Open your mind. LUT.
Lappeenranta University of Technology

TUOTANTOTALOUDEN KOULUTUSOHJELMA

Lohkoketjuteknologian käyttö yritysten tietoturvan parantamiseksi

Using blockchain technology to improve information security of businesses

Kandidaatintyö

Aleksi Toivanen

Erno Sjöblom

TIIVISTELMÄ

Tekijä: Aleksi Toivanen ja Erno Sjöblom

Työn nimi: Lohkoketjuteknologian käyttö yritysten tietoturvan parantamiseksi

Vuosi: 2018 **Paikka: Lappeenranta**

Kandidaatintyö. Lappeenrannan teknillinen yliopisto, tuotantotalous.
42 sivua, 4 kuvaa, 4 taulukkoa ja 4 liitettä
Tarkastaja(t): Apulaisprofessori Lea Hannola

Hakusanat: Lohkoketjuteknologia, Tietoturva, Hajautetut järjestelmät, Tiedon varastointi
Keywords: Blockchain, Information security, Decentralized systems, Data storing

Tämä työ on toteutettu kirjallisuuskatsauksena ja sen tavoitteena on selvittää, miten lohkoketjuteknologian avulla voidaan parantaa yritysten tietoturvaa. Työ käsittelee erityisesti tietoturvan merkitystä yrityksen liiketoiminnalle ja tietoturvan peruselementtejä liittyen tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Lisäksi käsitellään lohkoketjuteknologiaa ja tutkitaan sen potentiaalia parantaa yritysten edellä mainittujen tietoturvan peruselementtien nykyistä tilaa. Kandidaatintyö ei ole rajattu erikseen tietyntyyppisille yrityksille, vaan sen on tarkoitus antaa kattava näkemys lohkoketjuteknologian soveltuvuudesta erityyppistä tietoa käsittelevien yritysten tietoturvan tueksi.

Työssä huomattiin lohkoketjuteknologialla olevan huomattavaa potentiaalia yrityksen erityyppisen tiedon tietoturvallisessa varastoimisessa ja sen soveltuvuudessa manuaalisten tietoturvajärjestelmien tietokannaksi mm. hajautetun arkkitehtuurin ja ketjumaisen tiedon varastoinnin avulla. Lohkoketjuteknologian sovellukset ovat kuitenkin vielä varsin uusia ja kehittyvässä vaiheessa, jonka takia yritysten voi vielä olla vaikeaa hyödyntää teknologiaa tiedonvarastointiin tehokkaasti.

SISÄLLYSLUETTELO

1 Johdanto 1

1.1 Työn motiivi 1

1.2 Työn tavoitteet ja tutkimuskysymykset 1

1.3 Työn rakenne ja rajaukset 2

1.4 Työhön liittyvää sanastoa 2

2 Tietoturva 5

2.1 Tietoturvan merkitys 5

2.2 Tietoturvan CIA-malli 6

2.3 Tietotyyppien tietoturvaluokitukset 8

2.4 Keskeiset tietoturvaongelmat 10

2.5 Tietoturva kolmannen osapuolen pilvipalveluissa 13

2.6 Tietoturva osana yrityksen taloutta 15

2.7 Tietoturvan toteuttaminen 18

3 Lohkoketjuteknologia 21

3.1 Lohkoketjuteknologian perusteet 21

3.2 Lohkoketjuteknologian toiminta Bitcoinin avulla 24

3.3 Lohkoketjuteknologian jatkokehitys 26

4 Lohkoketjuteknologia tietoturvassa 29

4.1 Lohkoketjuteknologia perinteisten tietojärjestelmien rinnalla 29

4.2 Lohkoketjuteknologian CIA-ominaisuudet 30

4.3 Skaalautuvuus lohkoketjun tiedonvarastoinnissa 32

4.4 Taloudelliset tekijät lohkoketjuteknologian tietoturvajärjestelmässä 33

4.5 Lohkoketjuteknologian tietoturvajärjestelmät 34

4.6 Lohkoketjuteknologian soveltuvuus yritysten tietoturvaan 36

5 Johtopäätökset 39

6 Lähteet 43

Liitteet

1 JOHDANTO

1.1 Työn motiivi

Nykypäivänä yritysten erilaiset prosessit tuottavat massiivisesti erityyppistä tietoa, jonka säilöminen on yhä kannattavampaa. Esimerkiksi suuret kauppaketjut kuten Walmart joutuvat käsittelemään tuhansia teratavuja tietoa (Rainer & Prince 2016, s. 124). Tämän tiedon avulla puolestaan tehdään tärkeitä päätöksiä ja monet tietokoneavusteiset toiminnot hyödyntävät tätä tietoa, jonka takia sen tietoturva on yhä tärkeämpää (Gaetani et al. 2017). Lisäksi yhteiskunnan suuri riippuvuus teknologiasta ja internetistä luo alati uusia liiketoimintamalleja, joka puolestaan lisää houkuttelevuutta erilaisille kyberhyökkäyksille (Piscini et. al. 2017, s. 4). Ulkopuolisten uhkien lisäksi liittyy tiedon varastoimiseen sisäisiä haasteita sen saatavuuden, eheyden ja luottamuksellisuuden ylläpitämisessä.

Lisääntynyt tarve tiedon varastoinnille on tuonut myös mukanaan vaihtoehtoisia tapoja varastoida tietoa. Yksi näistä vaihtoehtoisista tavoista on tiedon varastointi lohkoketjuteknologian avulla. Lohkoketjuteknologiaa on tähän asti pitkälti käytetty erilaisten kryptovaluuttojen luomiseen, mutta sen potentiaalia tiedon varastoinnissa ollaan alettu huomioida yhä enemmän. Teknologian ominaisuuksien avulla voi olla mahdollista parantaa yritysten tietoturvaa parantamalla tiedon saatavuutta, eheyttä ja luottamuksellisuutta. Lisäksi lohkoketjuteknologia tarjoaa mahdollisuuden suunnitella vakaampia elegantisti sulautettuja internetpohjaisia tietoturvajärjestelmiä, joihin tunnistautuminen on joustavampaa ja nopeampaa (Swan 2015, s. 15).

1.2 Työn tavoitteet ja tutkimuskysymykset

Työn tavoitteena on tarkastella lohkoketjuteknologiaan perustuvan tiedonvarastoinnin tietoturvaominaisuuksia ja tarkastella sen sopivuutta yritysten tietoturvan parantamiseksi mm. tietoturvallisempana vaihtoehtona varastoida tietoa sekä parempana alustana manuaalisten tietoturvajärjestelmien toiminnassa. Lisäksi tavoitteena on määritellä, minkä tyyppisen tiedon varastointi lohkoketjuun on kannattavaa. Tavoitteena on myös selvittää, miten lohkoketjuteknologiaa käyttämällä saavutettu tietoturvan lisäys voisi parantaa yrityksen kannattavuutta. Työn keskeiset tutkimuskysymykset ovat:

1. Millä tavoin lohkoketjuteknologian avulla voidaan parantaa yritysten tietoturvaa?
2. Minkä tyyppisen tiedon varastointi lohkoketjuun on kannattavaa?
3. Miten lohkoketjuteknologian käytöstä saavutettu tietoturvan lisäys parantaa yrityksen kannattavuutta?

Työn vastatessa näihin kysymyksiin, saa lukija laajan käsityksen yritysten tämänhetkisistä tietoturvaongelmista ja niiden korjaamisesta lohkoketjuteknologian avulla. Lukija saa myös käsityksen teknologian käytettävyyden kannattavuudesta tiedonvarastointiin nykypäivänä.

1.3 Työn rakenne ja rajaukset

Työn alussa on määritelty muutamia termejä, jotka helpottavat lukijaa työn ymmärtämisessä. Tämän jälkeen luodaan katsaus tietoturvaan, jossa käsitellään sen merkitystä yrityksille ja siihen liittyviä yleisiä käsitteitä ja ongelmia. Keskeisiä aiheita ovat mm. tietoturvan CIA-malli, eri tietotyyppien vaatimat CIA-ominaisuudet, keskeiset uhat tiedon CIA-ominaisuuksille ja tietoturvan taloudelliset vaikutteet. Kolmannessa osiossa esitellään lohkoketjuteknologian perusperiaatteet ja sille kehittyneet käyttötarkoitukset. Toiminnan havainnollistamista varten osiossa luodaan myös katsaus kryptovaluutta Bitcoinin toimintaan. Neljännessä luvussa yhdistetään tietoturvassa käsitellyt aiheet ja lohkoketjuteknologian toiminta tarkasteltaessa miten lohkoketjuteknologian avulla voidaan parantaa yrityksen tietoturvaa. Luvussa käsitellään mm. lohkoketjuteknologiaa perinteisten tietojärjestelmien rinnalla, lohkoketjuteknologian CIA-ominaisuuksia, skaalautuvuutta ja soveltuvuutta yritysten tietoturvaa ylläpitäviin esineiden internet -järjestelmiin. Viimeinen luku sisältää johtopäätöksiä ja mahdollisia jatkotutkimuskohteita lohkoketjuteknologiaan liittyen.

1.4 Työhön liittyvää sanastoa

Ymmärtääkseen tietoturvan toimintaa, täytyy lukijan sisäistää muutamia peruskäsitteitä ja määritelmiä, liittyen tietoturvaan, tietojärjestelmiin, tiedonvarastointiin ja lohkoketjuteknologiaan. Tässä kappaleessa käydään läpi kandidaatintyössä esiintyviä termejä näihin asioihin liittyen.

Tietotyyppi

Määritelty kategoria tiedolle sen ominaisuuksien mukaan (esim. salattu, lääketieteellinen, rahoitus, tutkiva jne.). Nämä tietotyypit yleensä määritellään organisaation toimesta tai joissain tapauksissa ne on lailla määrätty. (National Institute of Standards and Technology 2004, s. 7)

Tietomurto

Tapahtuma, jolloin jokin organisaation hallinnoiman tiedon tietoturvaominaisuuksista vaarantuu syystä tai toisesta. Näihin tietoturvaominaisuuksiin kuuluu tiedon saatavuus, eheys ja luottamuksellisuus. (Nayak & Rao 2014, s. 82)

Hashaus

Matemaattisen kaavan käyttö tietyn tiedon muuttamiseksi salattuun muotoon. Nämä muutokset toteutetaan käyttämällä erilaisia hashaus funktioita tai algoritmeja. Tämä salaus voidaan sen jälkeen purkaa toisella salaukselle määritellyllä algoritmilla. (Nayak & Rao 2014, s. 165)

Hajautettu ja keskitetty verkosto

Verkostojen tyypit voidaan määritellä niiden osallistujien vuorovaikutuksilla toisiinsa. Keskitetyssä verkostossa jokainen vuorovaikutus eri osallistujien välillä kulkee yhden keskitetyn osallistujan kautta. Hajautettu verkosto on kokoelma yksittäisiä osallistujia, jotka työskentelevät yhdessä muodostaakseen toimivan järjestelmän. Hajautetussa verkostossa ei ole vain yhtä osallistujaa, jonka kautta kaikki vuorovaikutteet kulkevat. (Tanenbaum & Van Steen 2007, s. 2, 36-42)

Julkinen ja yksityinen avain

Julkinen ja yksityinen avain –tekniikka käyttää tiedon salaamiseen avainpareja. Julkisen avaimen avulla kuka vain pystyy salaamaan tietyn tiedon ja lähettämään sen salattuna eteenpäin. Tämä salattu tieto voidaan purkaa julkisen avaimen yksityisellä avainparilla. (Nayak & Rao 2014, s. 168) Bitcoinin lohkoketju käyttää julkista ja yksityistä avainta mm. transaktioiden suorittamiseen (Swan 2015, s. 98)

P2p-transaktiot

P2p-transaktioilla tarkoitetaan transaktioita, joissa molemmat transaktioon osallistuvat toimivat ikään kuin asiakkaina ja servereinä. Tämä tarkoittaa, että kukin osapuoli pystyy tarkastelemaan toisen osallistujan tietoja transaktiossa ja jakamaan omia tietojaan transaktioon osallistuville. (Rainer & Prince 2016, s. 171) Yleensä julkiset lohkoketjut, kuten Bitcoin, toimivat näiden p2p-transaktioiden avulla (Nakamoto 2008).

Bysanttilaisten kenraalien ongelma

Bysanttilaisten kenraalien ongelma on järjestelmän toimintaan liitettävä ongelma. Järjestelmä saattaa toimia väärin, mikäli jotkin sen osista toimivat väärin ja lähettävät väärää tieto muille järjestelmän osille. Ongelman nimi kumpuaa tilanteesta, jossa Bysanttilaiset kenraalit pystyvät kommunikoimaan omia havaintojaan ainoastaan lähetin avulla, jolloin on vaikea varmistaa antaako jokin kenraali tahallisesti väärää tietoa. Yhtä lailla myös tietynlaisissa järjestelmissä voi olla hyvin vaikeaa päätellä mitkä osista tuottavat oikeaa tietoa, ja mitkä puolestaan väärää tietoa (Lamport, Shostak & Pease 1982).

Relaatiotietokanta

Relaatiotietokanta tarkoittaa taulukoitua tiedonvarastointia, jota hallinnoidaan sille ominaisella tietokannan hallintajärjestelmällä. Tietokannassa on monta taulukkoa ja nämä taulukot koostuvat järjestelmällisesti erinäisistä arvoista. Relaatiotietokanta on suosittu tietokantamalli, sillä niitä on helppo käyttää ja ne ovat järjestelmällisiä (Rainer & Prince 2016, s.129)

Esineiden internet

Esineiden internet (The Internet of Things) tarkoittaa järjestelmiä, joissa tekninen laite lähettää tietoa siihen liitettyyn tietojärjestelmään ilman ihmisen interaktiota. Toimiakseen esineiden internet vaatii hyvin toteutettuja ratkaisuja mm. langattomassa teknologiassa ja nopeassa ja laadukkaassa tietovarastoinnissa. (Rainer & Prince 2016, s. 251)

2 TIETOTURVA

Nykypäiväinen tiedon kriittisyys yritysten prosesseissa asettaa sen alttiiksi ulkopuolisten kiinnostukselle ja muille tietoturvariskeille. Myös teknologian kehittyminen, internetpohjaisten toimintamallien yleistyminen, tarvittavan tuen kasvu ja rikollisjärjestöjen kiinnostuksen suuntautuminen tietomurtoihin lisäävät yritysten tietoturvan haavoittuvaisuutta. (Prince & Rainer. 2016, s. 88-89) Osiossa perehdytään tietoturvaan yritysten liiketoiminnan tukena, tietoturvan perusteisiin, ongelmiin ja toteuttamiseen yrityksissä.

2.1 Tietoturvan merkitys

Tietoturva viittaa kaikkiin prosesseihin ja käytäntöihin, jotka on tarkoitettu suojaamaan yrityksen tai organisaation tietoja ja tietojärjestelmiä. Tiedon haavoittuvuudella tarkoitetaan sen mahdollisuutta altistua erilaisille uhille. (Rainer & Prince 2016, s. 88-89) Yrityksen kannalta tietoturva toimii apuvälineenä kaikelle, mitä yrityksessä tehdään. Yleisesti sillä ei tuoda lisäarvoa yritykseen, vaan sen tehtävä on suojata sitä, mikä tuottaa lisäarvoa. Yrityksen sisällä tietoturvalla on neljä tärkeää tehtävää täytettävänä:

1. Suojata organisaation kykyä toimia ja suorittaa liiketoimintaa
2. Mahdollistaa turvallisen tietojen käsittelyn yrityksen sisäisessä verkossa
3. Turvata kaikkea tietoa yrityksessä, mitä kerätään ja käytetään
4. Suojata yrityksen teknologista omaisuutta

(Whitman & Mattord 2012, s. 41)

Yrityksen puutteellinen kyky noudattaa ja implementoida sopivia tietoturvan säännöksiä johtaa useimmiten sen puutteelliseen kykyyn myös toteuttaa omaa missiotaan. Tämän takia on kriittistä ymmärtää, miten jokainen tietoturvajärjestelmä tukee yrityksen mission toteutusta. Yksityisen ja julkisen sektorin organisaatiot parantavat tuottoaan ja palvelun tasoaan asiakkaille, kun ne noudattavat oikeanlaisia tietoturvamenetelmiä. Nykypäivän erilaisten tietoturvariskien, kuten haitallisten koodien, ulkoisten tietomurtojen, sisäisten uhkien ja julkaistujen tietoturvaongelmien myötä yritykselle voi koitua vakavia taloudellisia ja imagollisia tappioita, mikäli se ei kykene ylläpitämään tietoturvaansa. (Nieles et al. 2017, s. 7)

Yhtenä esimerkkinä tietoturvan tärkeydestä yrityksen toiminnalle voidaan pitää vuonna 2011 tapahtunutta ulkoista tietomurtoa peliyhtiö Sonyn tietojärjestelmään. Tällöin ulkopuoliset

hakkerit murtautuivat Sonyn PlayStation-verkoston tietojärjestelmään ja noin 77 miljoonan PlayStation-käyttäjätilin sähköposteja, käyttäjänimiä, salasanoja, turvakysymyksiä ja muita tietoja päätyi heidän käsiinsä. Tästä syystä Sony joutui sulkemaan PlayStation-verkoston noin viikon ajaksi. (Quinn & Arthur 2011) Sony julkaisi myöhemmin tästä asiasta tiedotteen, jonka mukaan sille koituneet kustannukset tästä tietomurrosta olivat noin 170 miljoonaa dollaria. On kuitenkin hyvin vaikea arvioida tietomurrosta koituneet todelliset kustannukset mm. asiakassuhteissa ja imagossa. (Tassi 2011)

Tietoturvaa mietittäessä tulee myös ajatella keskeisesti riskienhallintaa. Yrityksen tulee arvioida erilaiset tietoturvariskit ja niiden realisoitumisen vaikutukset. Esimerkiksi nopeasti kehittyvillä aloilla on hyvinkin perusteltua pyrkiä suojaamaan tuotekehitykseen liittyvä tieto mahdollisimman hyvin, sillä sen vuotaminen kilpaileville yrityksille voisi haitata liiketoimintaa merkittävästi. (Nayak & Rao 2014, s. 5-6)

2.2 Tietoturvan CIA-malli

Yhdysvaltain kansallinen standardien ja teknologian instituutti määrittelee tietoturvan suojana, jota on varaa ylläpitää automaattisen tietojärjestelmän tietojen saatavuuden, eheyden ja luottamuksellisuuden turvaamiseksi. Tähän sisältyy laitteisto, ohjelmisto, tieto ja yhteydet (National Institute of Standards and Technology 1995, s. 5). Tätä tietoturvan kolmesta pääasiallisesta tehtävästä koostuvaa mallia kutsutaan CIA-malliksi, joka tulee sanoista luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). (Nayak & Rao 2014, s. 29)

Tiedon luottamuksellisuudella pyritään pitämään tiedon saatavuus poissa luvattomilta tahoilta (National Institute of Standards and Technology 1995, s. 7). Tiedon luottamuksellisuuden ylläpitäminen voi olla erityisen tärkeää silloin, kun tietojen päätyminen ulkopuolisten käsiin saattaisi aiheuttaa yritykselle merkittävää haittaa. Tieto voi levitä ulkopuolisten käsiin joko ulkoisen tietomurron, sisäpiiritekijän tai yksinkertaisen virheen takia. (Nayak & Rao 2014, s. 52) Tiedon luottamuksellisuus on vaarantunut, kun sitä päätyy luvattomasti ulkopuolisten saataville (National Institute of Standards and Technology 2004, s. 2) Olipa syy mikä tahansa, se ei kuitenkaan muuta tietojen päätymistä ei halutulle taholle. Esimerkiksi Sonyn PlayStation-

verkoston tietomurto vahingoitti sen asiakkaiden tietojen luottamuksellisuutta tietojen päätyessä ulkopuolisten käsiin.

