Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

HENRI SALMI

Vertaisverkon hyödyntäminen

TIETOJENKÄSITTELYN KOULUTUSOHJELMA
2020

Tekijä(t)
Salmi, Henri

Julkaisun laji
Opinnäytetyö, AMK

Päivämäärä
Joulukuu 2020

Sivumäärä
37

Julkaisun kieli
Suomi

Julkaisun nimi
Vertaisverkon hyödyntäminen

Tutkinto-ohjelma
Tietojenkäsittelyn koulutusohjelma

Tämän opinnäytetyön tavoitteena oli tutkia vertaisverkkoteknologian hyödyntämismahdollisuuksia asiakas-palvelin -mallin rinnalla ja sen käyttäjien välisessä tiedostojen jaossa. Selvitin, miten ne saivat alkunsa, millä tavalla niitä on hyödynnetty ja miltä niiden tulevaisuus näyttää.

Työn alussa tutkin vertaisverkkojen historiaa, toimintaperiaatetta, etuja sekä ongelmakohtia verrattuna perinteiseen asiakas-palvelin -malliin. Tutkin kolmea vertaisverkkoteknologian käyttökohdetta käyden läpi niiden toimintaperiaatteet ja tulevaisuuden näkymät. Lisäksi käyn läpi vertaisverkkoteknologian mahdollistamaa laitonta toimintaa ja sen myötä Suomessa tapahtuneita oikeudellisia toimia.

Työn lopussa on oma pohdintani liittyen vertaisverkkojen ja niiden myötä syntyneiden uusien teknologioiden realistisiin hyödyntämismahdollisuuksiin tällä hetkellä ja tulevaisuudessa. Pohdin myös laittoman toiminnan tämänhetkistä tilannetta, tulevaisuutta sekä omaa suhtautumistani siihen.

Asiasanat
vertaisverkot, p2p-verkot, lohkoketju, bittorrent, internet

Author(s) Salmi, Henri	Type of Publication Bachelor's thesis	Date December 2020
	Number of pages 37	Language of publication: Finnish

Title of publication
Making use of a peer-to-peer network

Degree program
Degree programme in Business Information Technology

The objective of this thesis was to research the possibilities of peer-to-peer network technology besides the client-server model and with sharing files between its users. My research includes how peer-to-peer networking got started, how it has been used and what its future looks like.

At the start of my work I researched the history of peer-to-peer networks, its principle, benefits as well as its problems compared to the traditional client-server model. I examined three applications made possible by peer-to-peer technology and their principles as well as their future. Additionally, I go through illegal activities made possible by peer-to-peer technology and the juridical activities that have happened in Finland.

At the end of my work I contemplate about the realistic possibilities of new technology made possible by peer-to-peer networks at the moment and in the future as well as the illegal activities and give my thoughts on it.

Key words
peer-to-peer network, p2p, blockchain, bittorrent, internet

SISÄLLYS

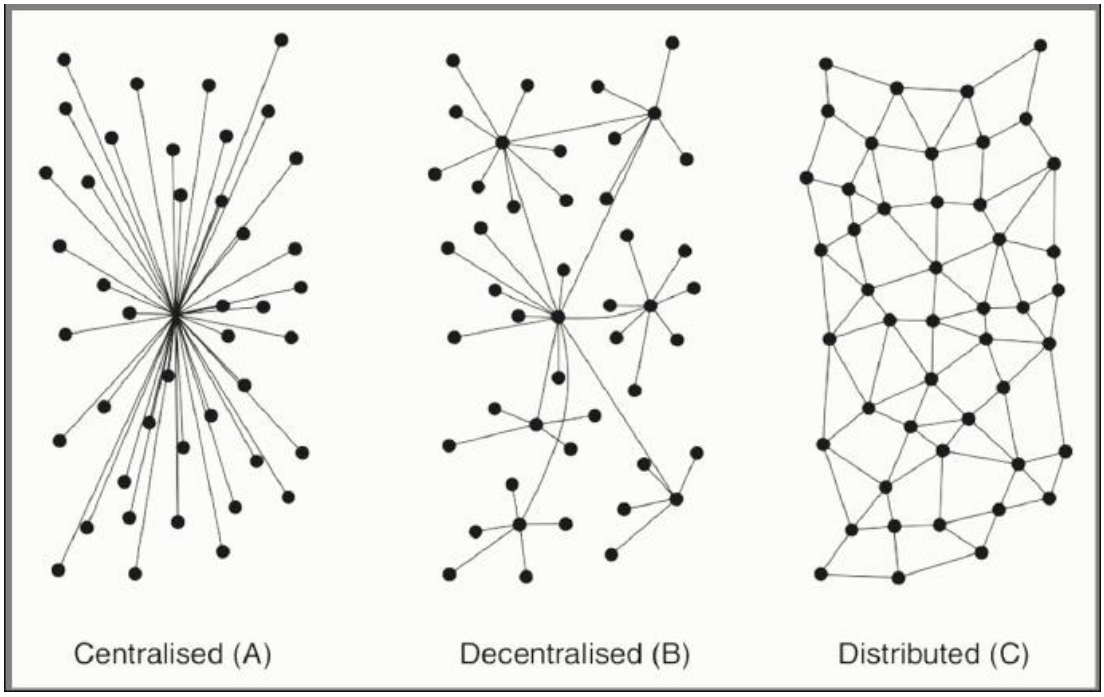
LÄHTEET

1 JOHDANTO

Internet on toiminut alusta alkaen pääosin asiakas-palvelin -mallin periaatteella, jossa ihmiset ottavat omilta tietokoneiltaan yhteyden tiettyyn samaan palvelimeen, josta tieto ladataan esimerkiksi verkkosivun tai valokuvan muodossa. Tällä palvelimella ja sen ylläpitämällä sisällöllä on omistaja, jolloin sitä hallitsee jokin yksittäinen taho. Vertaisverkkoteknologian kehitys toi tähän asiaan muutoksen. Vertaisverkkojen avulla ihmiset pystyvät jakamaan tietoa keskenään vaivattomasti jokaisen tietokoneen toimiessa sekä asiakkaana että palvelimena. Vertaisverkoissa jaettava tieto ei siis ole millään yksittäisellä palvelimella kuten asiakas-palvelin -mallissa, vaan yksinkertaistetusti kaikki tieto on kaikkien ladattavissa ja jaettavissa ympäri maailmaa. Työssä esitelty BitTorrent -protokolla on hyvä esimerkki tästä, koska sitä hyödynnettäessä yksittäinen tiedosto voidaan koota täysin eri puolelta maapalloa ladatuista palasista.

