailivat markkinoista. 2013 vuoden lopussa niitä oli jo 200.

Alt-coinin luominen on helppoa, ja tämän takia nykypäivänä näitä on jo yli 500. Useimmat alt-coinit poikkeavat todella vähän bitcoinista tai eivät tarjoa mitään erilaisia ominaisuuksia. Monet näistä ovat itseasiassa pyramidihuijauksia. Näiden kopioiden ja pyramidihuijausten joukossa on myös poikkeuksia ja loistavia innovaatioita bitcoinin toimintamalliin. On kolme kategoriaa, miten alt-coinit poikkeavat bitcoinista:

- Erilaiset rahakäytännöt

- Erilaiset työtodistukset ja ratkaisut luoda luottamusta käyttäjien välillä
- Tietyt ominaisuudet kuten vahva anonymiteetti

(Antonopoulos, 2015)

# 9 TUTKIMUKSEN TULOKSET

Lohkoketjuteknologia on hajautetussa ympäristössä toimiva tietokanta, jota ylläpitävät toisilleen tuntemattomat toimijat. Tieto syötetään lohkoihin, jotka referoivat aina aiempaa lohkoa tiivisteen avulla. Lohkoketjuteknologiaa käytetään muissakin kryptovaluutoissa ja lohkoketju järjestelmissä kuin bitcoinissa. Lohkoketjuteknologiaa voidaan käyttää hyvin laajasti, esimerkiksi järjestelmissä, joissa varastoidaan tietoa.

Bitcoinin turvallisuuden peruste on sen hajautettu luonne, joka siirtää vastuun käyttäjille. Se ei vaadi kolmannen osapuolen hallintaa, jotta se pysyisi turvallisena. Bitcoin tietoverkon turvallisuus perustuu louhijoiden työtodistuksiin eikä verkoston hallintaan. Kaikki bitcoin siirrot ovat julkisia, mutta siirron tekijät ja vastaanottajat pysyvät anonyymeinä.

Bitcoin oli seuraus Lehman Brothersin hakeutumisesta yrityssaneeraukseen vuonna 2008. Tämän seurauksena haluttiin valuutta, jota voidaan itse hallita. Bitcoinin idea oli olla käyttäjien valvoma valuutta, jonka siirrot tapahtuisivat välittömästi. Valuutan käyttäjän ei tarvitsisi luottaa pankkiin, joka säilyttäisi valuuttaa käyttäjän puolesta ja hallitsisi sitä.

Bitcoin on ensimmäinen kryptovaluutta mutta emme usko valtioiden ottavan tätä viralliseen käyttöön. Bitcoin on suunnannäyttäjä siihen, mihin suuntaan pankkipalvelut menevät. Tulevaisuudessa uskomme, että valuutta on käyttäjien hallussa ja he voivat käyttää sitä, ilman kolmansia osapuolia. Tähän kyllä menee aikaa ennen kuin tämä skenaario toteutuu. Uskomme että ensimmäinen virallinen kryptovaluutta ei ole yhden käyttäjän luoma, vaan valtion keksimä virallinen valuutta, joka tulee hyödyntämään lohkoketjuteknologiaa. Bitcoinin arvo ominaisuus ei ole valuutta, vaan innovoiva ja joustava lohkoketjuteknologia.

Opinnäytetyömme tarkoituksena oli pohtia bitcoinia ja lohkoketjuteknologiaa osana tulevaisuuden valuuttoja. Tutkimuksemme perusteella voimme todeta, että bitcoin ei välttämättä ole juuri yksi ja oikea kryptovaluutta. Uskomme, että yksikään maailman valtio ei ole valmis antamaan bitcoinille täysiä valuutan oikeuksia,

koska yhdelläkään valtiolla ei ole valtuuksia valvoa ja ylläpitää tämän valuutan arvoa ja käytettävyyttä. Bitcoinia ei käytetä missään valtiossa virallisena valuuttana ja tuskin tätä tullaan koskaan edes tekemään, sen arvaamattoman ja hajautetun teknologian vuoksi.