Tiedon eheydellä tarkoitetaan tiedon ajoitettua, tarkkaa, täydennettyä ja ristiriidatonta dokumentointia. Eheys voidaan jakaa kahteen eri aliluokkaan: tiedon eheyteen ja järjestelmän eheyteen. (National Institute of Standards and Technology 1995, s. 5-6) Tiedon eheys viittaa tiedon muuttamisen tietokannassa oikeaoppisilla tavoilla ja se käsittää varastoidun tiedon, prosessoitavan tiedon ja siirtymävaiheessa olevan tiedon. Järjestelmän eheys viittaa järjestelmän kykyyn toimia vapaasti oikealla tavalla käsitellessään sen tietokannan tietoja ilman ulkopuolisten tahojen tahallista tai tahatonta manipulointia. (Nieles, K. et al. 2017, s. 3) Tiedon eheys voidaan myös määritellä suojana epäasiallista muokkausta tai tuhoamista vastaan ja tietojen oikeellisuuden varmistuksella (Nayak & Rao 2014, s. 52). Tiedon eheys on vaarantunut, kun tietoja päästään muokkaamaan tai tuhoamaan luvatta (National Institute of Standards and Technology 2004, s. 2).

Hajautetuissa järjestelmissä tiedon eheys voi olla hyvin tärkeä kriteeri, jottei osa järjestelmästä toimi eri tietojen perusteella kuin toinen. Tiedon eheys voi myös olla keskeisessä asemassa, kun tieto on hajautettu eri paikkoihin tai siitä on tehty kopioita, jotka sijaitsevat eri paikoissa. Esimerkiksi sovellusten tietoturva on suuri ongelma maailmanlaajuisesti ja huonosti testatut tai väärin konfiguroidut sovellukset voivat toiminnallaan aiheuttaa virheitä tietokantaan ja vahingoittaa sen tiedon eheyttä (Nayak & Rao 2014, s. 37).

Tiedon saatavuus tarkoittaa, että tietokantaa käyttävä järjestelmä toimii joutuisasti ja tiedot ovat aina saatavilla luvallisille käyttäjille (National Institute of Standards and Technology 1995, s. 7). Saatavuus voidaan jakaa vielä neljään alaluokkaan: käytettävyyteen, palauttamiseen, varmuuteen ja ketteryyteen. Käytettävyys viittaa kykyyn luoda ja ylläpitää ympäristöä, jonka avulla palvelu saadaan mahdollistettua käyttäjille. Palauttaminen viittaa kykyyn palauttaa tietokantapalvelu, mikäli sen toiminta lakkaa syystä tai toisesta. Varmuus viittaa kykyyn tarjota palvelua käyttäjille tietyntasoisesti tietyillä aikajaksoilla. Ketteryys viittaa kykyyn tunnistaa mahdolliset ongelmat tietokannassa, jäljittää näiden ongelmien aiheuttajat ja lopulta korjata ongelmat. (Mullins 2002, s. 210) Tiedon saatavuus on vaarantunut, kun siihen tai sen

käyttöjärjestelmään käsiksi pääsy tai käyttö häiriintyy (National Institute of Standards and Technology 2004, s. 2).

Yrityksen toimiessa kansainvälisesti, voidaan sen tietokannan tietoja tarvita hyvinkin ruuhkaisesti jopa kellon ympäri, sillä jokainen hetki on paras aika käyttää tietokannan tietoja jossain päin maailmaa. Kilpailijoiden palveluiden ollessa vain muutaman klikkauksen päässä, saattaa kuluttajien olla hyvinkin helppo saada haluamansa jostain muualta. Palveluiden saatavuus puolestaan ei vaikuta ainoastaan yrityksen myyntiin ja sivustojen aktiivisuuteen, vaan myös kuluttajien mielikuvaan yrityksestä ja tätä kautta osittain myös sen brändiin. (Mullins 2002, s. 217-218) Esimerkiksi Sonyn sulkiessa sen PlayStation-verkoston viikon ajaksi, aiheutui sille varmasti suorien taloudellisten kustannusten lisäksi myös vaikeasti arvioitavia brändiin ja asiakassuhteisiin liittyviä taloudellisia tappioita.

Näiden CIA-ominaisuuksien vaarantumisen vaikutukset yrityksen toimintaan voidaan jakaa kolmeen eri tasoon, jotka ovat vähäinen, kohtalainen ja suuri. Niiden tarkemmat kuvaukset löytyvät liitteestä 1. Käytäntöön sovellettaessa tulee näiden tasojen määritelmien olla sidottu kunkin organisaation tai yrityksen etujen mukaisesti. (National Institute of Standards and Technology 2004, s. 2)

Tasot ovat siis sidottu CIA-ominaisuuden vaarantumisen vaikutuksiin yrityksen toiminnassa, varoissa tai sen yksilöissä. Esimerkiksi Sonyn tietomurron vaikutukset olivat yritykselle kohtalaisia, sillä sen varoihin kohdistuvat vaikutukset olivat hyvinkin suuret ja sen toiminta lakkautui tietyiltä osin joksikin aikaa. Myös yritystä koskettaville yksilöille tapahtui kohtalaista harmia, sillä heidän tietojaan päätyi ulkopuolisten käsiin.

2.3 Tietotyyppien tietoturvaluokitukset

Edellisessä kappaleessa käsiteltyjen tasojen avulla voidaan luokitella CIA-ominaisuuksien tärkeys eri tietotyyppejä käsitteleville yrityksille. Tätä luokittelua voidaan hyödyntää käyttäjätietojen käsittelemiseen ja tietojärjestelmän tietoihin ja se soveltuu niin elektronisen formaatin, kuin myös fyysisen formaatin omaaviin tietoihin. Luokittelun tuloksia voidaan käyttää hyödyksi mm. suunniteltaessa oikeanlaista tietoturvatasoa yrityksen käytetylle tietojärjestelmälle. Oikeanlainen tietoturvaluokittelu tietyn tietotyypin käsittelemisessä vaatii

jokaisen CIA-elementin potentiaalisen vaarantumisen vaikutuksen läpikäymistä kyseisessä tapauksessa. (National Institute of Standards and Technology 2004, s. 3)

Tietoturvaluokittelussa yritys arvioi sen tietojärjestelmän varastoivan tiedon eri CIA-ominaisuuksien vaarantumisen vaikutukset sen toimintaan ja näin ollen pystyy päättelemään järjestelmälle asetettavat tietoturvavaatimukset. Esimerkiksi julkista tietoa tietojärjestelmässään käsittelevä yritys voi todeta, ettei sen tiedon luottamuksellisuus voi vaarantua. Sen sijaan eheyden vaarantumisen vaikutus olisi kohtalainen ja saatavuuden vaarantumisen vaikutus olisi myös kohtalainen. Rikostutkimusperäistä tietoa käsittelevä lakiyritys voi taas määritellä tiedon luottamuksellisuuden vaarantumisen vaikutukset suurina, eheyden vaarantumisen vaikutukset kohtalaisina ja saatavuuden vaarantumisen vaikutukset myös kohtalaisina. Tällöin sen tietojärjestelmän tietoturvavaatimukset olisivat erilaiset, kuin julkista tietoa käsittelevän yrityksen tietojärjestelmän. (National Institute of Standards and Technology 2004, s. 3-4)

Laajempi kokonaisuus pelkän yhdenlaisen tiedon käsittelemiseen on tietojärjestelmä, johon on varastoitu erityyppistä tietoa. Tällöin ei riitä, että järjestelmälle tehdään tietoturvaluokitus vain yhden tietotyypin mukaan, vaan joudutaan tehdä tietoturvaluokitus jokaisen tietyypin mukaan. Tällöin saadaan kaikkien mahdollisten tietojen vaarantumisen vaikutukset selville ja pystytään tekemään tietoturvaluokitus koko tietojärjestelmälle. Mikäli tietojärjestelmän tietojen vaarantumisen vaikutusten välillä on eriäväisyyksiä, otetaan jokaisesta tapauksesta aina korkeimmat arvot ja sijoitetaan ne koko tietojärjestelmän turvaluokitukseen. (National Institute of Standards and Technology 2004, s. 4)

Tätä samaa tietojärjestelmän periaatetta voidaan soveltaa myös erilaisiin tietoa varastoiviin pilvipalveluihin. Tällöin myös pilvipalvelun sisältämille tiedoille tulee tehdä yksityiskohtainen tarkastelu jokaisen tietotyypin mukaan. Näiden tietotyyppien ominaisuuksien vaarantumisen vaikutukset ovat kuitenkin vaikeasti arvioitavissa pilvipalvelua ylläpitävälle yritykselle, sillä sen voi olla vaikea tietää miten tärkeitä sen varastoimat eri tiedot ovat tärkeitä näille tietoa käyttäville yrityksille. (Almorsy et al. 2011, s. 367)

2.4 Keskeiset tietoturvaongelmat

Nykyaikana yritykset ja organisaatiot kohtaavat monenlaisia ongelmia tietoturvan saralla. Mahdolliset seuraukset tietovuodoista tai tietojen katoamisesta voivat merkittävästi alentaa yrityksen arvoa. Toimivaan ja tehokkaaseen tietoturvajärjestelmään päästään, kun panostetaan sekä teknologiaan että sen käyttäjiin. Teknologia itsessään kehittyy ja kehityksen myötä tietoturvajärjestelmiin tulla aukkoja, mutta yleisesti organisaatioissa sekä yrityksissä on vaikeaa saada työntekijät sitoutumaan sisäisiin säädöksiin ja ohjeisiin. (Bulgurcu et al. 2010) Epämieluisaksi tilanteen tekee yritykselle ja organisaatioille tietojen suojaamisen vaikeus verrattuna esimerkiksi ohjelmistohyökkäyksen tekemiseen. Internetistä löytää ilmaiseksi tietoa sekä ohjeita, kuinka murtaudutaan toisiin järjestelmiin, sen sijaan tietoturvallisuus maksaa yritykselle todella paljon erilaisten koulutusten, työpaikkojen sekä ohjelmistojen muodossa. (Rainer & Prince 2016, s. 99-100)

Tietoturva liittyy läheisesti riskienhallintaan, sillä tietoturvan parantamiseksi täytyy olla tiedossa, mitä vastaan ollaan suojautumassa ja kuinka todennäköinen tapahtuma on. Tehdäkseen päätöksiä suojautumisesta uhkia kohtaan täytyy ensiksi kartoittaa, mitä riskejä toimintaan liittyy. Todennäköisyys riskeille toimii eräänlaisena kertoimena riskille sen seurausten vakavuuden kanssa ja näiden kombinaatio antaa riskille arvon, jota verrataan siihen paljonko mahdollinen suojautuminen kustantaa. Uhkia on monenlaisia ja ne voivat olla sisäisiä tai ulkoisia, mutta suojautua voi myös monella eri keinolla. (Rainer & Prince 2016, s. 101-103)

Sisäisellä uhkalla tarkoitetaan yrityksen sisältä tulevaa riskiä. Tämä voi tarkoittaa esimerkiksi yhteistyökumppania tai yrityksen omaa työntekijää, joka toiminnallaan voi luoda tietomurron tahattomasti tai tahallisesti. Mahdollisen sisäisen tietomurron syiden skaalakin on käytännössä ääretön vaihdellen hetkellisestä mielijohteesta aina huonoon ammattitaitoon. Oli syy mikä tahansa, sisäinen tietomurto on erittäin tehokas tapa aiheuttaa yritykselle suuria taloudellisia tappioita. (Probst et al. 2010, s. 4-6).

Sisäisistä uhkista puhuttaessa työntekijät ja inhimilliset virheet yrityksissä ovat yleisin ongelma. Työntekijöiden tietoturvauhkien ehkäisemiseksi heitä voidaan kouluttaa sekä luoda

yleisesti tietoturvatoimintatavat yrityksen sisälle. On tärkeää, että työntekijät ovat tietoisia yrityksen tietoturvasta. Riittävään tietoisuuden tasoon päästään, kun työntekijöiden yleinen tietämys tietoturvasta sekä yrityksen sisäisestä toimintatavasta ovat riittävää sekä niihin ollaan sitouduttu. Riittävyyden taso riippuu työtehtävistä ja siitä, miten olennaista ja arkaluontoista tietoa niihin sisältyy. Mitä korkeammalla tasolla työntekijä on yrityksen sisällä, sitä suurempi merkitys inhimillisillä virheillä on. Inhimillisiin virheisiin kuuluvat kaikki huolimattomuusvirheet, kuten väärien laitteiden käyttö tai muistitikun ja tietokoneen unohtaminen avoimelle paikalle. Lisäksi liian yksinkertaiset salasanat ja epäilyttävien linkkien sekä sähköpostien avaaminen ovat inhimillisiä virheitä. Inhimilliset virheet ovat tahattomia tapahtumia, jotka tapahtuvat jokapäiväisen työskentelyn lomassa. (Bulgurcu et al. 2010; Rainer & Prince 2016, s. 88-93)

Ulkopuolisia uhkia on monenlaisia, mutta tarkoituksella tehdyt hyökkäykset ovat yleisimpiä. Yleisin motiivi hyökkäyksille on saavuttaa taloudellisia hyötyjä, mutta se voidaan saavuttaa monella eri tavalla esimerkiksi tiedon avulla kiristäminen. Hyökkäyksiä on monenlaisia ja hyökkäysten päämäärät voivat vaihdella suuresti. Esimerkiksi palvelunestohyökkäys (Denial-of-Service,DoS tai Distributed Denial-of-Service, DDoS) tapahtuu verkkohyökkäyksenä, jossa palvelimelle kohdistetaan suuri määrä liikennettä samanaikaisesti yhdestä tai useammasta lähteestä. Suuren liikenteen vuoksi palvelin ei pysty käsittelemään kaikkea ja yleensä se kaatuu vaarantaen tiedon saatavuuden. Toisenlainen hyökkäysesimerkki on välistävetohyökkäys (Man-in-the-Middle, MitM), jossa hyökkääjä tunkeutuu kahdenväliseen keskusteluun ja esittää molemmille olevansa toinen osapuoli. Tällä hyökkäyksellä pystytään esimerkiksi kalastelemaan tietoa kuten salasanoja. Yhdenlainen tapa hyökätä on esimerkiksi kehittää haittaohjelma tai virus, jonka päämäärän voi hyökkääjä itse ohjelmoida. Se voi olla kohdistettu hyökkäys jotakin tiettyä kohdetta kohtaan tai laajamittaisempi hyökkäys. Helppo kohde on hyökkäysten yleisin syy, koska hyökkääjä itse saa vaivattomimmin taloudellisia hyötyjä. (Rainer & Prince 2016, s. 94-98)

Onnistuneen hyökkäyksen kohteeksi joutuessa yrityksen tiedon luottamuksellisuus sekä eheys kärsii. Samankaltaista luottamuksellisuuden menetyksen yritys kohtaa, kun salattuihin tiedostoihin pääsee käsiksi taho, jolle ne eivät kuulu. Tämä taho voi tulla yrityksen sisältä

esimerkiksi työntekijä, joka tietämättään on saanut käsiinsä hänelle kuulumatonta tietoa, tai ulkopuolelta sovellushyökkäyksen tehnyt yksityishenkilö. (Rainer & Prince 2016, s. 99-100)

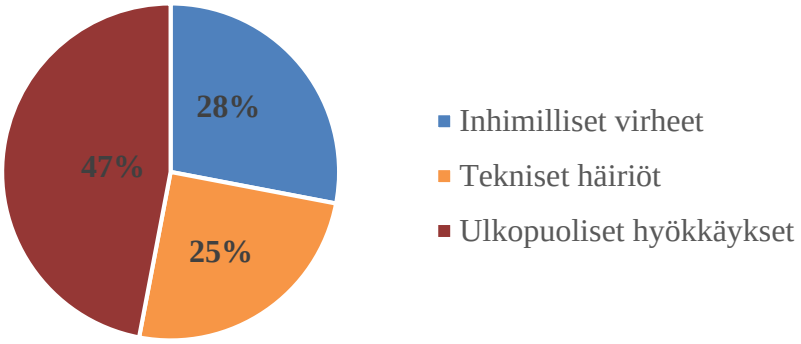
Tahallisten ulkopuolisten uhkien lisäksi tahattomia tapahtumia saattavat olla tulipalot, sähkökatkot, luonnonkatastrofit sekä muut samankaltaiset tapahtumat. Näistä voi aiheutua Erityisen pahoja seurauksia, jos tärkeimmät serverit ja tietovarastot ovat keskitettynä eikä hajautettuna ja niiden tuhoutuminen aiheuttaa kriittisiä menetyksiä. Tämä vaarantaa tiedostojen saatavuuden ja eheyden, kun mahdollisesti tiedostoja tuhoutuu tai vaurioituu tietokannasta. (Rainer & Prince 2016, s. 92-93)