Työssäni keskityn tutkimaan vertaisverkkojen toimintamalleja ja niiden etuja sekä ongelmia verrattuna perinteiseen asiakas-palvelin -malliin. Käyn läpi kolme tällä hetkellä itselleni kiinnostavinta käyttökohdetta vertaisverkkoteknologialle ja pureudun niiden toimintaan hieman pintaa syvemmältä. Lisäksi käyn läpi vertaisverkkoteknologian yleistymisen myötä siellä väistämättömästi tapahtuvaa laitonta toimintaa koskien kopiosuojatun maksullisen sisällön jakamista. Työn lopussa on oma pohdintani liittyen vertaisverkkojen mahdollisuuksiin ja sen myötä syntyneiden eri teknologioiden realistisiin mahdollisuuksiin asiakas-palvelin -mallin rinnalla sekä laittoman toiminnan tulevaisuuden näkymiin.

2 VERTAISVERKOT



Kuva 1. Vasemmalla keskitetty malli, keskellä hajautettu ja oikealla jaettu verkkomalli. Asiakas-palvelin malli on keskitetty, hybridimalli on hajautettu ja strukturoimaton eli puhdas vertaisverkkomalli on jaettu. (Rehman 2017.)

Vertaisverkot eli peer-to-peer (P2P) -verkot ovat jaetuilla resursseilla toimivia tietokoneverkkoja. Kaikki tietokoneet ja laitteet, jotka ovat osana vertaisverkkoa ovat niin sanottuja vertaistoimijoita, koska ne vaihtavat ja jakavat työkuormiaan. Toimijat verkossa ovat samanarvoisia toistensa kanssa, eli yksikään käyttäjä ei omaa mitään erityisoikeuksia verrattuna muihin ja verkossa ei ole ylläpidosta huolehtivaa laitetta tai käyttäjää. Vertaisverkot ovat tavallaan kaikista tasa-arvoisimpia verkkoja koko maailmassa, koska jokaisella käyttäjällä on samat oikeudet ja velvollisuudet kuin toisella eli ne toimivat sekä asiakkaina että palvelimina samanaikaisesti. Jokainen verkossa saatavilla oleva resurssi jaetaan käyttäjien kesken ilman minkäänlaista keskuspalvelinta. Mahdollisia jaettavia resursseja vertaisverkossa ovat mm. prosessointiteho, levytila tai verkkokaista. (Neagu 2019, Binance Academy 2020.)

Vertaisverkkojen päätarkoitus on jakaa resursseja ja saada laitteet toimimaan yhteistyössä tuottamaan palveluita ja suorittamaan tehtäviä. Yleisin vertaisverkkojen käyttökohde on tiedostojen jakaminen internetin välityksellä. Vertaisverkot ovat ideaaleja

tiedostojen jakamiseen, koska ne mahdollistavat niihin kytketyt tietokoneet vastaanottamaan ja lähettämään tiedostoja samanaikaisesti. Esimerkkitilanne: Avaat verkkoselaimen ja vierailet sivulla, josta voit ladata tiedoston. Tässä tapauksessa verkkosivu toimii palvelimena ja tietokoneesi asiakkaana vastaanottaessasi tiedoston. Tätä voisi verrata yksisuuntaiseksi tieksi. Kun käyttäjä lataa saman tiedoston käyttäen esimerkiksi vertaisverkkoa hyödyntävää BitTorrent -alustaa lataus suoritetaan eri tavalla; tiedosto ladataan osissa useista eri lähteistä eli muista tietokoneista, jotka ovat yhteydessä samaan vertaisverkkoon ja joilla on valmiiksi jo kyseinen tiedosto ladattuna tai ainakin osa siitä. Samaan aikaan tiedostoa ladattaessa sitä myös lähetetään muille laitteille, jotka pyytävät sitä. Tämä tilanne on verrattavissa kaksisuuntaiseen tiehen; tiedosto on kuin useita pieniä autoja tulossa kohti ja myös vastaan niin pyydettäessä. (Neagu 2019, Binance Academy 2020.)

2.1 Historiaa

2.1.1 USENET

Vertaisverkkojen edeltäjänä toimi vuonna 1979 kehitetty USENET-järjestelmä, joka oli tehty käyttäjille uutisten ja viestien lähettämiseen sekä lukemiseen. Se oli nettifoorumeihin verrattava verkkojärjestelmä sillä erolla, että siinä ei ollut keskitettyä palvelinta tai ylläpitäjää. USENET kopioi saman viestin tai uutisen jokaiselle verkossa olevalle palvelimelle. Samaan tapaan vertaisverkot jakavat ja käyttävät kaikkia saatavilla olevia resursseja. (Neagu 2019.)

2.1.2 Napster

Ensimmäinen yleisesti käytössä ollut vertaisverkkoratkaisuun perustuva sovellus oli Napster. Napster oli vuosina 1999-2001 toiminut sovellus, jonka avulla ihmiset voivat jakaa MP3-tiedostoja. Napster käytti hybridimallia vertaisverkosta, jossa keskuspalvelin yhdisti kaksi käyttäjää toisiinsa perustuen haettavaan ja omistettavaan tiedostoon. Napsterin käyttämä protokolla mahdollisti vain MP3-tiedostojen hakemisen ja

lataamisen, jota pidettiin sen ongelmakohtana. Tähän kehitettiin ratkaisuna työkalu, joka sai muita tiedostotyyppejä näyttämään MP3-muotoiselta, jolloin Napsterin palvelimet sallivat ne haettavaksi. Käyttäjän tuli muodostaa TCP-yhteys tiedostojen jakamiseksi. TCP/IP protokolla ei sisällä itsessään tietoturvallisuutta, joten tiedostojen siirtoja oli mahdotonta piilottaa seuraajilta. Toinen ongelma Napsterin toiminnassa oli sen käyttämä keskuspalvelin. Keskuspalvelimen kaaduttua esimerkiksi palvelunestohyökkäyksen takia koko palvelu muuttui toimimattomaksi. Napsterin jälkeen tuli useita siihen perustuvia sovelluksia, jotka käyttivät myös vertaisverkkoratkaisua. Näissä sovelluksissa jaettiin kaikentyyppisiä tiedostoja, ei pelkästään MP3:sia. Muita verkkoarkkitehtuurillisia ratkaisuja kehitettiin ja otettiin käyttöön tavoitteena luoda tehokkaampi ja tietoturvallisempi verkko. (Washbourne 2015.)