Lohkoketjuteknologia, jota bitcoin ja muut kryptovaluutat hyödyntävät on tulevaisuuden teknologiaa innovoiva ja mullistava keksintö, joka varmasti löytää roolinsa tulevaisuuden valuutoissa ja kaupankäynnissä. Lohkoketju toimii hyvänä pohjana mahdollisille teknologioille, joissa tarvitaan hajautettua ja julkista tilikirjaa.

Uskomme, että tulevaisuudessa jos kryptovaluutat saavat kansainvälistä valtioiden virallista tunnustusta, tulee tämä kryptovaluutta olemaan valtioiden tai keskuspankin kehittämä oma kryptovaluuttansa. Uskomme myös, että tämä virallinen valuutta tulee hyödyntämään lohkoketjuteknologiaa tämän kehityskaaressa ja implementoinnissa.

Bitcoin-verkko on tutkimuksiemme mukaan turvallinen, mutta tämän ympärille ei ole vielä rakennettu tarpeeksi juridista pohjaa ja turvaa. Bitcoin tarvitsee lisää lakirakenteita ympärilleen, jotta tämä olisi turvallinen käyttäjille. Bitcoinin verotus ja tämän käyttö rikoksissa, kuten pimeillä markkinoilla ja rahanpesussa on vaikea valvoa. Bitcoinin ideana on käyttäjän anonymiteetti ja byrokratian välttely. Emme usko, että bitcoinin kehittäjät olisivat valmiita luopumaan näistä arvoistaan. Bitcoin on kuitenkin avointa lähdekoodia, eli jos joku valtio haluaa hyödyntää tätä teknologiaa, on tästä helppo luoda mahdollinen valtioiden välinen virallinen valuutta.

# LÄHTEET


Antonopoulos, A.M. 2015. Mastering Bitcoin: Unlocking Digital Crypto-curriencies. O'Reilly Media Inc. Sebastopol.

Bitcoin Wiki, FAQ

https://bitcoin.org/en/faq Viitattu 11.1.2019

Bitcoin Mining

https://www.bitcoinmining.com/ Viitattu 11.1.2019

Bitcoin Wiki, Satoshi Unit

https://en.bitcoin.it/wiki/Satoshi_(unit) Viitattu 11.1.2019

Bitcoin Wiki, Why do bitcoins have value

https://bitcoin.org/en/faq#why-do-bitcoins-have-value Viitattu 11.1.2019

Blockonomi, Best bitcoin wallets 2019: Hardware vs Software vs Paper https://blockonomi.com/best-bitcoin-wallets/ Viitattu 20.2.2019

Blog Trezor Learn about: Recovery seed https://blog.trezor.io/learn-about-trezor-recovery-seed-offline-backup-fe235873c69f Viitattu 9.3.2019

CryptoCompare How do digital signatures in Bitcoin work?

https://www.cryptocompare.com/wallets/guides/how-do-digital-signatu-res-in-bitcoin-work/ Viitattu 30.1.2019

Fiorillo, 2018, Bitcoin History: Timeline, Origins and Founder

https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578

Viitattu 11.1.2019

Franco, P. 2014, Understanding Bitcoin: Cryptography, Engineering and Econimics. John Wiley & Sons, inc

Gupta, M. 2018, Blockchain for dummies. John Wiley & Sons, inc

Hill, B. Chopra, S. Valencourt, P. Prusty, N. 2018 Blockchain Developer's Guide. Packt Publishing

Laurence, T. 2017, Blockchain for dummies. John Wiley & Sons, inc

Lipovyanov, P. 2019 Blockchain for Business 2019. Pact Publishing

Tivi. Bitcoineja on kateissa jopa 30 miljardin euron edestä – ei saada ikinä takaisin

https://www.tivi.fi/Kaikki_uutiset/bitcoineja-on-kateissa-jopa-30-miljardin-euron-edesta-ei-saada-ikina-takaisin-6689333 viitattu 30.1.20.2019