Erilaisten tietoturvasovellusten sekä -politiikan lisäksi suuremmat toimitilat vaativat fyysisiä tietoturvasuojia. Käytännössä fyysisellä suojautumisella estetään yrityksen alueelle pääseminen sinne kuulumattomilta henkilöiltä. Fyysisiä suojautumistapoja ovat aidat, portit, ovet, vartijat, kulkuluvat sekä hälytysjärjestelmä. Jotta alueelle pääseminen on mahdollista, henkilön tulee ensiksi tunnistautua. Tunnistautumismenetelminä voi toimia esimerkiksi kulkukortti, kasvotunnistus tai jopa henkilön ääni. (Rainer & Prince 2016, 102-105)

Esineiden internetillä voidaan helpottaa tunnistaumisprosessia ja pienentää kustannuksia. Vartijoiden tarpeellisuus voidaan kyseenalaistaa, jos alueelle pääsyn edellytyksiä on tunnistautua henkilökohtaisella kulkukortilla ja yleisellä salasanalla. Lisäksi kameravalvonta on automaattista ja tilanteissa, jossa salasana kirjoitetaan väärin, kamera automaattisesti ottaa kuvan henkilön kasvoista sekä järjestelmä ottaa havainnon ylös. Esineiden internetin ongelmia ovat kuitenkin yleensä keskitetty verkosto, joka aiheuttaa esimerkiksi ylläpito- sekä tietoturvaongelmia. Tekniset häiriöt kriittisissä kohdissa verkostoa aiheuttavat suuria tietoturvariskejä. Lisäksi koko järjestelmä voidaan kaataa, jos keskitetyn verkon solmu kohta hakkeroidaan. (Li et al. 2015)

Vuonna 2017 kesäkuussa Ponemon instituution ja IBM:n julkaisemassa tutkimusraportissa kerrotaan 419 eri yrityksen kohtaamista tietomurroista, jotka ovat 13 eri maasta tai alueesta (Lähi-itä sekä ASEAN). Tutkimukseen osallistuvat yritykset olivat pääsääntöisesti suuria yrityksiä, sillä 88 % osallistuneista työllisti vähintään 500 työntekijää kansainvälisesti. Tutkimuksessa havaittiin kuvan 1 mukaisesti, että keskimäärin jopa 47 % tietomurroista johtui

ulkopuolisista hyökkäyksistä yrityksiä kohtaan. Sen sijaan tekniikasta johtuvat tietomurrot sekä inhimilliset virheet aiheuttivat lähes yhtä suuren määrän tietomurtoja. (Ponemon Institute & IBM Security 2017, s. 1, 14-15, 31) Tietomurrot kokonaisuutena, murron syystä riippumatta, aiheuttavat yrityksille kustannuksia sekä heikentävät tilanteesta riippuen eri CIA-ominaisuuksia.



Kuva 1. Tietomurtojen jakautuminen (Ponemon Institute & IBM Security 2017, s. 14)

2.5 Tietoturva kolmannen osapuolen pilvipalveluissa

Pilvipalvelut ovat kasvattaneet suosiotaan yritysten tiedonvarastoinnissa, sillä ne tarjoavat kustannustehokkaan vaihtoehdon tiedon varmuuskopiointiin ja sen varastointiin. Erityisesti varmuuskopioinnin tärkeyttä lisää nykyaikana se, että esimerkiksi tärkeitä sopimuksia ja asiakirjoja säilytetään vain sähköisesti. On siis täysin mahdollista, että pelkästään sähköisessä muodossa olevia sopimuksia varastoidaan tietyssä sijainnissa ilman varmuuskopiota. Jos tiedosto häviää, ei ole mitään keinoa, millä se voitaisiin palauttaa ilman varmuuskopiointia. (Nayak & Rao 2014, s. 263-264) Teknologiayritys Ciscon arvioiden mukaan vuoteen 2020 mennessä pilvipalvelimiin tallennetun tiedon määrä on 88 % kaikesta tallennetusta tiedosta (Kshetri 2017). Vaikka pilvipalvelu nähdään yleensä kustannustehokkaampana ratkaisuna oman tietovarastoinnin sijaan, liittyy siihen paljon riskejä ostavan yrityksen kannalta (Nayak & Rao 2014, s. 272-274).

Pilvipalveluja on neljää eri tyyppiä: julkinen, yhteisö, yksityinen ja hybridi. Yhteistä eri palvelutyypeillä on kuitenkin omistaminen, ylläpitäminen ja hallinnointi, jotka voivat olla toteutettu kolmannen osapuolen turvin tai pilveen osallistujien voimin.

1. Julkinen pilvi on tarjolla avoimesti suurelle ihmismäärälle.
2. Yhteisöpilvi on nimen mukaisesti tietylle yhteisölle kohdistettu pilvipalvelu. Yhteisöön voi kuulua esimerkiksi useita eri yhtiöitä, jotka toimivat yhteistyössä tai työskentelevät saman projektin parissa.
3. Yksityinen pilvi kohdistettu pelkästään suljettuun ympäristöön esimerkiksi yrityksen sisäiseen tietoon. Helpompi turvata tietoa, kun se on suljetussa ympäristössä.
4. Hybridipilvi on aiemman kolmen vaihtoehdon kombinaatio. Siihen voi kuulua kaksi variaatiota tai kaikki kolme. Yhdistetyt pilvipalvelut pysyvät ainutlaatuisina kokonaisuuksina, mutta ovat sidoksissa toisiinsa, jolla mahdollistetaan tiedon sekä sovellusten siirron. (National Institute of Standards and Technology 2011)

Pilvipalvelu sopii hyvin sellaisen tiedon varastointiin, joka ei ole äärimmäisen luottamuksellista, koska osallisena on kolmas osapuoli. Tämän vuoksi esineiden internetin sensorien ja muun laitteiston tuottama tieto soveltuu hyvin pilvipalvelun kanssa yhteen. Tiedon määrän vaihdellessa pilvipalvelu pystyy nostamaan kapasiteettinsa määrää, mikä on yksi hyöty niiden käyttöönotossa. Yhteistyön etu on myös automaattisuus eli tieto voidaan automaattisesti varastoida. (Botta et al. 2015)

Pilvipalveluissa yhtenä ongelmana on luottaminen kolmanteen osapuoleen mm. luottamuksellisen tiedon varastoijana. Yksi suurimmista haittapuolista pilvipalveluissa kiertää tietoturvan sekä luottamuksellisuuden ympärillä, koska se on huolenaihe yrityksille, jotka kohtaavat tietomurtoja. Tietomurrot saattavat johtaa oikeudenkäynteihin, kun luottamuksellista tietoa on päässyt julkiseen jakeluun. Yhtenä suojamekaniikkana toimii zero trust –politiikka, jonka avulla yhden pilvipalveluun kuuluvan yksikön hakkerointi ei aiheuta suurta haittaa kokonaiskuvassa. Yksiköillä oikeudet ovat rajatut, jonka seurauksena vain verkostolla on oikeudet kaikkeen tietoon pilvessä – yksiköllä vain osaan siitä. (Kshetri 2017) Kaikki tietoturvalliset ongelmat eivät vaikuta samalla tavalla jokaiseen pilvipalvelutyyppiin, vaan eroja syntyy erityisesti julkisten ja yksityisten pilvien välillä.

Pilvipalveluissa suurimpia tietoturvariskejä ovat sisältä tulevat hyökkäykset. Sisältäpäin tulevassa hyökkäyksessä hyökkääjä pääsee käsiksi järjestelmään helposti ja mahdollisesti omaa

oikeudet tietoon, joka on luottamuksellista. Yksi ongelma pilvipalveluissa on juuri ulkopuolisten palveluiden käyttö, useimmat yritykset eivät näe tarpeelliseksi kehittää omaa pilvijärjestelmää, vaan ostavat sen kolmannelta osapuolelta. Tästä johtuen pilvipalveluja tarjoava yritys on osallisena palveluja ostavan yrityksen tiedon varastoinnissa. Ostettuun palveluun liittyy myös salaukseen mahdollisia ongelmia. Pilvipalvelut ovat salattuja sovelluksia, mutta salaukset ovat juuri niin hyviä kuin salaukseen käytetyt menetelmät ovat. Käytännössä tämä tarkoittaa, että ostettu pilvipalvelu salataan palvelun tarjoajan toimesta ja tällöin ostaja ei pysty vaikuttamaan salauksen vahvuuteen tai muokkaukseen. (Nayak & Rao 2014, s. 282-287; Rainer & Prince 2016, s. 447-450)

Pilvipalvelun ostajan on myös vaikea vaikuttaa miten ja minne tieto varastoidaan. Maakohtaisten lakien noudattaminen voi olla vaikeaa ja esimerkiksi monissa EU-maissa on tietyntyyppisen tiedon siirtäminen pois maan sisältä kiellettyä. Paikallisten lakien mahdollisen rikkomisen lisäksi on syytä miettiä, miten tietovuodon sattuessa tutkinta suoritetaan. Hyvä pilvipalvelujen tarjoaja kuitenkin tiedottaa, miten palvelujen ostavan tahon tieto varastoidaan. (Kavitha & Subashini 2011)

2.6 Tietoturva osana yrityksen taloutta

Tietoturvan kustannuksia ja etuja on tarkasteltava huolellisesti, jotta sen kustannukset eivät ylitä sen odotettuja hyötyjä. Näin ollen tietoturva on yksinkertaisuudessaan älykästä liiketoimintaa. Tietoturvan ylläpitämisen kustannukset voidaan jakaa suoriin ja epäsuoriin kustannuksiin. Suorat kustannukset liittyvät tietoturvajärjestelmän implementoimiseen ja ylläpitämiseen. Epäsuorat kustannukset liittyvät taas puolestaan uuden tietoturvajärjestelmän aiheuttamiin mahdollisiin kustannuksiin mm. työn tehokkuudessa, työntekijöiden moraalissa ja uusien tietoturvamenetelmien uudelleen kouluttamisessa. (National Institute of Standards and Technology 1995, s. 11)

Tietomurroista seuraa myös yritykselle kustannuksia. Nämä kustannukset voidaan jakaa lyhytaikaisiin ja pitkäaikaisiin kustannuksiin. Lyhytaikaiset kustannukset ovat mm. menetetty liiketoiminta, tiedon saatavuuden menetyksestä johtuvat kustannukset, tietoturvavian korjaamisen kustannukset, mahdolliset oikeuskulut ja tiedottamisesta johtuvat kulut. Pidempivaikutteisia kustannuksia yritykselle aiheuttavat pitkäaikaiset kustannukset mm.

asiakkaiden menetykset, brändin heikentymisen, yrityskumppanien luottamusten menetykset ja luottamuksellisen tiedon vuodosta johtuvat kustannukset. Heikentynyt tietoturva voi myös aiheuttaa yritykselle kustannuksia korkeampien vakuutusmaksujen kautta. (Cavusoglu et al. 2004, s. 72) Suurin osa näistä pitkäaikaisista kustannuksista on aineettomia, jonka takia niitä onkin hyvin vaikea laskea. Ne ovat kuitenkin erityisen tärkeitä kartoitettaessa yritykselle aiheutuneita kokonaiskustannuksia tietomurrosta. (Ko & Dorantes 2006, s. 15)

Pitkäaikaiset kustannukset tietomurrosta voivat kuitenkin olla paljolti pienemmät, kuin siitä aiheutuvat lyhytaikaiset kustannukset. Tämä voidaan osin selittää sillä, että tietomurrosta kärsineet yritykset tapaavat panostaa jatkossa enemmän tietoturvaan, jolloin pitkällä aikavälillä niiden tietomurrot vähentyvät kilpailijoihin nähden. (Ko & Dorantes 2006, s. 20) Tämä korreloi osittain IBM:n tutkimusrapotin tulosten kanssa, jonka mukaan tietomurron suuruus vaikuttaa laskevasti yrityksen seuraavan tietomurron tapahtumiseen 24 kuukauden sisällä. (Ponemon Institute & IBM Security 2017, s. 24) Toinen syy tähän voi löytyä ihmisten luonteesta unohtaa yritykselle tapahtuneet tietomurrot ajan kuluessa (Ko & Dorantes 2006, s. 20)

Mitä nopeammin tietomurto havaitaan ja saadaan kuriin, sitä pienemmät ovat siitä aiheutuvat kustannukset. IBM:n tutkimuksessa selvisi, että tietomurron havaitseminen kesti yrityksiltä keskimäärin 191 päivää ja sen korjaus 66 päivää vuonna 2017. Mikäli tietomurto havaittiin alle 100 päivän päästä koitui siitä kustannuksia noin 27% vähemmän, kuin yli 100 päivän päästä havaitusta tietomurrosta. (Ponemon Institute & IBM Security 2017, s. 26-27)

Tietomurron vaikutukset yritykselle voidaan määritellä kolmen eri ominaisuuden mukaan, jotka ovat yrityksen ominaisuudet, tietomurron tyyppi ja tietomurron ajankohta. Tietomurron taloudellisiin vaikutuksiin liittyvät yrityksen ominaisuudet ovat lähinnä sen tapa tehdä liiketoimintaa ja yrityksen koko. Esimerkiksi pelkällä kivijalkakaupalla liiketoimintaa tekevä yritys saattaa kärsiä vähemmän tietomurrosta sen tietokantaan, kuin esimerkiksi pelkällä verkkokauppatoiminnalla liiketoimintaa tekevä yritys. Yrityksen koko puolestaan vaikuttaa sen kykyyn selviytyä taloudellisista epävakauksista, joita tietomurrot saattavat sille asettaa. Tietomurtojen tyyppejä on erilaisia ja ne saattavat vaarantaa yrityksen tietojärjestelmän tietojen luottamuksellisuutta, eheyttä tai saatavuutta. Näin ollen jokaisen tietomurron tyypin

vaikutukset yrityksen tietojärjestelmän tietoihin ja talouteen ovat erilaisia. (Cavusoglu et al. 2004, s. 75-77)

Tietomurron ajankohta viittaa sekä sen ajankohtaiseen vaikutukseen yritykselle sekä alati kehittyvään tarpeeseen ja yritysten keskittymiseen tietojensa turvaamiseen. Tämä tarkoittaa, että aiemmin tapahtuneet tietomurrot ovat saattaneet olla vähemmän vaikuttavia yrityksen talouteen, kuin tulevaisuudessa tapahtuvat tietomurrot. (Cavusoglu et al. 2004, s. 77-78) Tämän takia on myös oleellista tarkastella potentiaalisen tietomurron ajankohdan vaikutuksia tulevaisuuden skenaarioissa.

Tietojen saatavuudesta aiheutuvat kustannukset mitataan yleensä yrityksen menetetyllä liiketoiminnalla varsinkin internetissä toimivilla yrityksillä, kuten Amazonilla tai Ebaylla. Tällöin yleensä myös mielletään näiden yritysten kustannukset tiedon saatavuuteen liittyen olevan suuret verrattuna mm. enemmän liiketoimintaa kivijalkamallin avulla. Tämä ei kuitenkaan välttämättä pidä paikkaansa, sillä kustannuksissa täytyisi myös ottaa huomioon menetetty työntekijöiden työpanos tietokatkon ajalta. Internetissä toimivalla yrityksellä saattaa tietokatkos aiheuttaa 90% menetykset liiketoiminnasta ja 90% menetykset työntekijöiden työpanoksesta tietokatkoksen ajalta, kun taas kivijalkatoimintaa harjoittavan yrityksen kustannukset voisivat muodostua 10% menetetyistä tuloista ja 90% työntekijöiden menetetystä työpanoksesta. (Patterson 2002)

Matemaattiset mallit, joissa käsitellään yrityksen tiedon uhkia, altistumisen todennäköisyyttä ja tiedon suojelemiseen käytettyä rahamäärää toteavat optimaalisen tietojen suojelemiseen käytetyn rahamäärän olevan pieni osa tietojen vuotamisen kuluista. Tämä skenaario pätee kuitenkin vain, mikäli tietojen menetyksestä ei aiheudu katastrofaalisia seuraamuksia yritykselle tai muille osapuolille (Gordon & Loeb 2002, s. 438).