2.1.3 Gnutella

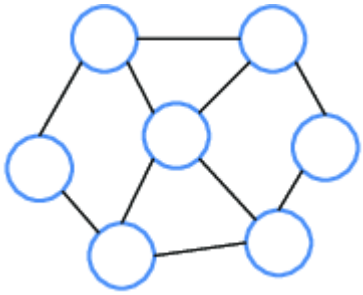
Gnutella -niminen sovellus aloitti toimintansa vuoden 2000 alussa. Sen kehitys lopetettiin nopeasti, mutta muutamat käyttäjät ehtivät ladata sen ja alkoivat kehittämään omaa versiotaan siitä, joka johti sovelluksen laajamittaiseen käyttöön ympäri maailmaa. Gnutellan käyttämä protokolla ei käytä keskuspalvelinta, vaan jokainen käyttäjä järjestelmässä toimi sekä asiakkaana että palvelimena. Gnutellan käyttämää verkkoa voidaan kutsua strukturoimattomaksi vertaisverkoksi, jossa jokainen asiakas on yhdistetty useaan muuhun asiakkaaseen. Tämä verkkoarkkitehtuuri auttoi sitä selviytymään paremmin, kun verkko ei kärsinyt yhden palvelimen muuttuessa toimimattomaksi. Tiedostojen jakaminen tapahtui HTTP-protokollan avulla suoraan käyttäjien välillä ilman keskuspalvelinta. Gnutellan käyttämän verkkoprotokollan ongelmana oli käyttäjät, joiden siirtonopeus oli hidas tai jotka eivät suostuneet jakamaan tiedostoja. (Washbourne 2015.)

2.2 Vertaisverkkomallit

Vertaisverkkomallit (kuva 1) eivät jakaudu pelkästään keskitettyihin ja hajautettuihin, vaan niistä löytyy myös välimuotoja. Jotkut vertaisverkkoja hyödyntävät

tiedostojenjakopalvelut esimerkiksi sallivat käyttäjien hakea ja ladata tiedostoja muilta käyttäjiltä, mutta käyttäjät eivät pysty muuten vaikuttamaan hakuprosesseihin, vaan sen hoitaa käyttäjien välissä oleva keskitetty palvelin. Vertaisverkot voidaan jakaa niiden arkkitehtuurien mukaan kolmeen eri kategoriaan, jotka ovat strukturoimaton, strukturoitu ja hybridi. (Binance Academy 2020.)

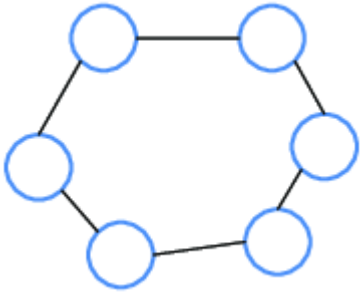
2.2.1 Strukturoimaton



Kuva 2. Strukturoimaton vertaisverkkomalli visualisoituna. (Yeferny 2020.)

Strukturoimattomassa tai puhtaassa vertaisverkkomallissa (kuva 2) verkon solmukohtia ei kontrolloida ja ne eivät ole minkään tietyn organisaation alaisuudessa. Solmukohdat keskustelevat keskenään satunnaisesti. Tällaisia järjestelmiä pidetään hyvinä kohteissa, joissa käyttäjien aktiivisuustaso on korkea eli verkkoon liittyy ja verkosta poistuu solmukohtia tiheään tahtiin. Strukturoimattomia vertaisverkkoja pidetään helpompina rakentaa, mutta ne voivat olla vaativia prosessori- ja muistikuormalle, koska hakupyynnöt lähetetään isoimmalle mahdolliselle määrälle solmukohtia. Tällaisen käytännön myötä verkko saattaa kuormittua hakupyynnöistä varsinkin tilanteissa, joissa vain pieni määrä solmukohtia tarjoaa haettua sisältöä. (Binance Academy 2020.)

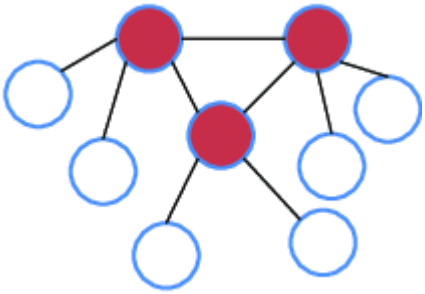
2.2.2 Strukturoitu



Kuva 3. Strukturoitu vertaisverkkomalli visualisoituna. (Yeferny 2020.)

Strukturoitu vertaisverkkomalli (kuva 3) on rakennettu organisoidun arkkitehtuurin päälle, joka mahdollistaa käyttäjille hakupyyntöjen tehokkaan lähetyksen, vaikka haettava sisältö ei olisikaan laajasti saatavilla. Useimmissa tapauksissa tämä saavutetaan tietokantahakuja helpottavien hash-funktioiden kautta. Tällaiset järjestelmät toimivat tehokkaammin, mutta niiden rakennus- ja ylläpitokulut ovat korkeammat palvelun keskittyneisyyden vuoksi. Ne eivät myöskään ole yhtä joustavia tilanteissa, jossa käyttäjiä liittyy ja poistuu verkosta kovalla tahdilla. (Binance Academy 2020.)

2.2.3 Hybridi



Kuva 4. Hybridi vertaisverkkomalli visualisoituna. (Yeferny 2020.)

Hybridimalli (kuva 4) yhdistää vertaisverkkomallin ominaisuuksia perinteisen asiakas-palvelin -mallin kanssa. Hybridimallilla toimiva järjestelmä voi sisältää esimerkiksi keskitetyn palvelimen, joka toimii yhteyspisteenä vertaisverkon käyttäjien välillä. Hybridimallin käyttö parantaa yleensä kokonaisuudessaan järjestelmän toimintakykyä verrattuna kahteen aikaisempaan malliin kohottamalla järjestelmän tehokkuutta

sekä hajauttamista, jolloin se siis yhdistää strukturoimattoman ja strukturoidun mallin hyödyt. (Binance Academy 2020.)