Vertailemalla kahta erilaista laajaa tapausta näihin matemaattisiin malleihin, voidaan havaita optimaalisen sijoituksen tietojen suojelemiseen olevan aina vähemmän kuin 37% tietojen menettämisen kustannuksista. Yleensä kuitenkin optimaalinen sijoitus on paljon vähemmän kuin 37%, mutta tämä on vertailuista saatu maksimiarvo. Tämä on kuitenkin vain

matemaattinen malli, eikä ota huomioon kaikkia realistisia vaikutuksia, jotka vaikuttavat tietoturvan tason valitsemiseen. (Gordon & Loeb 2002, s. 440-441)

IBM:n raportin mukaan yrityksille eniten kustannuksia aiheuttavia tietomurtoja olivat ulkopuolisten haitalliset hyökkäykset. Keskimääräinen kustannus yhden henkilötietotallenteen vaarantumisesta tällaisessa hyökkäyksessä oli noin 156 dollaria, kun taas järjestelmän vioista johtuvien virheiden kustannus oli 128 dollaria ja inhimillisestä virheestä johtuva tiedon vaarantuminen oli 126 dollaria yhtä henkilötietotallennetta kohden. Liitteessä 2 esitetään maantieteellisten erojen vaikutus tietomurtojen aiheuttamiin kustannuksiin yrityksille. Suurimmat keskimääräiset kustannukset yhden henkilötiedon vaarantumisesta vuonna 2017 olivat Yhdysvalloissa toimivilla yrityksillä ja pienimmät Intiassa toimivilla yrityksillä. (Ponemon Institute & IBM Security 2017, s. 6)

Tietomurtojen kustannukset vaihtelevat myös yrityksen liiketoiminnan mukaan. Yhdysvalloissa liiketoimintaa harrastavalle yritykselle koituu keskimääräisesti 141$ kustannukset yhden henkilötietoprofiilin tietomurrosta. Liite 3 kuvaa vuonna 2017 ja sitä neljänä edeltävänä vuonna tapahtuneiden tietomurtojen keskimääräisiä kustannuksia näille yrityksille. Tietomurto aiheuttaa keskimääräistä isommat kustannukset terveydenhuollon ja rahoituksen yrityksissä, kun taas julkisen sektorin ja tutkimustyötä tekeviin yrityksiin kohdistuvat tietomurrot aiheuttavat keskimääräistä pienemmät kustannukset. (Ponemon Institute & IBM Security 2017, s. 13) Nämä erot johtuvat mitä luultavimmin näiden tietotyyppien erilaisista tietoturvaluokituksista, jolloin myös niihin kohdistuvien tietomurtojen vaikutukset yritykselle ovat erilaiset.

2.7 Tietoturvan toteuttaminen

Onnistuneella tietoturvajärjestelmällä voidaan luoda yritykselle lisäarvoa, sillä sidosryhmät sekä asiakkaat saavat luottamusta toimivasta järjestelmästä. Tietoturvan toteuttamisen ja soveltamisen pohjana toimii yrityksen suunnitellut käytännöt ja standardit tietoturvan saralla. Niiden laatiminen ei kuitenkaan ole suurin haaste, vaan kuinka jo valmiiksi luotuja menetelmiä lähdetään soveltamaan ja kehittämään yrityksen sisällä sekä kuinka ne kattavat koko yrityksen tietoturvatarpeet sekä palvelee koko organisaation päämäärää. Myös ohjelmistot, laitteet ja menetelmät vanhenevat ajan myötä, joten jokapäiväinen tietoturvan parantaminen on iso osa

toimivaa tietoturvajärjestelmää. (Nayak & Rao 2014, s.56-58) Kuva 2 havainnollistaa tietoturvan toteuttamisen jatkuvaa kehittymistyötä sekä minkälaisista eri elementeistä se koostuu.

Kuva 2. Tietoturvan toteuttamisen kehä (Nayak & Rao 2014, s.56)

Tehokkaan tietoturvamallin rakentaminen yritykselle vaatii sen toimintaan liittyvien tietoturvariskien kartoittamista. Näiden riskien kartoittamisen avuksi on luotu erilaisia riskienhallintatyökaluja, kuten ISO 31000-standardi. Tavoitteena on suorittaa riskien kartoitus ja arviointi perusteellisesti sekä tehokkaasti, mutta sillä millä keinoin haluttuun lopputulokseen päästään ei ole merkitystä. Lopputuloksena on tarkoitus olla kattava hahmotelma riskeistä koko organisaation kannalta, johon on yhdistetty jo voimassa olevat toimenpiteet sekä niiden vaikutukset. Riskien havainnointia ja kartoittamista tulee jatkaa yrityksessä koko ajan ja sen on oltava osa jokapäiväistä työskentelyä. Näin voidaan mahdollistaa, että yrityksen tietoturva pysyy kehityksen mukana. (Blakley et al. 2001; Nayak & Rao 2014, s.56-57)

Valmiiksi olemassa olevissa yrityksissä suunnittelutyöhön kannattaa sisällyttää kaikki mahdolliset sidosryhmät, jotka ovat merkittäviä tekijöitä tietoturvan kannalta eli esimerkiksi sidosryhmät joiden kanssa vaihdetaan luottamuksellista tietoa. Suunnitteluvaiheessa pystytään myös selkeästi jakamaan vastuuta organisaation sisällä eri ihmisille ja myös muokkaamaan organisaatiorakennetta tarvittaessa. Aikatauluttamisella saadaan selkeät tavoitteet työskentelylle ja vastuunjakamisella vetäjät eri projekteille. Suunnitelman eri toteutusvaiheet

riippuvat pitkälti suunnitelmasta sekä minkälaisia menetelmiä ja standardeja on käytetty, mutta jokaisen suunnitelman tulee johtaa tehokkaaseen tietoturvajärjestelmään sekä arkkitehtuuriin. (Blakley et al. 2001; Nayak & Rao 2014, s.56-57)

Riskien merkittävyyttä on syytä arvioida kahdella parametrilla: todennäköisyys sekä vaikutus. Todennäköisyydellä tarkoitetaan yksinkertaisesti sitä, kuinka usein tapahtuma tapahtuu keskimäärin tietyn aikavälin aikana ja vaikutus kuinka suuria negatiivisia seurauksia tapahtuma aiheuttaa. Näiden tekijöiden tulolla voidaan laskea riskeille arvo, jonka avulla voidaan asettaa riskit tärkeysjärjestykseen. (Bowen et al. 2006, s. 89-90)

Valvontajärjestelmä on olennainen osa toimivaa tietoturvajärjestelmää, jonka avulla voidaan ehkäistä ja ennakoida mahdollisia tietomurtoja. Ongelmaksi valvonnassa muodostuu ajankäyttö, joka taas tuo lisäkustannuksia yritykselle. Valvontaa on monenlaista kuten yhteyksien seurantaa, levytilan käytön valvomista sekä kaistanleveyden käytön seurantaa. Esimerkiksi yrityksen sisäisellä raportoinnilla voidaan kerätä tietoa erilaisten inhimillisten virheiden yleisyydestä. Tulevaisuuden kannalta on myös suotavaa seurata sisäisten raporttien lisäksi muissa yrityksissä ja organisaatioissa tapahtuneita tietoturvamurtoja, josta voidaan ammentaa hyödyllistä tietoa omiin tietoturvajärjestelmiin. (Blakley et al. 2001; Nayak & Rao 2014, s.58)

Haasteita jatkuvasti kehittyvällä alalla on pitää koko organisaatio samassa tietämyksessä. Erityisesti suuremmissa yrityksissä haasteita luo eri työkalujen käyttö ja monissa toimipisteissä sekä mahdollisesti erilaiset toimintatavat. (Nayak & Rao 2014, s.57) Yritykset kohtaavat myös jatkuvia haasteita lakien ja säännösten muuttuessa. Esimerkiksi henkilötietojen käsittelyyn liittyvä tietosuoja-asetus GPDR (General Data Protection Regulation) astuu voimaan 25.5.2018 Euroopan unionin alueella. Perusideana asetuksella on suojata henkilötietoja väärinkäytöltä sekä lisätä yksilön vaikutusvaltaa tietojen käytöstä. Yrityksille asetus asettaa suuremman vastuun kuin aiemmin ja henkilötietorekisteri pitäjän velvollisuudet kasvavat, mitä suurempia riskejä rekisterin ylläpitoon liittyy. (Tietosuojavaltuutetun toimisto 2018) Lisäksi erityisesti monikansallisilla yrityksillä ongelmaksi muodostuu eroavaisuudet maiden välillä. Erityisesti tietotekniikan alalla on lakeja, jotka estävät tietotekniikan sekä tiedon väärinkäyttöä. (Nayak & Rao 2014, s.58)

3 LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologia on viime aikoina kerännyt merkittävää huomiota niin potentiaalisena kryptovaluuttojen mahdollistajana, kuin myös alustana monimutkaisempien tietojärjestelmien toimintaan. Lohkoketjuteknologian ensimmäinen sovellus Bitcoin otettiin käyttöön vasta vuonna 2009, joten teknologian sovellus käytäntöön on vielä kehittyvässä tilassa (Mattila & Seppälä 2015, s. 8). Yksi teknologian ympärille kehittyneistä aiheista on sen soveltuvuus perinteisiä tietokantamenetelmiä tietoturvallisempaan tiedonvarastointiin (Gaetani et al. 2017). Tässä kappaleessa käsitellään lohkoketjuteknologian taustaa, toimintaa ja kehitystä.

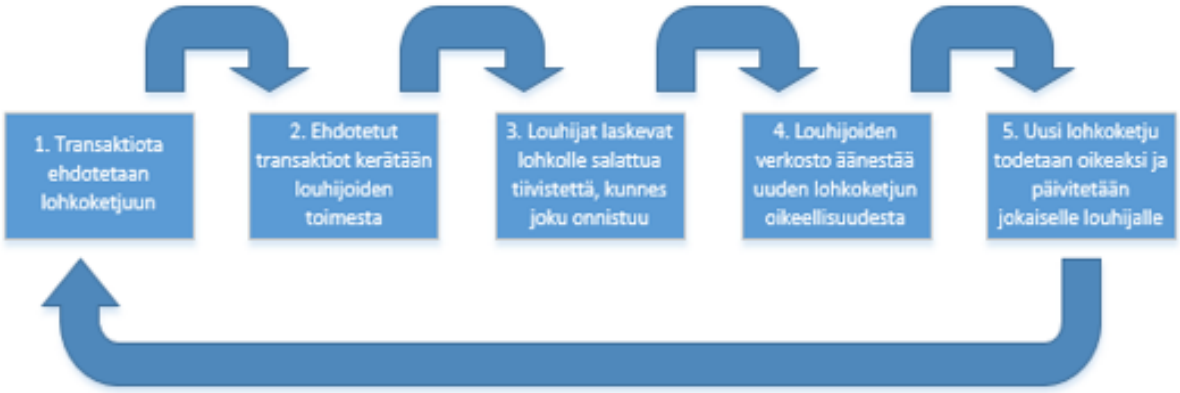
3.1 Lohkoketjuteknologian perusteet

Lohkoketjun perusperiaatteen määritelmänä voidaan pitää hajautettua p2p-tietokantaverkostoa, joka julkisen ja salatun avaimen avulla tallentaa salatussa muodossa olevia transaktioita tähän tietokantaan toisiinsa linkitettyinä lohkoina (Kshetri 2017a) Tämä mahdollistaa sen, ettei tarvita minkäänlaista keskitettyä kontrolloijaa, joka jakaisi, ylläpitäisi ja suojaisi tietokantaa omatoimisesti (Mattila & Seppälä 2015, s. 7). Lohkoketjuteknologian mahdollisuuksista puhuttaessa voidaan verrata internetin vaikutusta yhteiskuntaan. Potentiaalia teknologialle on paljon, mutta tulosta haluttaessa ne tulee pystyä konkretisoimaan tuotteiksi tai palveluiksi (Swan 2015, s. VII-X).

Lohkoketjuteknologia toimii lisäämällä yhden lohkon aina seuraavan perään, jolloin lohkoista muodostuu eräänlainen rikkoutumaton ketju. Tätä lohkoketjua voidaan ajatella ikään kuin digitaalisena pilvenpiirtäjänä, joka rakentuu yksi lohko kerrallaan. Lohko luodaan aina kun, järjestelmässä tapahtuu transaktio, jonka lohkoketjuteknologia kirjaa yhdeksi lohkoksi ketjuun. Tällöin kyseiseen lohkoon tallentuu haluttua tietoa kyseisestä transaktiosta ja näin rakentuu jokaisesta transaktiosta koostuva rikkoutumaton lohkoketju. (Bradbury 2015) Tähän lohkoketjuun lisätyt transaktiot ovat jokaiselle verkoston jäsenelle saatavissa, kuten kryptovaluutta Bitcoinin tapauksessa (Nakamoto 2008).

Lohkoketjuteknologia käyttää hyödykseen erilaisia hashaus-menetelmiä salatakseen jokaisen lohkon transaktion. Jokainen lohko sisältää myös edellisen lohkon hashin ja sisällyttää tämän tiedon laskiessaan hashia tämänhetkiselle lohkolle. Jokainen lohko sisältää myös sen transaktion aikaleiman, joka lisätään hashin laskemisen jälkeen ennen lohkon liittämistä

lohkoketjuun. (Swan 2015, s. 37) Lohkoketjun alkulohko on tästä säännöstä poikkeava, sillä siihen ei voida sisällyttää edellisen lohkon tietoja. Tällaisen ketjutuksen avulla pystytään tunnistamaan jokaisen lohkon paikka lohkoketjussa. (Bradbury 2015)



Kuva 3. Lohkoketjuteknologian toiminta yksinkertaistettuna (Bradbury 2015)

Lohkoketjuteknologian tavassa liittää lohkot toisiinsa piilee myös osa sen tärkeimmistä tietoturvallisuuden ominaisuuksista. Jokaisen lohkon hashin vaikutus seuraaviin lohkoihin tarkoittaa, että mikäli joku haluaa muokata tiettyä transaktiota lohkoketjun sisällä, täytyisi hänen hashata uudelleen jokainen kyseistä lohkoa seuraava lohko. Jokaisen lohkon vaatima hashi täytyy myös olla sille ennalta määritetyssä muodossa, jonka laskettavuuden vaikeusaste vaihtelee lohkoketjusta riippuen. Esimerkiksi Bitcoinin lohkoketju vaatii, että lohkon hashin alussa on tietty määrä nollia. Tämä taas vaikeuttaa hashin laskemista ja tätä kautta lohkoketjun transaktioiden väärentämisestä yhä vaikeampaa. (Bradbury 2015) Lohkoketjuteknologia tukee siis luonnostaan erinomaisesti sen varastoiman tiedon eheyttä.

Ketjun jatkamiseksi tarvitaan transaktioiden lisäksi myös työvoimaa näiden transaktioiden lisäämiseksi lohkoketjuun. Tätä varten lohkoketju tarvitsee niin sanottuja louhijoita. Termi ”louhija” tulee Bitcoin kryptovaluutan transaktioiden ylläpitäjistä. Bitcoinia käsitellään tarkemmin seuraavassa kappaleessa. Käytännössä transaktioiden vaatima työvoima on tietokoneiden laskentatehoa ja tämän laskentatehon käyttämää energiaa, eli mitä luultavimmin sähköä. (Nakamoto 2008) Jokainen lohkoketjun louhija, esimerkiksi yksi tietokone, on oma yksikkönsä potentiaalisesti valtavassa hajautetussa louhijoiden verkostossa. Jokainen louhija

lataa automaattisesti päivitetyn version lohkoketjusta aloittaessaan louhimisen, jolloin jokaisella louhijalla on käytössään päivitetty versio lohkoketjusta. (Swan 2015, X)

Lohkoketjuteknologia käyttää hyväkseen lohkoketjun louhijoiden verkostoa määrittääkseen lohkoketjun oikeellisuuden. Tämä poistaa myös kolmannen osapuolen tarpeen transaktioiden luotettavuutta määriteltäessä. Swan 2015, preface X) Tämä hajautetun järjestelmän arkkitehtuuri ja sen mahdollistama kolmannen osapuolen eliminointi transaktioissa on yksi sen pääasiallisista innovaatioista. Näitä tapoja määrittää lohkoketjun oikeellisuus verkoston avulla on erilaisia riippuen lohkoketjusta (Zheng et al. 2016).

Esimerkiksi lisättäessä Bitcoinin lohkoketjuun uusi transaktio, äänestävät kaikki louhijoiden verkostoon kuuluvat onko kyseinen uusi syntyvä lohkoketju oikea vai väärennetty. Lohkoketjun versio, joka saa puolelleen yli 50% verkoston laskentatehosta, todennetaan oikeaksi ja päivitetään taas edelleen jokaiselle louhijalle. (Bradbury 2015) Tätä laskentatehoon perustuvaa menetelmää kutsutaan ”Proof of Work” –menetelmäksi (Zheng et al. 2016). Taulukossa 1 on kuvailtu yleisimpien transaktioiden oikeellisuuden varmistuksen menetelmien ominaisuuksia yksinkertaistetusti.

Taulukko 1. Erilaisten lohkoketjujen äänestysmenetelmien erot (Zheng et al. 2016)

Ominaisuus	**Proof of Work**	**Proof of Stake**	**Practical byzantine fault tolerance**	**Delegated proof of stake**	**Ripple**	**Tendermint**
Äänestävät jäsenet	kaikki	kaikki	osa	kaikki	kaikki	osa
Energian kulutus	suuri	keskiverto	vähäinen	keskiverto	vähäinen	vähäinen
Hyväksytyn transaktion puoltaminen	suurin laskentateho	suurin valuutan omistus	3 vaihetta, joissa jokaisessa saatava 2/3 verkostosta puolelle	Panoksen avulla äänestetyt luotettavat jäsenet	80% jäsenistä	3 vaihetta, joissa jokaisessa saatava 2/3 verkostosta puolelle
Esimerkki	Bitcoin	Peercoin	Fabric	Bitshares	Ripple	Tendermint

Lohkoketjun tyyppi määrittyy myös osittain siihen päästettyjen jäsenien mukaan. Ne voidaan jakaa kolmeen yläluokkaan: julkiseen lohkoketjuun, rajattuun lohkoketjuun ja yksityiseen

lohkoketjuun. Kuten taulukossa 2 näkyy, julkiseen lohkoketjuun pääsevät käsiksi kaikki, rajattuun lohkoketjuun vaihtelevasti kaikki tai rajattu joukko ja yksityiseen lohkoketjuun vain erikseen rajattu joukko. Näillä lohkoketjuilla on myös muita eriäviä ominaisuuksia perustuen niiden jäsenten rajaukseen. (Zheng et al. 2016)

Taulukko 2. Julkisen, rajatun ja yksityisen lohkoketjun vertailu. (Zheng et al. 2016)

Ominaisuus	**Julkinen lohkoketju**	**Rajattu lohkoketju**	**Yksityinen lohkoketju**
Ylläpitäjät	Kaikki louhijat	Osa verkostosta	Yksi organisaatio
Lukuoikeus	Julkinen	Halutessa rajoitettu	Halutessa rajoitettu
Tietojen eheys	Vaikeasti vaarannettavissa	Mahdollisesti vaarannettavissa	Mahdollisesti vaarannettavissa
Tehokkuus	Matala	Korkea	Korkea
Hajautus	Hyvä	Kohtalainen	Heikko
Lupa ylläpitää	Kaikilla	Rajoitettu	Rajoitettu

Ajateltaessa lohkoketjuteknologiaa rahallisia transaktioita pidemmälle, voidaan huomata sen soveltuvan myös monen muun tyyppisen tiedon varastoimiseen tietoturvallisesti. Tällaisia asioita ovat esim. tuotteen seuranta, kuitti, potilastiedot ja muut henkilötiedot. Pystyäkseen hahmottamaan lohkoketjuteknologian erilaiset soveltuvuudet, täytyy siis hallita mm. julkisen ja yksityisen avaimen konsepti, salaustekniikat, p2p-transaktiot, hajautetut ja keskitetyt järjestelmät ja lohkoketjutilit. (Swan 2015, XI, s. 28)

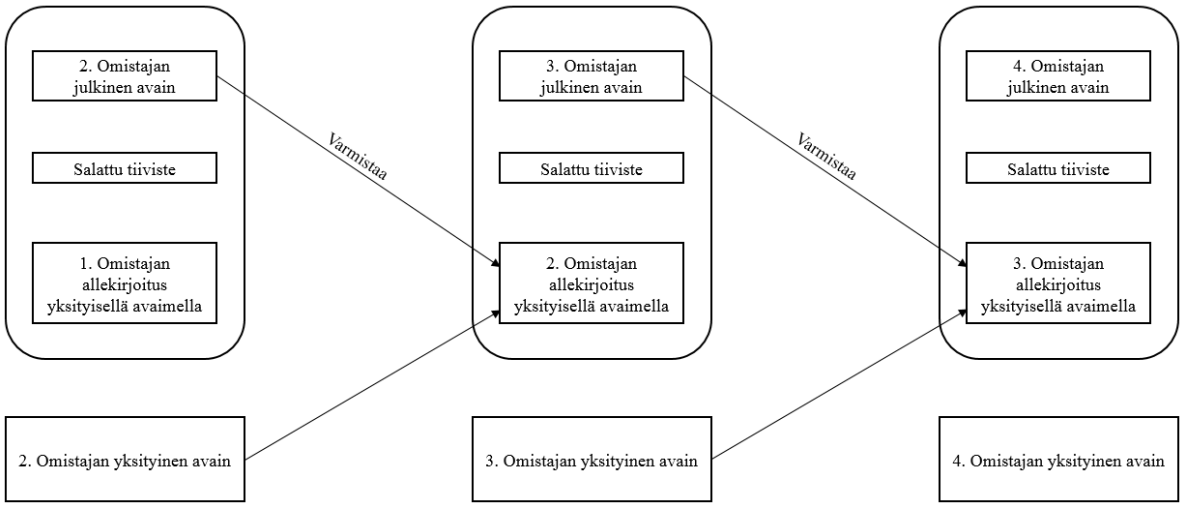
3.2 Lohkoketjuteknologian toiminta Bitcoinin avulla

Yksi lohkoketjuteknologian tärkeimmistä sovelluskohteista on viime vuosina ollut erilaiset kryptovaluutat, joista ensimmäisenä ja toistaiseksi markkina-arvoltaan isoimpana on Bitcoin. Bitcoinin toiminta perustuu vertaisverkkoon, joka oli jo vuonna 2013 noin 250 kertaa suurempi laskentateholtaan kuin maailman 500 nopeinta supertietokonetta yhdessä (Mattila & Seppälä 2015, s. 8). Tähän verkostoon kuuluu Bitcoinin käyttäjiä ympärimaailmaa ja se yhdistää käyttäjien koneet yhteiseen tietoverkkoon ja tätä kautta suojaa Bitcoinia yhdistetyllä laskentatehollaan. Bitcoin pyrkii ratkaisemaan bysanttilaisen kenraalien ongelman ilman

kolmannen osapuolen apua. Louhijat saavat antamastaan laskentatehostaan palkkion Bitcoineina, joka toimii motiivina verkostoon liittymiselle (Nakamoto 2008).

Bitcoinia voidaan käyttää ja vastaanottaa kuten normaalia valuuttaa vaihdannan välineenä lompakko-sovelluksella. Sovelluksen saa ladattua puhelimeen ja tietokoneelle tai vaihtoehtoisesti Bitcoineja voi siirtää ilman lompakko-sovellusta myös internet-selaimella. Bitcoinin turvaamiseksi tarvitaan siis vertaisverkkoa ja luotettavuutta, mutta elektronisen maksun tekemiseen tarvitaan kryptograafinen tosite. Tämän tekemisessä ei ole tarvetta kolmannelle osapuolelle, joka normaalissa rahansiirrossa olisi pakollista. (Swan 2015, s. 8-9)

Jokaisessa Bitcoinin transaktiossa omistaja siirtää vertaisverkossa vastaanottajalle allekirjoittamalla omalla yksityisellä avaimella Bitcoinin hashin ja kohdistetaan vastaanottajan henkilökohtaiseen julkiseen avaimeen. Transaktion vastaanottaja vahvistaa tapahtuman ja tieto tallentuu uutena lohkona lohkoketjun loppuun. Ongelmalliseksi tässä muodostuu se, miten voidaan estää useammat transaktiot samalla Bitcoinilla, ettei sitä uudelleen käytetä toisessa rahansiirrossa saman omistajan toimesta. Normaalilla valuutalla siirtotapahtuma varmistettaisiin kolmannella osapuolella. (Nakamoto 2008) Kuvassa 4 on havainnollistettu Bitcoin-transaktioita.



Kuva 4. Bitcoinin transaktio (Nakamoto 2008)

Transaktion hashauksen jälkeen sille tehdään aikamerkintä. Tämä tarkoittaa sitä, että lohkoketjun jokaisessa lohkossa on myös lohkolle oma aikamerkintä. Tällä tavoin tietojen

oikeellisuus pystytään varmistamaan vertaisverkon avulla, jolloin samojen Bitcoinien uudelleenkäyttäminen ei ole mahdollista. (Swan 2015, s. 37-38)

Jokaista uutta lohkoa kohden muodostuu Bitcoineja yksikölle, joka on suorittanut transaktion hashauksen. Alun perin jokaista transaktiota (lohkoa) kohden sai transaktion louhija 50 BTC, mutta jokaista 210 000 louhittua lohkoa kohden määrä puolittuu. Yhden lohko luomiseen menee aikaa noin 10 minuuttia, jonka seurauksena voidaan laskea, että vuonna 2140 saavutetaan maksimi Bitcoinien määrässä, joka on 21 miljoonaa. (Meiklejohn et al. 2013, s. 128-129) Käytännössä louhimisesta tulee siis pitkällä aikavälillä vähemmän kannattavaa, kun Bitcoineja saa vähemmän suhteutettuna tehtyyn työhön.

3.3 Lohkoketjuteknologian jatkokehitys

Lohkoketjuteknologian saattaa mieltää tietynlaiseen kiteytettyyn teknologiaan, mutta se on vuosien saatossa muokkautunut siihen liittyvien teknologioiden ja pintautuvien käyttötarkoitustensa myötä. Lohkoketjuteknologia on karkeasti jaettu eri versioihin, joista ensimmäinen on lohkoketjuteknologia 1.0, joka käsittää teknologian käytön valuuttana. Paras esimerkki tällaisesta lohkoketjuteknologiasta on Bitcoin. Bitcoin ja muut lohkoketjuteknologia 1.0 käyttävät kryptovaluutat toimivat käytännössä kolmen tason avulla. Alin taso on itse lohkoketjuteknologia, joka on pohja näille valuutoille. Keskimmäinen taso on protokolla ja ohjelmisto, jonka avulla valuuttaa voidaan lähettää toiselta tililtä toiselle. Päällimmäinen kerros on itse kryptovaluutta, joita on erilaisia kuten Bitcoin, Litecoin tai Dogecoin. (Swan 2015, s. 10-13)

Lohkoketjuteknologia 2.0 kattaa teknologian laajemman käytön ja sisältää mm. älykkäät sopimukset ja älykkään omaisuuden. Pääideana on, että lohkoketjuteknologian hajautetun tilijärjestelmän avulla pystyttäisiin myös rekisteröimään, vahvistamaan ja siirtämään kaiken tyyppisiä sopimuksia ja omaisuutta. Tällaisesta lohkoketjuun talletetusta omaisuudesta käytetään nimitystä älykäs omaisuus (eng. ”smart property”) ja tätä älykästä omaisuutta hallinnoidaan taas älykkäiden sopimusten (eng. ”smart contracts”) avulla. (Swan 2015, s. 13-15)

Älykkään omaisuuden perus konsepti on, että kaikki omaisuuteen liittyvät transaktiot kirjataan lohkoketjuteknologiaan nojaavaan järjestelmään. Älykkään omaisuuden omistamisen

pääideana on sen lohkoketjuun rekisteröimisen lisäksi pääsy sen yksityiseen avaimeen. Tällaisia älykkäitä omaisuuksia voivat olla joko fyysiset tavarat kuten pyörä, talo, tietokone tai aineettomat hyödykkeet kuten osakkeet, varaukset tai tekijänoikeudet. Oman ideansa voisi esimerkiksi patentoimisen sijaan sisällyttää lohkoketjuun, jolloin idean keksijällä olisi aikaleimalla varustettu todiste olevansa idean keksijä. (Swan 2015, s. 16-17)

Joissain tapauksissa fyysisten laitteiden kontrollointi ja esineiden internet voisi jopa toimia pelkästään lohkoketjun avulla. Esimerkiksi älypuhelin voisi tunnistaa käyttäjänsä identiteetin lohkoketjuun kirjattuna. Voisi myös olla mahdollista, että erilaisiin oviin asennettaisiin sensorit, joiden avulla käyttäjä pystyisi pyytämään oven avausta. Älykkään sopimuksen avulla pystyttäisiin päättämään, avataanko ovi käyttäjälle hänen lohkoketjussa olevien tietojensa perusteella. (Swan 2015, s. 18-19)

Toimiakseen älykäs omaisuus tarvitsee viitekehykset siihen liittyvistä transaktioista. Tämä on pitkälti lähtökohta älykkäiden sopimusten synnylle. Lohkoketjuteknologiassa nämä älykkäät sopimukset ovat lähinnä tarvittavia transaktioissa, jotka tarvitsevat ostamisen ja myymisen lisäksi myös muita sopimusehtoja. (Swan 2015, s. 16) Älykkäät sopimukset ovat luonteeltaan koodille rakentuvia tietokoneohjelmia, vaikka osa älykkäistä sopimuksista sisältääkin jollain tasolla tavanomaisten sopimusten logiikkaa ja piirteitä. Älykäs sopimus voi myös kyetä esimerkiksi keräämään ulkopuolisista lähteistä tietoa ja prosessoimaan sitä tehdessään toiminnallisia ratkaisuja. Älykkäiksi sopimuksiksi voidaan luonnehtia myös sopimuksia muistuttavien ohjelmien lisäksi muita vastaavia lohkoketjussa suoritettavia ohjelmia. (Mattila & Seppälä 2015, s. 13)

Kolme tärkeää asiaa erottavat älykkäät sopimukset normaaleista sopimuksista: autonomia, omavaraisuus ja hajautus. Autonomia tarkoittaa, että sopimus pystyy toimimaan itsenäisesti sen lanseeraamisen jälkeen ilman sen liikkeellepanijan interaktiota. Omavaraisuus viittaa sopimuksen kykyyn tavallaan kerätä toiminnastaan palkkaa ja käyttää tätä palkkaa mm. laskentatehon ylläpitoon tai tiedonvarastointiin. Hajautus taas viittaa niiden ominaisuuteen toimia lohkoketjun tapaan koko sen verkostossa hajautetusti. (Swan 2015, s. 19)
Alkeellinen esimerkki älykkäästä sopimuksesta on tavallinen myyntiautomaatti, jossa transaktio perustuu automaatioon. Myyntiautomaatti pystyy toiminnallaan valvomaan tuotteen

transaktion oikeellisuutta ja siihen koodatut ohjeet pakottavat sen toteuttamaan transaktion sovituilla ehdoilla, lukuun ottamatta manuaalisia virheitä laitteen toiminnassa. (Mattila & Seppälä 2015, s. 13) Samaan tapaan älykkäiden sopimusten on pakko noudattaa niille asetetun koodin määräyksiä käsitellessään transaktioita (Swan 2015, s. 20).

Lohkoketjuteknologia 3.0 kattaa teknologian käytön oikeudenmukaisiin applikaatioihin, jotka menevät valuuttojen, ekonomian ja markkinoiden yli. Pääargumentti 1.0 ja 2.0 lohkoketjuteknologiassa oli taloudellinen hyöty ja kustannussäästöt luomalla luottamuksen osapuolien välille, mutta 3.0 painottuu enemmän hajautetun verkoston tuomiin hyötyihin ja täyden automatisoinnin tuomiin mahdollisuuksiin teknologian käytössä. (Swan 2015, s. 30)

Yksi tällaisista käyttösovelluksista on erilaisten verkkosivujen rekisteröinti lohkoketjuun. Tämä mahdollistaisi tiedon levityksen ilman valtioiden kontrollointia, kunhan vapaaehtoiset verkoston jäsenet ajaisivat hajautettua palvelinohjelmaa omilla laitteillaan. Yksi tällaisista sovelluksista on Namecoin, jonka osoitteet rekisteröidään ”bit”-päätteeseen. 2014 vuoden lopuilla näitä osoitteita oli rekisteröity noin 180 tuhatta, joista yhtenä esimerkkinä toimii wikileaks.bit. Päästäkseen näille sivuille, täytyy käyttäjän tietynlainen välityspalvelin ohjelma omalle laitteelleen. (Swan 2015, s. 30-31)

Lohkoketjuteknologia voisi myös mahdollisesti soveltua isojen tietomassojen (eng. ”big data”) käsittelyyn. Lohkoketjuteknologia voitaisiin parittaa tietomassojen ennustusohjelmien kanssa, jolloin mm. älykkäiden sopimusten avulla pystyttäisiin automatisoidusti tekemään päätöksiä tietomassojen ennustusten ja toteutumisten perusteella. Tällainen toiminta voisi säästää valtavia määriä työtunteja, sillä työtehtävät suorittaisi ihmisten sijaan hajautettu tietokoneverkosto. Lohkoketjuteknologia saattaa potentiaalisesti olla reitti vielä isompien tietomassojen keräämiseen ja hyödyntämiseen, kuin tietomassojen nykyaikaiset hallintamenetelmät mahdollistavat. (Swan 2015, s. 31-32)

4 LOHKOKETJUTEKNOLOGIA TIETOTURVASSA

Tässä osiossa perehdytään lohkoketjuteknologian tietoturvaominaisuuksiin ja tutkitaan sen soveltumista perinteisten tietoturvaratkaisujen rinnalle. Käsiteltäviä aiheita ovat lohkoketjuteknologian CIA-tietoturvaominaisuudet, sen skaalautuminen tiedonvarastoinnissa, taloudelliset vaikutteet, sovelletut tietoturvajärjestelmät sekä soveltuminen liiketoimintamallin mukaan.

4.1 Lohkoketjuteknologia perinteisten tietojärjestelmien rinnalla

Useimmat yritykset varastoivat erilaista tietoa relaatiotietokantoihin. Sujuvan liiketoiminnan suorittamiseksi ja tiedon eheyden turvaamiseksi tarvitaan tästä tiedosta yleensä monia eri kopioita. Nämä tietokannat ovat myös yleensä hyvin keskitettyjä ja niiden tieto on salaamatonta. (Brandon 2016) Tällä hetkellä jopa pilvipalveluihin nojaavat tietojärjestelmät ovat hyvin keskitettyjä. Tämä keskittyneisyys on yksi vaarantava tekijä niiden tietoturvalle. (Kshetri 2017a) Keskitetty tietojärjestelmä on hajautettua järjestelmää alttiimpi tahallisille ja tahattomille sen saatavuutta vaarantaville ulkopuolisille tapahtumille (Mullins 2002, s. 440).