2.3 Edut

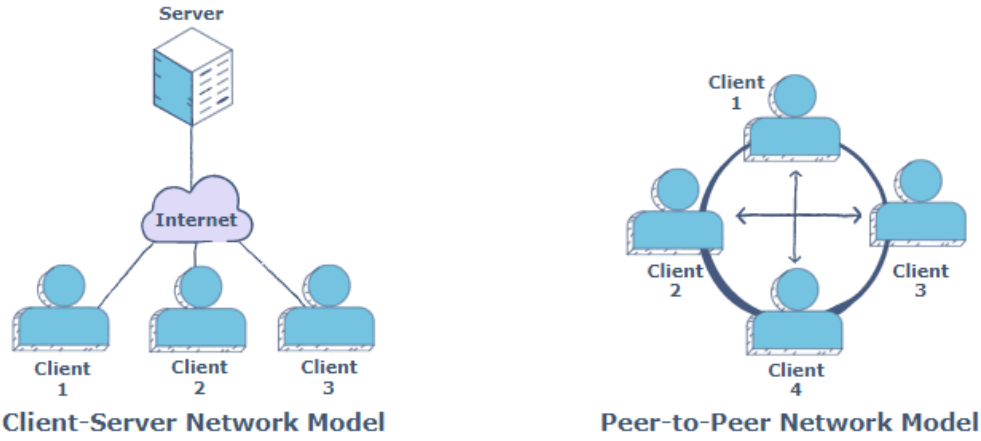
2.3.1 Saatavuus

Perinteisesti verkossa olevat palvelut on rakennettu keskitetysti toimivan asiakas-palvelin -mallin toimintaperiaatteella (kuva 5). Asiakas-palvelin malli on yleisin käytössä oleva malli datan siirtoon ja lähes kaikki isot verkkopalvelut kuten esimerkiksi Facebook, Twitter ja Google käyttävät tätä mallia. Yksi tietokone toimii palvelimena ja toinen asiakkaana, jolloin palvelimen tulee olla saatavilla koko ajan sekä yhteyden tulee olla toimiva. Palvelin tarjoaa asiakkaille dataa ja se voi myös vastaanottaa asiakkailta dataa. Yleisin ongelma asiakas-palvelin -mallissa on se, että palvelimen tulee olla jatkuvasti saatavilla. Kun palvelimen ohjelmistoon, verkkoyhteyteen tai fyysiseen laitteistoon tulee ongelma, palvelu katkeaa kaikilta asiakkailta. Tällöin palveluntarjoajan tulee hankkia korkean saatavuuden ratkaisu etukäteen, jotta järjestelmä voi vaihtaa varalla toimiviin komponentteihin tai verkkoyhteyteen ongelmatilanteen sattuessa. Tämä on monimutkainen ongelma, sillä datan tulee olla ajan tasalla varalla toimivassa koneessa eli data tulee pitää synkronoituna. Ohjelmisto- ja laitteistopäivitykset tulee suunnitella hyvissä ajoin etukäteen, jotta palvelu saadaan pidettyä saatavilla päivityksistä huolimatta. (Educative.io 2020a, Qureshi 2019.)

2.3.2 Palvelinkuorma

Toinen ongelma asiakas-palvelin -mallissa on korkean rasituksen tilanteet. Yksi paljon dataa kuluttava asiakas, tai yhtäkkinen iso määrä asiakkaita voi saada palvelun kaatumaan johtuen verkkoyhteyden, levytoimintojen tai prosessorikuorman liiallisesta kasvusta. Kaikilla asiakkailla tulee olla pääsy palvelimelle, joten resurssien kulutukselle pitää asettaa käyttäjäkohtaiset rajoitukset. Rajoitusten ollessa voimassa jokainen asiakas saa käyttöönsä vain minimaaliset pakolliset resurssit palvelimelta, jolloin palvelin ei toimi dynaamisesti tilanteessa, jossa resursseja voitaisiin jakaa yksittäiselle

asiakkaalle enemmänkin alhaisen kuorman takia. Jokaisen palvelimen resurssit on määritetty toimimaan tietylle määrälle asiakkaita. Asiakasmäärien kasvaessa tulee myös palvelimen resurssien määrän kasvaa. Joissain tilanteissa tarvitaan jo useampi palvelin, mikäli asiakkaiden määrä kasvaa niin isoksi, että yksittäinen palvelin ei pysty enää käsittelemään kaikkia. Järjestelmät ja palvelimet tulee siis suunnitella niin, että kuorma pystytään tasapainottamaan palvelinten välillä. (Educative.io 2020a.)



Kuva 5. Vasemmalla asiakas-palvelin -malli ja oikealla vertaisverkkomalli. (Educative.io 2020b.)

2.3.3 Dynaamisuus

Vertaisverkkojen maailmassa jokainen asiakas toimii myös palvelimena (kuva 5). Palvelua tarjoaa siis jokainen saatavilla oleva asiakas. Palvelun saatavuus ei ole tällöin riippuvainen yhdestä palvelimesta ja se ei vaadi korkean saatavuuden ratkaisun kehittämistä, kuten asiakas-palvelin -mallissa. Vertaisverkkomallissa jokainen asiakas voi ladata dataa korkeimmalla mahdollisella nopeudella ilman rajoituksia, mikäli resursseja eli muita asiakkaita on tarpeeksi saatavilla. Palvelun nopeus toimii dynaamisesti riippuen asiakkaiden määristä, toisin kuin asiakas-palvelin mallissa. Mitä enemmän laitteita vertaisverkossa on, sitä tehokkaammin dataa pystytään siirtämään. (Educative.io 2020a.)

Lisäksi vertaisverkosta hyödyllisen tekeviä ominaisuuksia ovat seuraavat:

- Kun vertaisverkko on saatu rakennettua toimivaksi, sitä on hankala sammuttaa. Mikäli yksi solmukohdista sammutetaan, toiset jatkavat toimintaa ja kommunikointia normaalisti. Jotta vertaisverkko saadaan kokonaan sammutettua, pitää kaikki siihen yhteydessä olevat solmukohdat sammuttaa erikseen.
- Vertaisverkot ovat erittäin skaalautuvia. Uusien solmukohtien lisääminen on helppoa, koska niitä ei tarvitse erikseen konfiguroida keskitetyltä palvelimelta, vaan ne voivat liittyä verkkoon vapaasti ilman rajoituksia.
- Mitä laajempi vertaisverkko on eli mitä enemmän siinä on solmukohtia tiedostoja jaettaessa, sitä nopeampi se on. Kaikkien tietokoneiden yhteiset resurssit tekevät verkosta aina nopeamman. Kun tiedosto on ladattavissa usealta eri tietokoneelta, se voidaan ladata niiltä kaikilta yhtäaikaisesti.
- Vertaisverkkojen käyttäminen on joissain tapauksissa huomattavasti halvempaa kuin keskitetyn palvelimen hankkiminen, sillä niiden hankinta vie usein enemmän aikaa ja niitä on hankalampi hallita.
  (Neagu 2019, Binance Academy 2020.)

2.4 Ongelmat

2.4.1 Epätasapaino

Vertaisverkkojen ongelmat johtuvat useimmiten niille ominaisista hajauttamisen ja anonymiteetin ominaisuuksista. Aikaisemmin mainitut leecherit aiheuttavat epätasapainoa verkossa lataamalla vain itselleen, koska tällöin vain pieni prosentti käyttäjistä kantaa suurimman osan jakokuormasta. Epätasapaino aiheuttaa tehottoman verkon hitailla siirtonopeuksilla. (Washbourne 2015.)

2.4.2 Urkinta

Hyökkäyksissä kokemattomat käyttäjät jakavat tietoa järjestelmistään kokeneemmille vertaisverkkojen käyttäjille, jotka voivat käyttää tätä tietoa hyväkseen mahdollisesti salasanojen urkintaan tai jopa koko järjestelmän kiintolevyn näkemiseen. Jatkuvasti

internettiin yhteydessä olevat tehokäyttäjät voivat pitää listaa jaetuista tiedostoista tietyille käyttäjille, joiden avulla voidaan määrittää käyttäjän identiteettiä tai tapoja. Tällainen toiminta rikkoo vertaisverkkojen käyttäjille luvattua anonymiteettiä. (Washbourne 2015.)

2.4.3 Palvelunestohyökkäykset

Palvelunestohyökkäykset tekevät käyttäjän tai verkon toimintakyvyttömäksi, jolloin kohde ei voi vastata pyyntöihin tehden siitä käyttökelvottoman. Palvelunestohyökkäyksissä käyttäjä lähettää toiselle käyttäjällä jatkuvalla syötöllä käyttökelvottomia paketteja, jotka vievät kohteen kaikki resurssit poistaen siltä mahdollisuuden tarjota palveluitaan vertaisverkossa. Palvelunestohyökkäykset eivät ole yhtä tehokkaita vertaisverkoissa sen hajautetun toimintaperiaatteen takia verrattuna asiakas-palvelin -mallilla toimiviin verkkoihin, koska verkko kokonaisuudessaan ei juurikaan kärsi yhden käyttäjän menetyksestä. (Washbourne 2015.)

2.4.4 Tiedon verifiointi

Yksi vaikeimmista ongelmista on tiedostojen sisällön verifiointi. Vertaisverkossa kaikki käyttäjät ovat yhtä vaikutusvaltaisia ilman keskitettyä käyttäjää, joka varmentaisi pyynnöt ja palvelut. Tällöin ei voida mitenkään varmentaa, että käyttäjät lähettävät toisilleen sellaisia tiedostoja, joita he lupaavat. Tämä on aiheuttanut virusten leviämistä vertaisverkkojen kautta. Paras puolustus tähän on olla arvioimatta itse tiedostoa, jota ladataan vaan käyttäjä, joka sitä lähettää. Joissain vertaisverkoissa käyttäjä voidaan arvostella rehellisyyden perusteella, jolloin vahingolliset käyttäjät saadaan merkittyä ja muita käyttäjiä varoitettua heistä. (Washbourne 2015.)

3 KÄYTTÖKOHTEET

3.1 BitTorrent-protokolla

BitTorrent on käyttäjien väliseen tiedostojen jakamiseen tehty protokolla ja sen kehitti Buffalon yliopistossa opiskelija Bram Cohen vuonna 2001. BitTorrentin verkkoarkkitehtuuri on hajautettu vertaisverkko. (Washbourne 2015.)

3.1.1 Toimintaperiaate

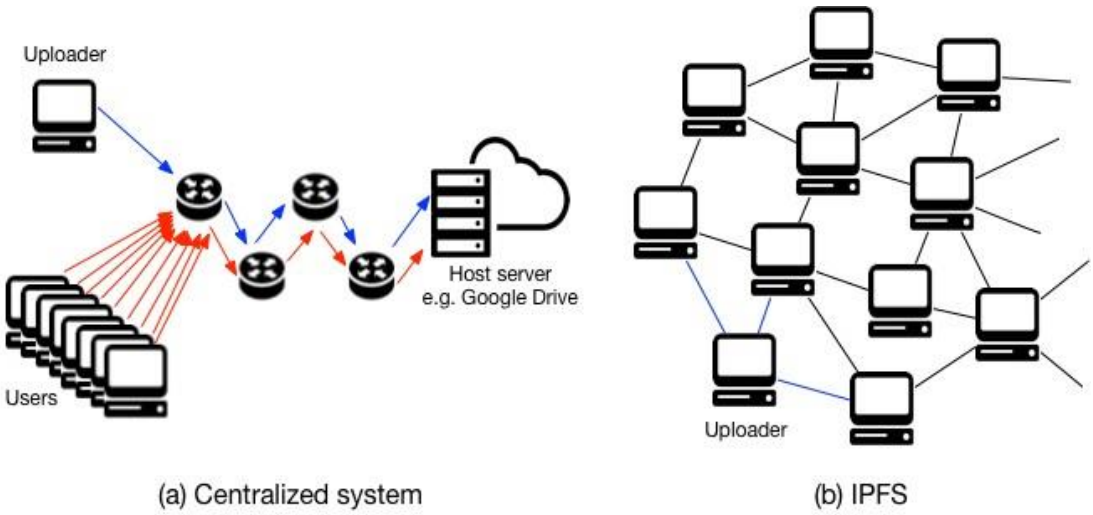
Tiedostojen siirto ei tapahdu protokollassa itsessään, vaan käyttäjien pitää käyttää seurantapalvelinta (eng. tracker) muiden käyttäjien löytämiseksi. Seurantapalvelin pitää sisällään listan käyttäjien IP-osoitteita, jotka jakavat tiettyä tiedostoa. Käyttäjän pitää löytää seurantapalvelin ladatakseen tietyn tiedoston ja seurantapalvelinten löytämiseen käytetään verkkosivuja kuten The Pirate Bay. Tracker-sivulta ladattu tiedosto sisältää tracker-tiedoston sekä torrent-tiedoston. Käyttäjän tulee luoda kyseinen torrent-tiedosto ja lähettää se jollekin seurantapalvelimelle, mikäli tiedosto halutaan saada muiden ihmisten ladattavaksi. Torrent-tiedoston sisältämän tiedon avulla käyttäjät saavat avustettua toisiaan tiedoston lataamisessa. BitTorrent-protokollan kautta jaetut tiedostot pitää hajoittaa ”palasiksi” ja ”blokeiksi”. Tyypillisesti palanen on 512 kilobittiä ja blokki 16 kilobittiä. Torrent-tiedosto sisältää tiedoston muodostavat palaset ja blokit, seurantapalvelimen IP-osoitteen ja porttinumeron sekä SHA1 hash-taulut tiedoston paloista. SHA1 hash-taulut mahdollistavat käyttäjille tiedoston sisällön oikeellisuuden varmistamisen. Protokolla mahdollistaa siis palasten hakemisen rinnakkain useista eri lähteistä samanaikaisesti tiedostoa ladattaessa. (Washbourne 2015, Savolainen 2020.)