Pääasiallisesti yrityksille syntyy kahdenlaista tietoa: pääasiallista tietoa ja transaktionaalista tietoa. Pääasiallinen tieto koostuu pääasiallisista tiedoista, kuten asiakkaiden tiedoista, tuotetiedoista, työntekijöiden tiedoista ja muista saman tyyppisistä tiedoista. Transaktionaalinen tieto koostuu lähinnä eri toiminnoista syntyvistä tiedoista, kuten ostotapahtumista ja muista operatiivisista toiminnoista. Transaktionaalista tietoa voidaan luokitella pääasiallisen tiedon mukaan ja niiden tietomurtojen vaikutukset voivat olla hyvin erilaisia. Tämän takia onkin tärkeää erottaa pääasiallinen ja transaktionaalinen tieto toisistaan. (Rainer & Prince 2016, s. 126)

Näille tiedoille voidaan luokitella suuruus, kerääntymisnopeus ja vaihtelevuus, jonka avulla niille voidaan määritellä paras säilöntätapa. Nykyajan tarve kerätä tietoa päätöksenteon tueksi on kerryttänyt yrityksille massiivisia, pääasiallisesti transaktionaalisia tietomääriä, joita kutsutaan big dataksi. (Brandon 2016) Big datalle ominaista on sen suuri määrä, kerääntymisnopeus ja vaihtelevuus (Rainer & Prince 2016, s. 133). Perinteiset relaatiotietokannat eivät ole loistaneet oikeastaan millään tiedonvarastoinnin alueella, eivätkä ne ole myöskään soveltuneet big datan varastointiin hyvin. Tämän takia monet organisaatiot

ovat alkaneet korvat perinteisiä relaatiotietokantoja uusilla NoSQL-tietokannoilla. (Brandon 2016)

NoSQL-tietokannat (Not only SQL) ovat suurien tietomäärien hallinnoimiseen suunniteltuja hajautettuja ei-relaatiotietokantoja. Alkujaan NoSQ-tietokannat suunniteltiin internet 2.0 sovelluksien massiivisten yhtäaikaisten käyttäjätoimintojen hallinnoimiseen. mm. Google, Amazon ja Facebook hyödyntävät NoSQL-tietokantoja niiden suurien tietomäärien hallinnoimiseen. (Moniruzzaman & Hossain 2013) Erityyppisten big datojen hallinnoimiseen on kehitetty erilaisia ohjelmistoja NoSQL-tietokantojen toiminnan tueksi. Lohkoketjuteknologia voidaan mieltää yhdeksi NoSQL-tietokannan tyyppiseksi hajautetuksi tietojärjestelmäksi. Lohkoketjuteknologia kirjailija, yrittäjä ja teoreetikko William Mougayar toteaa lohkoketjun olevan uusi tietojärjestelmä, joka tulee mullistamaan tiedon varastoinnin. (Brandon 2016)

4.2 Lohkoketjuteknologian CIA-ominaisuudet

tietojärjestelmän tietoturvaa mitataan sen CIA-ominaisuuksilla, joiden onnistunut toteutuminen takaa sen varastoiman tiedon turvallisuuden. Ollakseen tietoturvallinen, tulee järjestelmän turvata tiedon luottamuksellisuus, eheys ja saatavuus. Lohkoketjuteknologian luonne järjestelmällisenä, kryptattuna ja hajautettuna tiedonvarastoinnin välineenä asettaa sen potentiaaliseksi tietojärjestelmäksi CIA-ominaisuuksien turvaamiseen. (Brandon 2016)

Tiedon luottamuksellisuuden takaaminen herättää kysymyksiä organisaatioissa, jotka olisivat muuten kiinnostuneita lohkoketjuteknologiaan perustuvasta tietovarastoinnista. Teknologia on alun perin suunniteltu yleisen tiedon varastoimiseen, joten sen varastoiman tiedon luottamuksellisuus ei ole ollut merkittävä tekijä. (Piscini et. al. 2017, s. 5) Julkisen lohkoketjun sisältämä tieto on siis käytännössä näkyvissä kaikille halukkaille, joka asettaa ison ongelman sen käyttöön tiedonvarastoinnissa. Useat startup-yritykset kehittelevät kuitenkin yksityisiä lohkoketjuja, joita jaetaan vain valituille jäsenille käsiteltäviksi. (Heires 2016) Lohkoketjuteknologia kuitenkin tarjoaa vahvan kryptauksen sen sisältämille tiedoille, joka estää ulkopuolisia vaarantamasta sen tiedon luottamuksellisuutta. Tämä ominaisuus tekee siitä yhden haastajan mm. pilvipohjaiselle tietovarastoinnille, jossa mahdollisesti arkaluontoista tietoa varastoidaan ulkopuolisen tahon toimesta. (Aleidi et al. 2018) Lohkoketjuun voitaisiin

kirjata salatusti ihmisen tietoja, kuten passin, ajokortin, äänioikeuden tai muun vastaavan. (Swan 2015, s. 10) Esimerkiksi Kiinan valtion kokeilussa tallettaa sen kansalaisten tietoja lohkoketjuun huomattiin, että lohkoketjuteknologia soveltuu ominaisuuksiltaan erinomaisesti erilaisten henkilötietojen tallennukseen (Aleidi et al. 2018).

Eheyden takaaminen lohkoketjuun säilötyssä tiedossa on yksi sen vahvuuksista. Lohkoketjuteknologia käyttää hyväkseen hashausta, jonka avulla se myös varmistaa oikeiden transaktioiden pääsyn lohkoketjuun ja näin ollen pitää yllä tietojen eheyttä. Sen lohkojen tapa viitata aina edelliseen lohkoon alkulohkoa lukuun ottamatta, vahvistaa lohkon tietojen eheyttä. (Aleidi et al. 2018) Myös teknologian mahdollistama transaktioiden aikaleima lohkoihin parantaa tietojen eheyttä entisestään. Kryptovaluuttojen louhijat pyrkivät muodostamaan isoja louhintaryhmiä, jolloin yksi huolestuttavimmista uhista lohkoketjun tietojen eheyteen liittyen on 51% hyökkäys. Tällöin yli puolet lohkoketjun verkostosta olisi hallussa tietyllä taholla ja näin ollen lohkoketjuun pystyttäisiin syöttämään väärää tietoa. Varsinkin pienien lohkoketjujen tapauksessa tämä voisi olla erittäin suuri ongelma. (Swan 2015, preface VIII) Turvallisuusyritykset, kuten Kapesky Labs, ovat myös huolestuneita erinäisten tahojen mahdollisuudesta syöttää haittaohjelmia lohkoketjutransaktioihin (Heires 2016).

Lohkoketjuteknologia on luonnostaan hajautettu tietovarasto, jonka takia sillä ei ole yksittäistä heikkoa pistettä. Hajautuksella saavutettava saatavuuden lisäys edellyttää kuitenkin lohkoketjuverkoston hyvää ja tarpeeksi laajaa hajautusta. Se ei myöskään tarvitse ulkopuolista välittäjää, vaan tietojen lisäys onnistuu sen hashaus prosessin avulla. (Aleidi et al. 2018) Applied Blockchainin toimitusjohtaja Adi Ben-Ari sanoo teknologian yhtenä kulmakivenä olevan tämä ulkoisen osapuolen poisto. Tällöin tiedon saatavuus paranee, jolloin liiketoiminta saadaan nopeammaksi vähemmillä virheillä (Heires 2016). Myös Christian Brothers yliopiston professori Dan Brandonin näkemys lohkoketjuteknologian vahvuudesta tukee tätä ajatusta. (Brandon 2016)

Tietyt yritykset hyödyntävät lohkoketjuteknologiaa yrittäessään tehdä niiden tietoverkostosta vahvemman kyberhyökkäyksiä vastaan. Esimerkiksi verkkotunnuksia IP-osoitteiksi muuttavan järjestelmän tietoja voidaan säilöä lohkoketjuun, suojaten sitä paremmin palvelunestohyökkäyksiltä. Lohkoketjuteknologiaa voidaan hyödyntää transaktioiden

turvallisemmassa suorittamisessa verkostossa ilman keskitetyn verkoston serveriä. Tällöin myös tietojärjestelmän nopeus kasvaa transaktioiden ollessa turvallisia ja automatisoituja lohkoketjuun implementoitujen älykkäiden sopimusten avulla. Muun muassa teknologiayritys Huawei hyödyntää lohkoketjuteknologiaa tehdäkseen sen mobiiliverkosta vahvemman hyökkäyksiä vastaan. (Aleidi et al. 2018)

4.3 Skaalautuvuus lohkoketjun tiedonvarastoinnissa

Kuten aikaisemmin todettiin, yritykset hallinnoivat suuria määriä tietoa, joka johtaa myös siihen, että tiedon varastointiin käytettävällä tietojärjestelmällä tulisi olla kapasiteettia suurien tietomäärien hallinnoimiseen. Nämä nykyajan massiiviset tietomäärät pystytään nykyisillä menetelmillä tiivistämään tietyissä määrin tilan säästämiseksi. Tätä tiivistämistä ei kuitenkaan pystytä soveltamaan lohkoketjussa ilman sen tietoturvan ja siihen pääsyn heikentymistä. Lohkoketjun pidentyminen tiedon kertymisen myötä tekee sen hallinnoimisesta myös alati hankalampaa, joka kannustaa sen transaktioiden suorittamisen keskittämiseen. Tämä puolestaan huonontaa sen hajautusta ja näin ollen tekee sen alttiimmaksi 51% hyökkäyksille ja palvelunestohyökkäyksille. (Swan 2015, s. 82)

Lohkoketjuteknologian yksi ongelma on myös transaktioiden hidastuminen lohkoketjun kasvaessa. Esimerkiksi Bitcoinin transaktiolohkon luominen kestää jo noin 10 minuuttia, mikä on aivan liian kauan tehokkaalle välineelle transaktoiden luomiseen mm. nopeaa ja tarkkaa toimintaa vaativassa esineiden internetissä, jossa toimivat laitteet vuorovaikuttavat tietokannan kanssa jatkuvasti. (Tapscott & Tapscott 2016, s. 256) Bitcoinin maksimimäärä transaktioita sekunnissa on 7, joka on huomattavasti vähemmän kuin esimerkiksi VISA luottokortin transaktioiden määrä, joka saattaa yltää jopa 10 000 transaktioon sekunnissa ruuhka-aikoina. Tällöin olisi haastavaa käyttää pelkkää lohkoketjua tällaisten transaktioiden suorittamiseen. Tämä ongelma voidaan kuitenkin poistaa kasvattamalla lohkoketjun lohkojen kokoa, mutta se taas luo uusia haasteita lohkoketjun kokoon liittyen. (Swan 2015, s.82)

Tutkiessa Bitcoinin lohkoketjun skaalautuvuutta ja sen sopivuutta mm. esineiden internetin tietojärjestelmäksi saadaan vaikutelma, ettei sillä ole potentiaalia näillä osa-alueilla. Tarkasteltaessa lohkoketjuteknologiaa Bitcoinin lohkoketjua pidemmälle, voidaan kuitenkin huomata sen soveltuvuus esineiden internetin tietojärjestelmäksi. Itse lohkoketjuteknologian

skaalautuvuus, luotettavuus, tietojen salaus ja hajautus tekevät siitä erinomaisen kandidaatin mm. esineiden internetin tietojärjestelmäksi. (Aleidi et al. 2018) Sen hashaus-menetelmän skaalautuvuus tallennetun tiedon mukaan ja luonne skaalautuvana tiedon hallinnoijana tekee siitä varteenotettavan vaihtoehdon suuren tietojärjestelmän infrastruktuuriksi (Swan 2015, s. 95)

4.4 Taloudelliset tekijät lohkoketjuteknologian tietoturvajärjestelmässä

Vaikka siirtyminen lohkoketjuteknologiaan nojaavaan tietojärjestelmään parantaisikin sen sisältämän tiedon tietoturvaa, on myös oleellista huomioida minkälaisia kustannuksia tästä syntyisi. Isojen yritysten suosimat tavat tallentaa tietoa keskitetysti saattavat olla kalliita ja niiden implementointi saattaa viedä paljolti aikaa (Rainer & Prince 2016, s. 138). Toisaalta nykypäivän suosittu menetelmä tallettaa tietoa kolmannen osapuolen pilvipalveluun saattaa olla halvempaa, mutta siitä aiheutuvat riskit ja niiden realisoituminen voi lopulta tulla hyvinkin kalliiksi yritykselle. Pilvipalveluiden yleistyminen yritysten tiedonvarastoinnissa on tietoturvayritys McAfeen ennustusten mukaan yksi kasvavista haavoittuvaisuuksista kyberrikollisia vastaan (Nayak & Rao 2014 s. 156, 263).

Lohkoketjuteknologian perinteinen ongelma on sen vaatima työpanos lohkoketjun transaktioiden suorittamiseksi. Tämä työpanos taas puolestaan kuluttaa energiaa ja näin ollen maksaa transaktiota suorittavalle taholle. Tämä sama työpanos kuitenkin vaikeuttaa lohkoketjun transaktioiden väärentämistä ja näin ollen toimii yhtenä lohkoketjun tietoturvan takaajista. (Swan 2015, s. 83) Bitcoinin tapauksessa useat eri tahot ovat kehitelleet yhä parempia laitteita sen louhimiseen, jolloin voidaan myös olettaa teknologian kehittyvän paremmaksi myös erilaisten lohkoketjujen ylläpidossa (Tapscott & Tapscott 2016, s. 260). Tämä energiaa kuluttava työpanos transaktioiden luomiseksi ja lohkoketjun tietoturvan vahvistamiseksi rajoittuu kuitenkin paljolti vanhoihin ”Proof of Work” –menetelmää hyödyntäviin lohkoketjuihin, kuten Bitcoiniin. Muihin tarkoituksiin suunnitellut lohkoketjut yleensä hyödyntävät toisenlaisia menetelmiä saavuttaakseen transaktioiden uskottavuuden, jolloin myös niiden energian kulutus on paljolti pienempi. (Zheng et al. 2016)

Vaikka lohkoketjun ylläpitäminen kuluttaisikin enemmän energiaa kuin perinteiset tietovarastot, löytyy yksi sen taloudellisista vahvuuksista aivan muualta. Nimittäin

lohkoketjuteknologian ominaisuus poistaa kolmas osapuoli transaktioista saattaa tuoda huomattavia säästöjä kolmannen osapuolen maksujen, viiveen ja potentiaalisten riskien poistumisen myötä. (Brandon 2016) Banco Santanderin tekemän tutkimuksen mukaan lohkoketjuteknologiaan siirtyminen voisi vähentää pankkien infrastruktuurin, sovittelun ja vastapuolen kustannuksia jopa 20 miljardia dollaria vuodessa vuoteen 2022 mennessä. (Heires 2016)

Keskitetty tietojärjestelmä on haavoittuvaisempi erilaisille palvelunestohyökkäyksille ja muille sen tiedon saatavuutta vaarantaville tapahtumille. Tästä syystä hajautettu lohkoketju on tältä osin keskitettyä tietojärjestelmää kustannustehokkaampi vaihtoehto. Tiedon saatavuus on yritykselle tärkeimmistä asioista, sillä ilman tiedon saatavuutta tietojärjestelmien sovellukset eivät kykene toimimaan, jolloin yrityksen liiketoiminta kärsii. Globaalisti toimivilla yrityksillä ei ole varaa pitää taukoa liiketoiminnastaan, sillä jossain päin maailmaa on aina paras aika kuluttaa yrityksen palveluja. (Mullins 2002, s. 217)

4.5 Lohkoketjuteknologian tietoturvajärjestelmät

Tietoturvajärjestelmiä käsiteltiin enemmän kappaleessa 2.8, jossa kerrottiin, kuinka tietoturvajärjestelmien kehitystyö on jatkuva prosessi. Samalla tavalla tietoturvajärjestelmään voidaan kehitystyön mukana tuoda lohkoketjuteknologiaa osaksi sitä, jos yrityksessä nähdään sen olevan varteenotettava ratkaisu. Toistaiseksi lohkoketjuteknologia on vielä uusi ilmiö, jonka seurauksena esimerkkitapauksia on vaikeaa löytää. Mahdollisesti tulevaisuudessa lohkoketjuteknologia on osa suurten yritysten tietoturvajärjestelmiä, koska teknologialla on kiistatta etunsa muihin malleihin nähden.

Yritykset ovat ymmärtäneet, etteivät julkiset pilvipalvelut ole ratkaisu kaikkeen tiedon varastointiin. Ne toimivat hyvänä tietovarastona big data –tyyppiselle tiedolle, joka sisältää paljon vähäarvoista tietoa. Lohkoketjuteknologia voisikin toimia juuri pilvipalvelimien rinnalla tai syrjäyttäjänä. Teknologioissa on paljon yhtäläisyyksiä niin tietoturva kuin yksityisyys kysymyksissä, koska molemmat ovat kehitelty tarjoamaan kustannustehokkaita ratkaisuja tietoturvaan. Tavallaan myös eri käyttöönottomallit pilvipalvelemien ja lohkoketjuteknologian kanssa toimivat vertailukelpoisina, molemmilla on avoimet mallit sekä yksityiset ja kahden mallin välimallit. Lisäksi molemmat mallit ovat suojattu salauksella. Alla olevassa taulukossa

3 on vertailtu ostetun pilvipalvelu- ja lohkoketjumallin yhtäläisyyksiä ja eroavaisuuksia tietoturvan kannalta. (Kshetri 2017a)

Taulukko 3. Pilvipalveluiden sekä lohkoketjuteknologian vertailu (Kshetri 2017a)

	Pilvipalvelu	Lohkoketju
Käyttöönottomallit	Yksityinen, yhteisö, julkinen ja hybridi	Yksityinen, rajattu ja julkinen
Kustannustehokkuus	Maksetaan resurssien käytöstä palveluntarjoajalle käytön mukaan	Ei tarvetta kolmannelle osapuolelle tiedonvarastoinnissa
Tietoturvan vahvistamismenetelmiä	Salaus Zero trust –politiikka	Salaus Julkisella ja yksityisellä avaimella varmistetaan, että tiedon vastaanottaa oikea kohde
Suurimpia haasteita	Moni pilvipalvelu käyttää palomuureja, joilla valvotaan sekä hallinnoidaan verkkoliikennettä. Hyökkääjät yleensä löytävät keinon ohittaa palomuurin.	Teknologian uutuuden vuoksi se ei ole vielä laajamittaisessa käytössä eikä testattu, pimennyshyökkäykset

Toinen mahdollinen lohkoketjuteknologian lähitulevaisuuden sovellus voisi liittyä esineiden internetiin. Liitteessä 4 on pyritty taulukolla havainnollistamaan nykymallin sekä mahdollisen lohkoketjumallin eroja. Esineiden internetillä on ollut pitkään ongelma, koska se on perustunut keskitettyihin malleihin. Valmistajan kannalta keskitetyillä malleilla on ollut suuret ylläpitokustannukset, koska ylläpitopäivityksiä jaetaan mahdollisesti miljoonille laitteille. Osa näistä laitteista ovat jo pois käytöstä, mutta silti rasittavat suuren verkoston ylläpitoa. (Christidis & Devetsikiotis 2016)

Nykyistä mallia paremmin voisi toimia lohkoketjuteknologian avulla kehitelty ratkaisu. Esimerkiksi voisimme olla tilanteessa, jossa yhden valmistajan kaikki esineiden internet –

laitteet toimivat samassa lohkoketjussa. Lohkoketjun avulla valmistaja voi älykkäiden sopimusten avulla automaattisesti päivittää laitteistoa. Älykkäät sopimukset tulevat lohkoketjun kautta tai erillisen latauspalvelun kautta laitteiden tietoon. Päivitys lähtee valmistajan yksiköstä, joka on lohkoketjussa, mutta päivityksen siirryttäessä lohkoketjussa useammalle ei lähettävää yksikköä enää käytännössä tarvita. Tämän kaltaista mallia voitaisiin soveltaa esimerkiksi toimitusketjun seurannassa, jossa laitteet automaattisesti seuraavat tavaraliikennettä ja keräävät tietoa. (Christidis & Devetsikiotis 2016)

Tällä hetkellä esineiden internet on pitkälti keskitetyssä pilvipalvelumallissa. Lohkoketjun avulla voitaisiin toteuttaa malli, joka toimii hajautetusti. Hajautetussa mallissa esineiden internettiin kuuluvat laitteet pystyisivät keskustelemaan keskenään salauksen kanssa, jakamaan tehokkaasti tietoa sekä toimimaan automaattisesti älykkäiden sopimusten avulla. Pilvipalvelumalli on haavoittuvaisempi hyökkäyksille kuten palvelunestohyökkäys, koska järjestelmässä on heikkoja kohtia. Sen sijaan hajautetussa lohkoketjussa ei ole samanlaisia solmukohtia ja identtistä tietoa on tallennettuna useammassa, kunhan lohkoketjuun lisätty tieto pysyy oikeanlaisena. Valvomisella tapahtumaa voidaan pyrkiä ehkäisemään – ainakin sen vaikutuksia. Alla olevassa taulukossa on pyritty tiivistämään ja selventämään esineiden internetin nykymallin sekä mahdollisen lohkoketjuun perustuvan mallin eroja. (Kshetri 2017b)

Liite 4 kiteyttää nykyisen esineiden internet –mallin ongelmat ja näihin vastaavat lohkoketjuteknologian avulla toteutettavat ratkaisut. Suuria huolenaiheita ovat esimerkiksi kolmannen osapuolen pilvipalveluiden huoltokatkot ja sensoreiden kerryttämän tiedon eksponentiaalinen kasvu tulevaisuudessa. (Kshetri 2017a, Kshetri 2017b)

4.6 Lohkoketjuteknologian soveltuvuus yritysten tietoturvaan

Lohkoketjuteknologialla on havaittu olevan niin hyviä, kuin huonojakin puolia sovellettaessa sitä yritysten tietoturvan parantamiseen. Teknologian soveltuvuutta voidaan arvioida kiteyttämällä sen vahvuudet, heikkoudet, uhat ja mahdollisuudet yritysten tietoturvan hyväksi tekemällä sille SWOT-analyysi (Pickton & Wright 1998).