BitTorrent-protokolla käyttää useita rinnakkaisia verkkoyhteyksiä tiedoston latauksen nopeuttamiseksi, kun taas verkkoselaimet käyttävät tyypillisesti vain yhtä TCP-porttia http-pyyntöihin ja vastauksiin. BitTorrent-protokolla toimii siis muiden käyttäjien avustuksella, kun taas HTTP-protokolla perustuu puhtaasti asiakas-palvelin -mallin toimintaperiaatteeseen. (Savolainen 2020.)

3.1.2 Käyttäjätyypit

Käyttäjä voi olla niin sanottu ”leecher” tai ”seeder” BitTorrent-protokollassa. Leecher on käyttäjä, joka on ladannut tiedoston itselleen, mutta ei ole osallistunut tiedoston jakamiseen kokonaisuudessaan. Seeder on käyttäjä, joka on ladannut ja jakanut tiedoston muille käyttäjille kokonaisuudessaan. BitTorrent -protokolla suosii käyttäjiä, jotka jakavat tiedostoja aktiivisesti. Jakajat tasaisin väliajoin tarkistavat muiden käyttäjien lähetysmäärät ja jakavat ainoastaan niiden kanssa, jotka myös lähettävät. Tätä toimenpidettä kutsutaan nimellä tit-for-tat ja se hidastaa tai jopa rajoittaa leechereitä lataamasta kyseiseltä seurantapalvelimelta. Tit-for-tat periaatteessa lähetyskaistaa verrataan latauskaistaan ja mikäli käyttäjä pelkästään lataa, sen latausta hidastetaan tai se lopetetaan. Solmukohtia on rajallisesti ja estetyn käyttäjän paikka luovutetaan toiselle. (Washbourne 2015, Savolainen 2020.)

3.2 IPFS



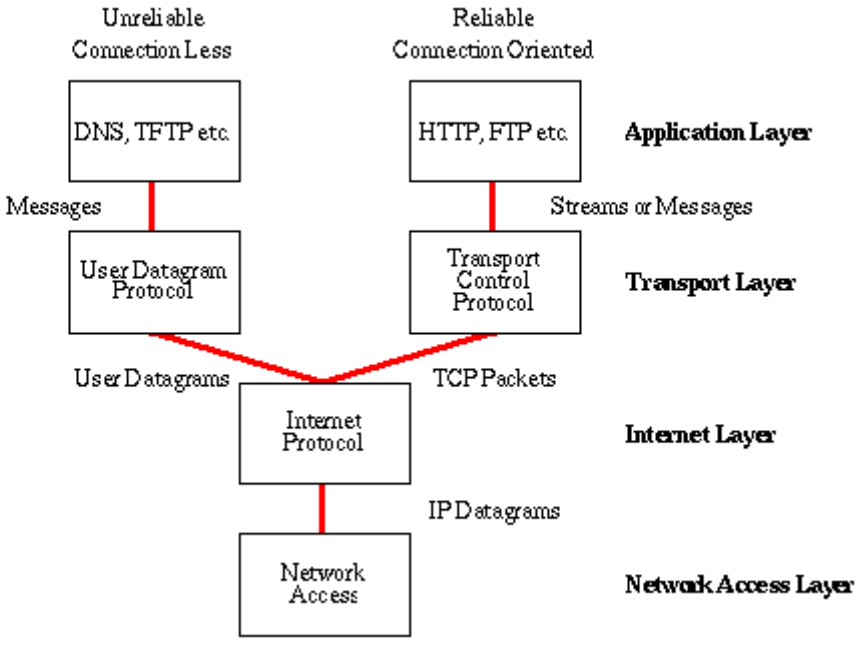
Kuva 6. Keskitetty järjestelmä verrattuna IPFS:n toimintamalliin. (zk Capital 2018.)

IPFS eli Interplanetary File System (kuva 6) on vertaisverkkoteknologiaan perustuva tiedostonjakojärjestelmä, jonka tavoitteena on muuttaa tapa, jolla tietoa jaetaan ja siirretään ympäri maailmaa. IPFS-teknologia on kommunikointiprotokollien ja jaettujen

järjestelmien innovaatioista tehty yhdistelmä, josta on saatu tehtyä uniikki tiedostonjakojärjestelmä. Jotta voidaan kunnolla ymmärtää se, mitä IPFS:llä yritetään saavuttaa, tulee myös ymmärtää teknologisessa kehityksessä tapahtuneet läpimurrot, jotka tekevät sen mahdolliseksi. (Addaquay 2018, zk Capital 2018.)

3.2.1 Toimintaperiaate

Kahden ihmisen välisessä tiedon jakamisessa tulee noudattaa tiettyjä sääntöjä, jotka määrittävät miten ja milloin tietoa siirretään. Nämä säännöt tunnettaan yleisesti nimellä kommunikaatioprotokollat, jotka ovat verrattavissa ihmisten käyttämiin puhekieliin. Tietokoneilla on siis sama ongelma kuin ihmisillä eri maista, kun he eivät ymmärrä toistensa puhekieliä. 1980-luvun alussa tämä ongelma ratkesi ensimmäisten kommunikaatioprotokollien myötä. Kommunikaatioprotokollat ovat yleensä niin sanotuissa pinoissa eli ne toimivat usealla eri tasolla kuten esimerkiksi internetprotokollapino (kuva 7). (Addaquay 2018, zk Capital 2018.)



Kuva 7. Internetprotokollapino. (Frystyk 1994.)

Internetprotokollapinossa on siis neljä tasoa, joista jokainen vastaa tietyistä toiminnoista. Lisäksi on tärkeää ymmärtää tietokoneiden välisen yhteyden arkkitehtuuri eli verkkorakenne, joita ovat esimerkiksi aikaisemmin mainitut asiakas-palvelin- ja

vertaisverkkomalli. Internet koostuu pääosiin asiakas-palvelin -mallilla toimivista suhteista, jotka toimivat internetprotokollapinon päällä ja joissa HTTP-protokolla on kommunikaation perusta. (Addaquay 2018.)

Internetissä data tallennetaan normaalisti keskitetyille palvelimille ja sitä haetaan sijaintiin perustuvalla osoitteella. Tämä tekee siitä helpomman jaettavuuden, hallittavuuden, tietoturvan sekä koneiden kapasiteetin skaalautuvuuden kannalta. Tietoturvan, yksityisyyden ja tehokkuuden kannalta siinä on kuitenkin useita heikkouksia, sillä mahdollisuus palvelimen hallintaan antaa pääsyn myös sen sisältämän datan hallintaan. Tämä tarkoittaa sitä, että käyttäjä, joka pääsee käsiksi palvelimeen voi muokata tai poistaa sen sisältämää dataa. Sijaintiin perustuvan osoituksen myötä dataa ei identifioida sen sisällön vaan sen sijainnin mukaan, jonka myötä tiedon hakemiseksi tulee se hakea tietystä sijainnista, vaikka se voisi olla saatavilla myös lähempänä. Tietoa hakevan osapuolen on mahdotonta tietää datan oikeellisuutta, koska se haetaan sijainnin eikä sisällön mukaan. (Addaquay 2018, zk Capital 2018.)

Asiakas-palvelin -malli ja HTTP-protokolla ovat palvelleet internettiä melko luotettavasti koko sen historian ajan, koska ne ovat tehokkaita pienten tiedostojen kuten tekstin ja kuvien siirtoon. Webin ensimmäisen kahden vuosikymmenen aikana keskikokoisen verkkosivun koko on kasvanut kahdesta kilobitistä kahteen megabittiin, mutta nykypäivänä haasteita tuottavat video- ja äänitiedostojen isot datamäärät. Nämä rajoitukset mahdollistivat ja toivat suureen suosioon esimerkiksi elokuvien jakamiseen vertaisverkkoa hyödyntävät aikaisemmin mainitut torrent-palvelut. (IPFS.IO 2020a, Addaquay 2018.)

Nykypäivänä esimerkiksi isot videotiedostot ovat heti kaikkien ladattavissa, jolloin ihmiset käyttävät jatkuvasti enemmän dataa ja sen ohella kehitetään tehokkaampia tietokoneita sen käsittelyyn. Tämän ilmiön on mahdollistanut valtava kehitys pilvipalveluissa, vaikka pohjalla oleva infrastruktuuri on pysynyt laajalta osin samana. (Addaquay 2018.)

IPFS pyrkii ratkomaan asiakas-palvelin -mallin ja HTTP-protokollan heikkoudet uudenlaisen vertaisverkkomalliin perustuvan tiedostonjakojärjestelmän avulla. IPFS on

Protocol Labsin kehittämä avoimen lähdekoodin projekti, johon sadat kehittäjät ympäri maailmaa ovat osallistuneet. IPFS-mallin pääkomponentit ovat seuraavat:

- Hajautettu tiiviste (Distributed hash table)
  Tiiviste on datastruktuuri, johon tieto tallennetaan avain/arvo pareina. Hajautetuissa tiivisteissä data on jaettu verkossa olevien tietokoneiden kesken ja sitä voidaan koordinoida mahdollistaen tehokkaan pääsyn ja saavutettavuuden tietokoneiden kesken. Hajauttaminen, vikasietoisuus ja skaalautuvuus ovat tässä etuina. Solmukohdat eivät vaadi keskitettyä hallintaa ja järjestelmä toimii luotettavasti niiden kaatuessa tai poistuessa verkosta. Hajautetun tiivisteen skaalautuvuus mahdollistaa sen sisältämään miljoonia solmukohtia. Yhdessä näistä ominaisuuksista syntyy järjestelmä, joka on pääosin kestävämpi kuin asiakas-palvelin -malli.

- Block Exhange
  Aikaisemmin mainittu BitTorrent käyttää datansiirron koordinoimiseen onnistuneesti tätä lohkoketjuun perustuvaa innovatiivista protokollaa, joka on kuitenkin rajoittunut toimimaan vain sen protokollassa. IPFS käyttää tästä protokollasta kehitettyä yleisversiota nimeltä BitSwap, joka toimii kauppapaikkana minkälaiselle datalle tahansa.

- Merkle DAG
  Merkle DAG on yhdistelmä lohkoketjussa käytettävää Merkle Tree -teknologiaa ja matemaattista Directer Acyclic Graph -teoriaa. Merkle treet varmistavat, että vertaisverkoissa jaettavat datablokit ovat oikeita, vahingoittumatomia ja muokkaamattomia. Tämä varmistus tehdään siten, että datablokit järjestetään käyttäen kryptograafisia tiivistefunktioita. Tämä funktio ottaa arvon sisäänsä ja laskee sille uniikin aakkosnumeerisen tiivisteen, joka vastaa annettua syötettä. DAG on tapa mallintaa topologisia tietoketjuja, josta yksinkertainen esimerkki on sukupuu. Merkle DAG on käytännössä datastruktuuri, jossa käytetään tiivisteitä viittamaan datablokkeihin ja objekteihin DAG:ssa. Tämä luo useita hyödyllisiä ominaisuuksia; kaikki sisältö IPFS-verkossa voidaan identifioida uniikisti, koska jokaisella datablokilla on uniikki tiiviste. Data on myös suojattu muokkauksilta, koska sen muokkaaminen muuttaa sen tiivistettä.

IPFS:n keskeisin toimintaperiaate on kaiken datan mallintaminen Merkle DAG -yhdistelmällä. Tämän turvaominaisuuden tärkeyttä on vaikea liioitella.

- Versionhallintajärjestelmä

  Yksi Merkle DAG yhdistelmän tärkeistä ominaisuuksista on sen mahdollistama jaetun versionhallintajärjestelmän rakentaminen (VCS). Yksi suosittu esimerkki VCS:stä on GitHub, joka mahdollistaa kehittäjien samanaikaisen yhteistyön projekteissa. GitHubissa olevat tiedostot tallennetaan ja versioidaan käyttäen Merkle DAGia. Sen avulla käyttäjät voivat itsenäisesti monistaa ja muokata useita eri versioita tiedostosta ja tallentaa nämä versiot myöhemmin yhdistettäväksi alkuperäiseen tiedostoon. IPFS käyttää samankaltaista mallia dataobjekteihin; tiedoston koko historia pystytään hakemaan niin kauan, kun objektit vastaavat alkuperäistä dataa ja mikä tahansa uusi versio on saatavilla. IPFS-objektit voidaan tallentaa pysyvästi, kun datablokit on tallennettu paikallisesti eri tietokoneiden välimuistiin ympäri verkkoa. IPFS-verkko ei myöskään luota internetprotokollien käyttöoikeuteen, koska data voidaan jakaa kerrostetuissa verkoissa (overlay network), jotka ovat toistensa päälle rakennettuja verkkoja. Nämä ominaisuudet ovat huomattavan tärkeitä, koska ne toimivat ydinelementteinä sensuurinvastaisen verkon rakennuksessa.
  (IPFS.IO 2020b, Addaquay 2018, zk Capital 2018.)