Taulukko 4. SWOT-analyysitaulukko lohkoketjuteknologiasta

Vahvuudet	**Heikkoudet**
• Parantaa varastoidun tiedon saatavuutta hajautetulla arkkitehtuurilla • Ylläpitää varastoidun tiedon luottamuksellisuutta tarjoamalla vahvan salaustekniikan varastoidulle tiedolle • Vaihtelevia lohkoketjuja sopien tiettyihin tarkoituksiin • Tiedon talletustapa tukee tiedon eheyttä • Poistaa kolmannen osapuolen tietojen käsittelystä	• Energiankulutus mahdollisesti liian suuri • Saattaa viedä valtavasti enemmän talletustilaa • Lohkoketjun kasvaessa sen käyttö saattaa hidastua jopa liikaa • Teknologian monimutkaisuus voi vaikeuttaa käyttöä ja virheiden korjausta järjestelmässä • Tallennettu tieto vaikeampaa tiivistää kuin perinteisissä menetelmissä
Mahdollisuudet	**Uhat**
• Pilvipalveluiden korvaus lohkoketjuteknologiaan pohjautuvalla arkkitehtuurilla • Soveltuvuus turvallisempaan big datan hallinnointiin • Hyvä soveltuvuus fyysisten tietoturvalaitteiden tietojärjestelmäksi • Älykkäiden sopimusten mahdollisuudet tietoturvan ylläpidon helpottamiseksi • Uusia käyttökohteita pintautuu teknologian kehittyessä	• Ulkopuolisten lähteiden tuottama tieto voi olla huonolaatuista ja sitä ei päästä muokkaamaan jälkikäteen • Tietyt pienet lohkoketjut alttiita mm. 51% hyökkäyksille • Uudet kehittyvät hyökkäykset mm. tietojen saatavuuden vaarantamiseksi

Voidaan siis huomata, että lohkoketjuteknologia tukee kaikkia kolmea tietoturvan CIA-ominaisuutta ja sen käyttömahdollisuudet fyysisten tietoturvalaitteiden kanssa ovat laajat. Sillä on kuitenkin tiettyjä heikkouksia käytännöllisyyteen liittyen, jolloin siihen liittyvien kustannusten tarkasteleminen on todella oleellista. Teknologia on myös varsin uutta, joten sille saattaa tulevaisuudessa pintautua vielä pahojakin uhkia, mutta toisaalta myös mahdollisuuksia saattaa pintautua.

Näiden ominaisuuksien valossa voidaan päätellä, että lohkoketjuteknologia sopisi hyvin esimerkiksi sellaisen tiedon taltioimiseen, jonka tietomurrosta aiheutuvat kustannukset olisivat yritykselle suuret. Liitteestä 4 voidaan nähdä tällaisen tiedon olevan mm. terveyteen ja rahoitukseen liittyvää tietoa. Mikäli ajatellaan maantieteellisiä ominaisuuksia, olisi se hyvä käyttökohde pääasiassa mm. Yhdysvalloissa tai Kanadassa toimiville yrityksille. Kuten liitteestä 2 voidaan nähdä, näissä maissa toimiville yrityksille koituu eniten kustannuksia, mikäli niiden tietojen tietoturva vaarantuu. Teknologia soveltuu myös liiketoimintamallista riippumatta hyvin transaktionaalisen tiedon taltioimiseen. Se soveltuu myös ominaisuuksiltaan hyvin fyysisten tietoturvalaitteiden tietojärjestelmäksi poistamalla kolmannen osapuolen riskit tietoturvalaitteiden toiminnan vaarantumisesta.

Lohkoketjuteknologian adaptointi osana yrityksen tietoturvaa voi olla kuitenkin haasteellista yrityksille. Mikäli yritys on pieni, voi sen olla vaikeaa ylläpitää tarpeeksi laajasti hajautettua lohkoketjua mahdollisten hyökkäysten torjumiseen. Yrityksen tulee olla myös tietoinen, kuinka paljon se tarvitsee tietotaitoa siirtyäkseen käyttämään tätä varsin uutta teknologiaa, ja sen jälkeen tehdä arvio siihen siirtymisen kannattavuudesta. Ideaalisesti lohkoketjuteknologiaa hyödyntävät tietovarastot ja tietoturvasovellukset kehittyisivät pilvipalveluiden tavoin, jolloin niiden implementointi olisi vaivattomampaa ja yritys pystyisi keskittymään paremmin omaan ydinosaamiseensa tietoturvan sijaan. (Swan 2015, s. 17-20)

5 JOHTOPÄÄTÖKSET

Kandidaatin työn tutkimus jakautui pääasiassa kolmeen osioon: tietoturvaan, lohkoketjuteknologiaan ja näiden kahden yhdistämiseen. Vaikka tutkimuskysymykset suuntautuivat lähinnä lohkoketjuteknologian käyttöön tietoturvassa, oli oleellista käsitellä aluksi näitä aiheita erikseen ja sen jälkeen vasta muodostaa niistä yhtenäinen kokonaisuus. Työn aihetta lähestyttiin kolmella tutkimuskysymyksellä, joista ensimmäinen tutkimuskysymys oli

1. Millä tavoin lohkoketjuteknologian avulla voidaan parantaa yritysten tietoturvaa?

Tietoturvaa tarkasteltiin tässä työssä tiedon luottamuksellisuuden, eheyden ja saatavuuden kannalta. Lohkoketjuteknologia tarjoaa erinomaiset puitteet näiden kolmen ominaisuuden turvaamiseen tiedonvarastoinnissa.

Tallennettaessa tietoa lohkoketjuun se voidaan helposti salata käyttäen sille ominaisia erilaisia hashaus –algoritmeja. Tällöin se tukee hyvin tiedon luottamuksellisuutta, sillä ulkopuolisten päästessä käsiksi tietoon on se heille salatussa muodossa. Myös lohkoketjuteknologian ominaisuus poistaa kolmas osapuoli tiedon käsittelystä parantaa sen tietojen luottamuksellisuutta.

Lohkoketjuteknologia tarjoaa myös hyvin eheyttä tukevan tavan dokumentoida tietoa sen lohkoihin. Jokaisessa lohkossa on aikaleima ja lohkot ovat linkitetty toisiinsa näiden aikaleimojen avulla, jolloin tieto säilyy eheänä. Tietoja ei myöskään pääse jälkikäteen muokkaamaan, jolloin voidaan varmistua jo tallennettujen tietojen eheydestä perinteisiä menetelmiä helpommin. Luonnostaan hajautettuna järjestelmänä lohkoketjuteknologia tukee tiedon saatavuutta. Lisäksi sen ominaisuus poistaa kolmas osapuoli tiedon käsittelyyn liittyvissä prosesseissa, parantaa tiedon saatavuutta yleisesti käytettyihin pilvipalveluihin verrattuna pysyen kuitenkin mahdollisesti kustannustehokkaampana vaihtoehtona omille tietovarastoille.

Lohkoketjuteknologia soveltuu myös hyvin esineiden internetin tapaisten manuaalisten tietoturvajärjestelmien tietokannaksi. Se vähentää manuaalisen tietoturvajärjestelmän toimimattomuuden riskejä eliminoimalla kolmannen osapuolen tietovarastojen käyttöön

liittyvät riskit mm. niiden tietojen saatavuuteen ja eheyteen liittyen. Myös teknologiaan liitettävien älykkäiden sopimusten avulla on mahdollista vähentää mm. inhimillisiä virheitä ja näin ollen parantaa yrityksen tietoturvaa.

Työssä käsiteltiin myös minkälaista tietoa eri yritykset tallentavat ja miten eri tietotyypit vaikuttavat yrityksen tarpeeseen suojella tietoa. Vaikka lohkoketjuteknologia tarjoaisikin tietoturvan eri ominaisuuksiin parannuksia, on silti oleellista tietää, minkä tyyppisen tiedon tallentamiseen se soveltuu. Tähän asiaan perehtyvä toinen tutkimuskysymys oli

2. Minkä tyyppisen tiedon varastointi lohkoketjuun on kannattavaa?

Tieto voidaan jakaa eri tyyppeihin perustuen sen vaatimiin tietoturvaominaisuuksiin yrityksen mielestä. Nämä tietoturvaominaisuuksien vaatimukset on yleensä sidottu yritykselle aiheutuneisiin vahinkoihin sen toiminnassa, varoissa ja yksilöissä, mikäli jokin tiedon tietoturvaominaisuuksista vaarantuu. Tunnistettaessa näiden vahinkojen vakavuus, voidaan eri tietotyypeille tehdä omat tietoturvaluokituksensa. Näillä tietotyypeillä oli myös kaksi pääasiallista yläluokkaa: pääasiallinen ja transaktionaalinen tieto. Pääasiallisen tiedon tietoturvaluokitus on yleensä suurempi kuin transaktionaalisen tiedon.

Lohkoketjuun tallennetun tiedon saatavuus on todettu olevan erinomainen, minkä takia tätä tietoturvan ominaisuutta vaativia tietoja on kannattavaa tallettaa lohkoketjuun. Se tukee myös erinomaisesti tiedon eheyttä, minkä takia hyvää eheyttä vaativia tietoja on kannattavaa varastoida lohkoketjuun. Toisaalta siihen varastoituja tietoja ei pysty enää muokkaamaan, joten toistuvasti korjaamista vaativan tiedon talletus kannattaa jättää pois lohkoketjusta.

Vaikka lohkoketjuteknologia tukeekin hyvin tiedon luottamuksellisuutta tiedonvarastoinnissa, täytyy miettiä, onko siihen järkevää tallettaa yrityksen kriittisintä tietoa. Esimerkiksi tietoa, jonka luottamuksellisuuden tai eheyden vaarantuminen olisi katastrofaalista yritykselle, ei kannata taltioida laajasti hajautettuun lohkoketjuun.

Lohkoketjuteknologia on myös ominaisuuksiltaan verrattavissa hajautettuun NoSQL-tietokantaan. Tämä tarkoittaa, että lohkoketjuun on kannattavaa myös varastoida

transaktionaalisesta tiedosta koostuvaa big dataa. Myös kolmannen osapuolen varastoimiksi sopimattomien tietotyyppien varastoiminen mm. yrityksen sisäisesti ylläpidettävään lohkoketjuun voi olla kannattavaa.

Työssä keskityttiin paljolti tietotekniikkaa käsitteleviin asioihin, kuten tietoturvaan ja lohkoketjuteknologiaan. Tarkoituksena oli kuitenkin tutkia mitä hyötyä yritykselle olisi lohkoketjuteknologian mahdollistaman tietoturvan lisäyksestä. Tästä syystä kolmas tutkimuskysymys oli

3. Miten lohkoketjuteknologian käytöstä saavutettu tietoturvan lisäys parantaa yrityksen kannattavuutta?

Tietoturvaa voidaan pitää osana yrityksen kannattavaa liiketoimintaa ja mission tukijana. Puutteellinen kyky noudattaa ja implementoida sopivia tietoturvan säännöksiä johtaa useimmiten yrityksen puutteelliseen kykyyn tehdä liiketoimintaa ja toteuttaa sen missiota. Tämän takia tietoturvan lisääminen yrityksessä parantaa myös kannattavuutta.

Lohkoketjuteknologian avulla saavutettu tiedon saatavuuden lisäys parantaa yrityksen mahdollisuutta tehdä liiketoimintaa vähentämällä palveluiden katkeamista. Tämä puolestaan vaikuttaa myös osiltaan yrityksen imagoon ja lisää sen kannattavuutta pitkällä aikavälillä. Lohkoketjuteknologian avulla saavutettu lisäys tietoturvaan kolmannen osapuolen poistamisella lisää yrityksen kannattavuutta mm. poistamalla kolmannen osapuolen tietoturvariskit liittyen tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen.. Tämän avulla saavutettu mm. paranneltu tietojen saatavuus nopeuttaa yrityksen prosesseja ja näin ollen parantaa sen kannattavuutta. Tämän vaikutukset kannattavuuteen voidaan huomata mm globaalisti toimivilla yrityksillä, joissa tiedon nopea ja ympärivuorokautinen saatavuus on tärkeää johtuen yrityksen palvelujen jatkuvasta kulutuksesta kellonajasta riippumatta.

Lohkoketjuteknologiaan liitettävät älykkäät sopimukset tarjoavat myös mahdollisuuksia joidenkin prosessien automatisointiin vähentämällä sekä inhimillisten virheiden aiheuttamia kustannuksia että manuaalisesta työstä aiheutuvia kuluja. Lohkoketjuteknologian avulla

pystytään myös luomaan paremmin toimiva manuaalisia tietoturvajärjestelmiä ja vähentämään siten niiden ylläpidosta ja mahdollisista häiriöistä aiheutuvia kustannuksia.

Siirtymällä lohkoketjuteknologiapohjaisien tietojärjestelmien käyttöön voi yritys parantaa sen kannattavuutta etenkin pitkällä aikavälillä. Tällöin yrityksen tietomurrot ja niistä aiheutuvat kustannukset vähenisivät pitkällä aikavälillä yrityksen panostaessa lohkoketjuteknologiaan nojautuvan tietojärjestelmän käyttöönottoon pitkällä aikavälillä. Tästä seuraisi yritykselle aluksi lyhytvaikutteisia kustannuksia, joiden vaikutteet kumottaisiin kuitenkin pitkällä aikavälillä saavutettavien kustannusten vähennysten avulla.

Tutkimusta tehdessä huomattiin kuinka laajasti lohkoketjuteknologia ja sen sovelluskohteet ovat kehittyneet vain muutaman vuoden kuluessa. Yksi esille nousseista erinomaisista soveltuvuuksista lohkoketjuteknologialle oli sen käyttö esineiden internetin tietokantana. Tästä syystä mielenkiintoinen jatkotutkimuskohde voisi olla esimerkiksi lohkoketjuteknologian yhdistäminen esineiden internetin toimintaan.

6 LÄHTEET

Abeyratne, S.A. & Monafred R.P. 2016. Blockchain ready manufacturing supply chain using distributed leder. Internation Journal of Research in Engineering and Technology. Vol. 5, nro. 9, s. 1-10.

Aleidi, A., Albesher, A. & Al-Akhras, M. 2018. Using Blockchain Technology to Validate the Integrity and Confidentiality of Backups Versions on the Cloud. General Cybersecurity Conference.

Almorsy, M., Grundy, J & Ibrahim, A.S. Collaboration-Based Cloud Computing Security Management Framework. 2011. IEEE 4th International Conference on Cloud Computing. s. 364-371.

Blakley, B., McDermott, E. & Geer, D. 2001. Information Security is Risk Management. Proceedings of the 2001 workshop on New security paradigms. s. 97-104.

Botta, A., de Donato, W., Persico, V. & Pescapé, A. 2015. Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems. Vol 56, s. 684-700.

Bowen, P., Hash, J. & Wilson, M. 2006. Information Security Handbook: A Guide for Managers. Gaithersburg, National Institute of Standards and Technology. S.135

Bradbury, D. 3.2015. In blocks we trust. Engineering & Technology. Vol. 10, nro. 2, s. 68-71.

Brandon, D. 2016. The Blockchain: The Future of Business Information Systems? International Journal of the Academic Business World. Vol. 10, nro. 2, s. 33-40.

Bulgurcu, B., Cavusoglu, H. &. Benbasat, I. 2010. Information security police compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. Vol. 34, nro. 3, s. 523-548.

Cavusoglu, H., Mishra, B. & Raghunathan S. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce. Vol 9, nro 1. s. 70-104.

Christidis, K & Devetsikiotis, M. 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access. Vol. 4. S. 2292-2303

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A. & Sassone, V. 2017. Blockchain-based database to ensure data integrity in cloud computing environments. ITA-SEC. Vol. 1816.

Goldberg, S., Heilman, E., Kendler, A. & Zohar, A. 2015. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. Proceedings of the 24th USENIX Security Symposium.

Gordon L.A. & Loeb, M.P. 2002. The Economics of Information Security Investment. ACM Transactions on Information and System Security. Vol. 5, nro. 4, s. 438-457.

Heires, K. 2016. The Risks and Rewards of Blockchain Technology. Risk Management; New York. Vol. 63, nro. 2, s. 4, 6-7.

Huckle, S., Bhattacharya, R., White, M. & Beloff, N.2016. Internet of Things, Blockchain and Shared Economy Applications [verkkodokumentti]. [viitattu 18.2.2018]. Saatavissa:

Kavitha, V. & Subashini, S. 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. Vol 34, nro 1, s. 1-11.

Ko, M. & Dorantes, C. 2006. The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation. Journal of Information Technology Management. Vol 17, nro 2, s. 13-22.

Kshetri, N. 2017a. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy forthcoming. Vol 41, nro 10, s. 1027-1038.

Kshetri, N. 2017b. Can Blockchain Stregthen the Internet of Things? IT Professional. Vol 19, nro 4, s. 68-72.

Lamport, L. Shostak, R. & Pease, M. 1982. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. Vol. 4, nro. 3, s. 382-401.

Lauslahti, K., Mattila, J. & Seppälä, T. 12.9.2016. Älykäs sopimus – Miten blockchain muuttaa sopimuskäytäntöjä? [verkkodokumentti]. [viitattu 16.2.2018]. Saatavissa: https://www.researchgate.net/profile/Timo_Seppaelae3/publication/308022606_Smart_Contracts_-_How_will_Blockchain_Technology_Affect_Contractual_Practices/links/57d6f3fd08ae0c0081ea7e33/Smart-Contracts-How-will-Blockchain-Technology-Affect-Contractual-Practices.pdf

Li, S., Tryfonas, T. & Li, H. 2016 The Internet of Things: a security point of view. Internet Research. Vol. 26, nro. 2, s. 337-359.

Li, X., Jiang, P., Chen, T., Luo, X. & Wen, Q. 2017. A survey on the security of blockchain systems. Future Generation Computer Systems.

Mattila, J. & Seppälä, T. 2015. Laitteet pilveen – vai pilvi laitteisiin? Keskustelunavauksia teollisuuden ja yhteiskunnan digialustojen uusista kehitystrendeistä. ETLA Raportit No 44. [Verkkodokumentti]. [Viitattu 15.2.2018]. Saatavissa: https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-44.pdf

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D. Voelker, G.M. & Savage, S. 2013. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Proceedings of the 2013 conference on Internet measurement conference, s. 127-140.

Moniruzzaman, A. B. M. & Hossain, S. A. 2013. NoSQL Database: New Era of Databases for Big Dara Analytics – Classification, Characteristics and Comparison. International Journal of Database Theory and Application. Vol. 6, nro. 4.

Mullins, C. 2002. Database Administration: The Complete Guide to Practices and Procedures. First edition. Addison Wesley. [E-kirja].

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. [Verkkodokumentti]. [Viitattu 14.2.2018]. Saatavilla https://bitcoin.org/bitcoin.pdf

National Institute of Standards and Technology. 2011. The NIST Definition of Cloud Computing. [www-dokumentti]. [Viitattu 9.4.2018]. Saatavissa: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

National Institute of Standards and Technology. 1995. An Introduction to Computer Security: The NIST Handbook [verkkodokumentti]. [Viitattu 10.3.2018]. Saatavissa: http://www.davidsalomon.name/CompSec/auxiliary/handbook.pdf

National Institute of Standards and Technology. 2004. Standards for Security Categorization of Federal Information and Information Systems. [WWW-dokumentti]. [Viitattu 12.3.2018]. Saatavissa: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Nayak, U. & Rao, U.H. 2014. The InfoSec Handbook: An Introduction to Information Security. New York, Apress Media.

Nieles, M., Dempsey, K. & Pillitteri, V.Y. 2017 National Institute of Standards and Technology Special Publication 800-12 Revision 1. An Introduction to Information Security. [WWW-dokumentti]. Saatavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Patterson, D.A. 2002. A Simple Way to Estimate the Cost of Downtime. 16th Systems Administration Conference. S. 185-188.

Pickton, D. W. & Wright, S. 1998. What's swot in strategic analysis? Strategic Change. Vol. 7, s. 101-109.

Piscini, E., Dalton, D & Kehoe, L. Blockchain & Cyber Security. 4.2017 [WWW-dokumentti. [viitattu 17.2.2018] Saatavissa: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf

Ponemon Institute & IBM Security. 2017. 2017 Cost of Data Breach Study. [verkkodokumentti]. Saatavissa: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Probst, C.W., Hunker, J., Bishop, M. & Gollmann, D. 2010. Insider Threats in Cyber Security. London, Springer.

Quinn, B. & Arthur, C. The Guardian. 26.4.2011. PlayStation Network hackers access data of 77 million users. [Verkkosivu]. [Viitattu 10.3.2018]. Saatavissa: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Rainer, R.K.Jr. & Prince, B. 2016. Introduction to Information Systems: Supporting and Transforming Business. USA, Wiley. [e-kirja]

Siponen, M.T. & Oinas-Kukkonen, H. 2007. A Review of Information Security Issues and Respective Research Contributions. The DATA BASE for Advances in Information Systems. Vol. 38, nro. 1, s. 60-80.

Swan, M. 2015. Blockchain: Blueprint for a New Economy. Sebastopol, O´Reilly Media.

Tanenbaum, A.S. & Van Steen, M. 2007. Distributed Systems: Principles and Paradigms. New Jersey, Pearson.

Tapscott, D. & Tapscott, A. 2016. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin. [e-kirja]

Tassi, P. Forbes Tech. Sony Pegs PSN Attack Costs at $170 million, $3.1B Total Loss for 2011. 23.5.2011. [Verkkosivu]. [Viitattu 10.3.2018]. Saatavissa: https://www.forbes.com/sites/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million/#66abaa0944ca

Tietosuojavaltuutetun toimisto. 2018. EU:n tietosuoja uudistus. [viitattu 4.4.2018]. Saatavissa: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Whitman, M. & Mattord, H. 2012. Principles of Information Security. 4. painos. Boston, Course Techonology. s. 623

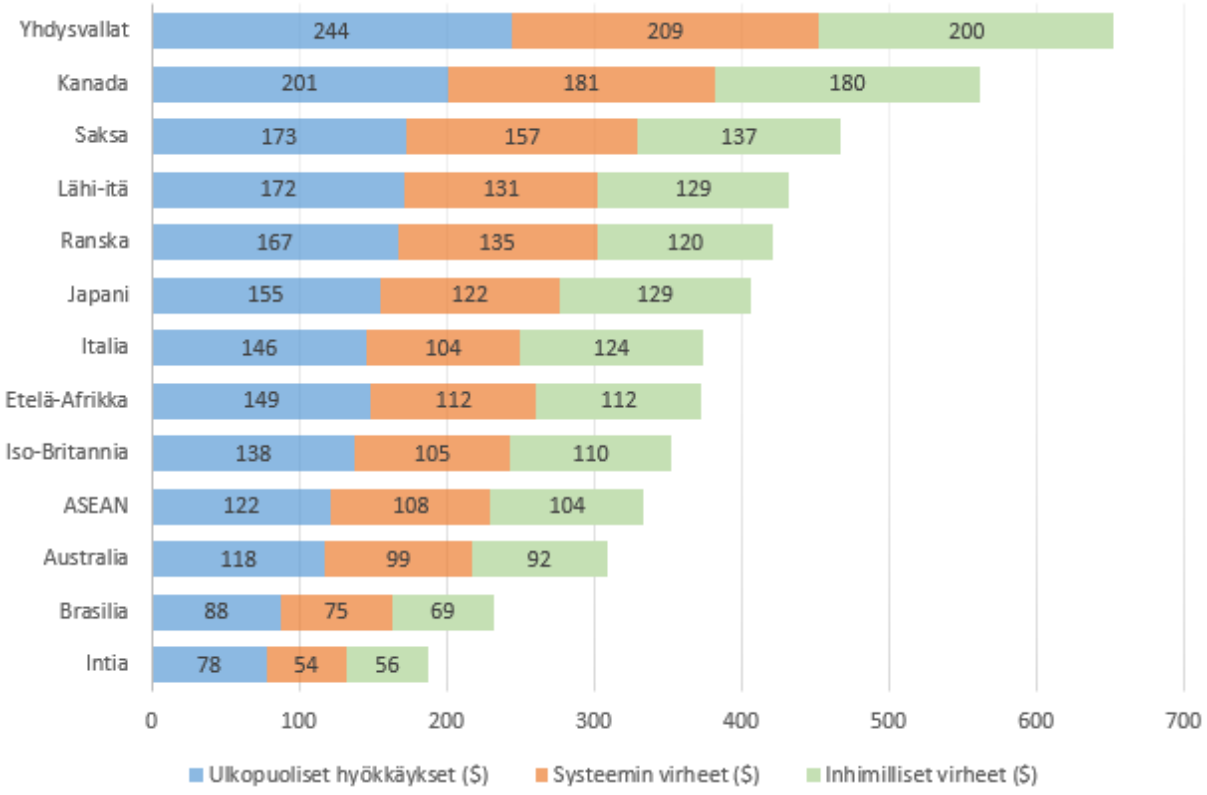
Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. 2016. Blockchain Challenges and Opportunities: A Survey. Internat. J. Web Grid Services.

Liitteet

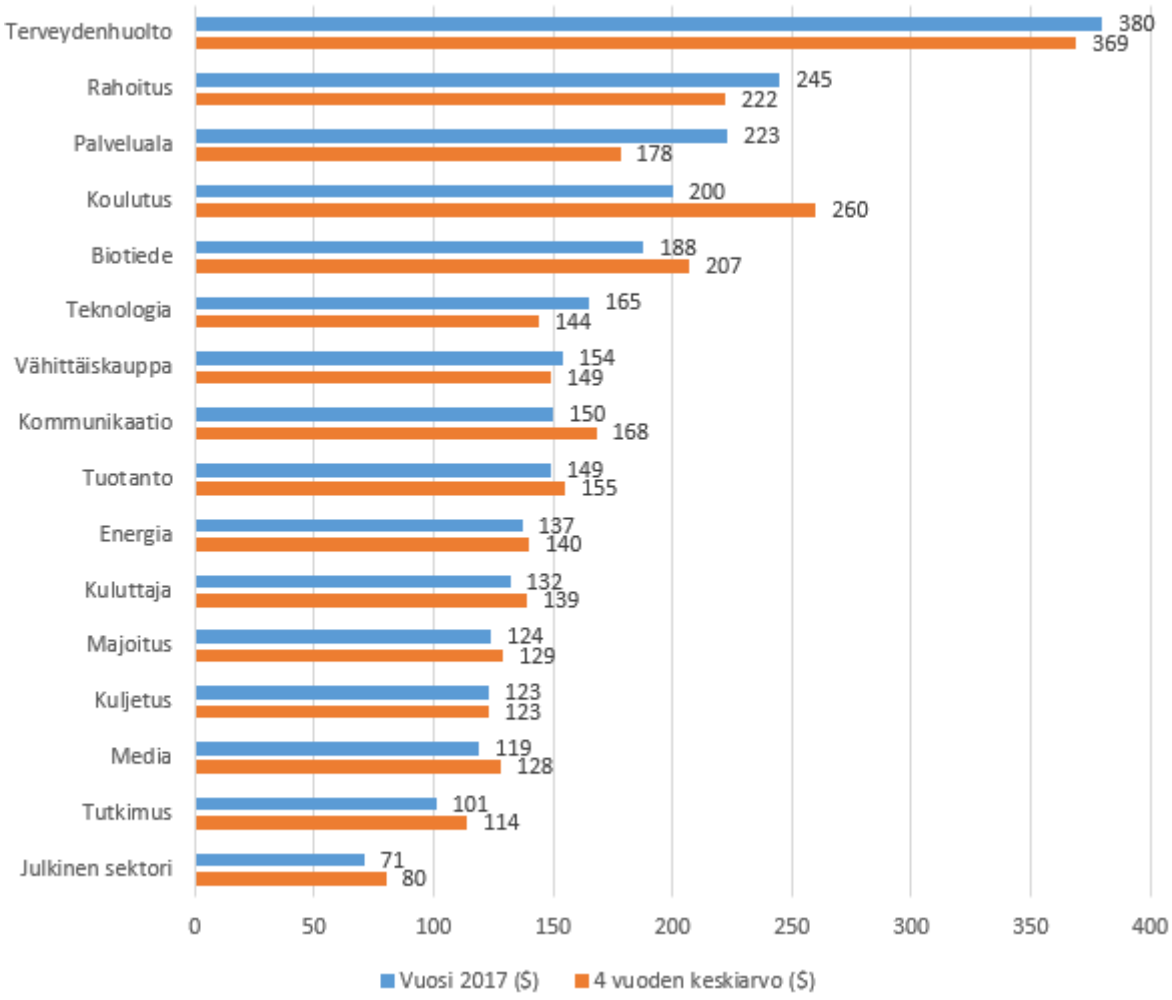
Liite 1. Tietoturvan CIA ominaisuudet, niiden tavoitteet ja vaarantumisen vaikutukset. (National Institute of Standards and Technology. 2004, s. 6; Nayak & Rao. 2014, s. 83)

	POTENTIAALISEN VAARANTUMISEN VAIKUTUS		
Tietoturvatavoite	**Vähäinen**	**Kohtalainen**	**Suuri**
Luottamuksellisuus, Tiedon saatavuuden ja levittämisen rajoitusten ylläpitäminen.	Luvaton pääsy tietoihin aiheuttaisi **rajattuja** haittoja yrityksen toimintaan, varoihin tai yksilöihin.	Luvaton pääsy tietoihin aiheuttaisi **vakavia** haittoja yrityksen toimintaan, varoihin tai yksilöihin.	Luvaton pääsy tietoihin aiheuttaisi **huomattavan vakavia tai katastrofaalisia** haittoja yrityksen toimintaan, varoihin tai yksilöihin.
Eheys, Suojaus tietojen epäasiallista muokkausta tai tuhoamista vastaan ja tietojen oikeellisuuden varmistus.	Luvaton tietojen muokkaus tai tuhoaminen aiheuttaisi **rajattuja** haittoja yrityksen toimintaan, varoihin tai yksilöihin.	Luvaton tietojen muokkaus tai tuhoaminen aiheuttaisi **vakavia** haittoja yrityksen toimintaan, varoihin tai yksilöihin.	Luvaton tietojen muokkaus tai tuhoaminen aiheuttaisi **huomattavan vakavia tai katastrofaalisia** haittoja yrityksen toimintaan, varoihin tai yksilöihin.
Saatavuus, Tiedon reaaliaikaisen ja luotettavan saatavuuden ja käytön ylläpitäminen.	Tiedon saatavuuden häiriintyminen aiheuttaisi **rajattuja** haittoja yrityksen toimintaan, varoihin tai yksilöihin.	Tiedon saatavuuden häiriintyminen aiheuttaisi **vakavia** haittoja yrityksen toimintaan, varoihin tai yksilöihin.	Tiedon saatavuuden häiriintyminen aiheuttaisi **huomattavan vakavia tai katastrofaalisia** haittoja yrityksen toimintaan, varoihin tai yksilöihin.

Liite 2. Tietomurtojen kustannukset per vaarantunut henkilötietotallenne dollareina eri maantieteellisillä alueilla toimiville yrityksille. (Ponemon Institute & IBM Security. 2017, s. 16)



Liite 3. Eri toimialojen tietomurtojen kustannukset Yhdysvalloissa vuonna 2017 ja neljänä edeltävänä vuotena. (Ponemon Institute & IBM Security. 2017, s. 13)



Liite 4. Esineiden internetin nykymallin ongelmat ja lohkoketjumallin ratkaisu. (Kshetri 2017a, Kshetri 2017b)

Haaste	Nykyinen malli	Lohkoketjun ratkaisu
Kustannus ja tiedon varastointirajoitteet	Eksponentiaalisen kasvun myötä vuoden 2016 kapasiteetti tulisi 1000-kertaista vuoteen 2020 mennessä, joka on haastavaa kustantaa keskitetyssä mallissa.	Hajautettu malli, jossa laitteet pystyvät toimimaan itsenäisesti älykkäiden sopimusten avulla sekä kommunikoimaan keskenään. Hajautetussa mallissa tiedon varastointi on helpompi toteuttaa suuressa skaalassa.
Arkkitehtuuriongelma	Nykyisessä mallissa keskittymiä, jotka oleellisia koko verkoston kannalta. Haavoittuvaisuus erilaisia hyökkäyksiä kohtaan kuten MitM ja DDoS.	Salattu tiedon välitys sekä julkisella ja yksityisellä avaimella varmennus, että tieto lähtee ja saapuu oikeaan paikkaan
Pilvipalveluserverien ylläpito-ongelmat	Pilvipalvelut välillä pois käytöstä mm. huoltokatkojen ja hyökkäysten seurauksena.	Hajautetussa verkossa useat yksiköt omaavat samaa tietoa, joka takaa varmuuskopioinnin ja tiedon säilyvyyden
Tiedon manipulointi	Tietoa on mahdollista manipuloida ja väärinkäyttää suhteellisen pienellä vaivalla (MitM)	Hajautettu pääsy sekä muuttumattomuus, haitalliset toimenpiteet voidaan valvonnalla havaita sekä estää, 51-hyökkäys