Vaikka IPFS sisältää paljon kompleksista teknologiaa, sen fundamentaalinen idea on muuttaa se, miten ihmisistä ja tietokoneista muodostuvat verkot kommunikoivat keskenään. World Wide Web tänä päivänä on rakennettu omistajuuden ja pääsyn periaatteiden päälle. Tämä tarkoittaa sitä, että tiedostot saadaan niiden omistajilta, mikäli he antavat niihin pääsyn. IPFS taas perustuu hallussapidon ja osallistumisen periaatteiden päälle, jolloin useat eri käyttäjät pitävät hallussaan toistensa tiedostoja ja osallistuvat niiden jakamiseen. IPFS toimii siis hyvin ainoastaan silloin, kun ihmiset aktiivisesti osallistuvat tiedostojensa jakamiseen. Esimerkki: Käyttäjä jakaa tietokoneella olevia tiedostoja IPFS:n avulla ja sammuttaa tietokoneen. Muut käyttäjät eivät pääse enää käsiksi kyseisiin tiedostoihin, mutta mikäli tiedostoista on tehty kopioita ja ne on tallennettu muille IPFS:ää käyttäville tietokoneille, ne ovat edelleen saatavilla. (IPFS.IO 2020a, zk Capital 2018.)

3.2.2 Ongelmakohdat

Datan säilöminen ei ole koskaan ilmaista. Todellisuus IPFS:n kohdalla on se, että dataa säilötään yritysomisteisten palvelinten IPFS-nodeilla. Ainakin yhden solmukohdan (eng. node) tulee ylläpitää tiettyä tiedostoa, jotta se on saatavilla IPFS-verkossa. Tähän tarvitaan jokin kannustin, että tiedosto pysyy saatavilla. IPFS-verkossa olevaa sisältöä ei voi hakea ilman yhdyskäytävänä toimivaa tietokonetta (eng. gateway), mikäli käyttäjä ei itse ylläpidä omaa IPFS-nodea. Sisällön hakeminen nopeutuu ilman gatewayta, kun useat käyttäjät lähettävät pyyntöjä kyseiselle sisällölle. Gatewayta käytettäessä tämä prosessi ei ole mahdollinen ja sisällön hakeminen hidastuu, koska gateway saattaa olla sijanniltaan todella kaukana. Paikallisia IPFS-nodeja käytettäessä sisältö haetaan lähimmältä nodelta. Gateway joutuu hakemaan sisällön joltakin IPFS-verkossa olevalta nodelta, jolloin sisällön hakeminen on huomattavasti hitaampaa kuin esimerkiksi nykyistä http-protokollaa käytettäessä. Gatewayta käytettäessä muodostuu ongelma, kun sisältöä haetaan yhdeltä tietyltä koneelta useiden sijaan. Mitä enemmän käyttäjät käyttävät yhtä tiettyä gatewayta, sitä enemmän sisällön hakeminen hidastuu, kun gateway kuormittuu. Mahdollisimman monen käyttäjän tulisi siis ylläpitää sisältöä omalla IPFS-nodellaan. Tätä harva tekee vapaaehtoisesti ilman mitään kannustinta, jolloin IPFS-verkon käyttäjämäärän saaminen kasvuun on hyvin haastavaa. (Ober 2018, Ober 2019, zk Capital 2018.)

3.2.3 Tulevaisuus

Tällä hetkellä oman IPFS-noden pystyttäminen on sen verran haastavaa, että suuren yleisön mukaan saaminen on lähes mahdotonta. Voidaan kuitenkin nähdä mahdollisuus IPFS:n kasvuun, mikäli suuret yritykset ottaisivat sen haltuunsa ja näin ollen ihmiset alkaisivat käyttämään sitä laajemmin. Näin kävi esimerkiksi http-protokollan tapauksessa ja nykyään suurin osa sen käyttäjistä ei edes tiedä tai välitä käyttävänsä kyseistä protokollaa. Käytännössä tarvitaan lisää projekteja ja infrastruktuuria IPFS:n ympärille, jotta se saadaan kasvamaan. Lisäksi natiivi selaintuki yleisimmiltä tarjoajilta kuten Google ja Microsoft on pakollinen, mikäli halutaan että IPFS tulee menestymään verkkoprotokollana. (Ober 2018, Ober 2019, zk Capital 2018.)

3.3 Bitcoin

Bitcoin on tammikuussa 2009 luotu vertaisverkkomallilla toimivaan lohkoketjuun perustuva virtuaalivaluutta, jonka tarkoitus on mahdollistaa suorat ihmisten väliset rahasiirrot ilman pankkien tai muiden yritysten välikäsiä. Bitcoin on yksi ensimmäisistä virtuaalivaluutoista, joka käyttää vertaisverkkoihin sovellettua teknologiaa mahdollistaakseen välittömät valuuttasiirrot. (Frankenfield 2020, Freitas 2020, Nakamoto 2009.)

3.3.1 Lohkoketju

Lohkoketju (eng. blockchain) on yksinkertaisimmillaan sarja aikamerkittyjä ja muuttumattomia datatallenteita, joita hallitsee parvi tietokoneita, joilla ei ole yhtä tiettyä omistajaa. Bitcoineilla tehtävä valuuttasiirto tapahtuu hyödyntäen blockchain-teknologiaa seuraavalla tavalla:

1. Käyttäjä pyytää valuuttasiirtoa.
2. Pyyntö valuuttasiirrosta lähetetään useista solmukohdista koostuvaan vertaisverkkoon.
3. Vertaisverkossa olevat tietokoneet varmistavat käyttäjän tilan ja valuuttasiirron käyttäen tunnettuja algoritmeja.
4. Varmistuksen jälkeen valuuttasiirto kiinnitetään uutena datablokkina muihin valuuttasiirtoihin.
5. Uusi datablokki kiinnitetään olemassa olevaan sarjaan datablokkeja tavalla, joka on pysyvä ja muuttumaton.
6. Valuuttasiirto on valmis.

(Frankenfield 2020, Freitas 2020, Nakamoto 2009.)

3.3.2 Louhinta

Uusia bitcoineja luodaan niin sanotun louhimisprosessin kautta. Louhiminen tarkoittaa käytännössä sitä, että käyttäjät hyödyntävät tietokoneidensa resursseja suorittamalla

aikaisemmin mainittuja valuuttasiirtoja ylläpitäen bitcoinin verkostoa. Louhimiseen käytetään nykyään siihen tarkoitettuja korkeatehoisia tietokoneita, jotka ratkovat erittäin kompleksisia matemaattisia ongelmia sekä varmistavat käyttäjien valuuttasiirtoja. Louhijoille palkinnoksi annettavat uudet bitcoinit valmistuvat siis datablokkien louhimisen myötä. Tarkemmin ottaen louhinnassa yritetään luoda 64-merkkistä heksadesimaalinumeroa, jota kutsutaan nimellä hash eli tarkiste. Louhiva tietokone tuottaa tarkisteita tietyn määrän sekunnissa arvaten kaikkia mahdollisia yhdistelmiä 64 numerosta, joten toisin sanoen sitä voi kutsua lottoarvonnaksi. Toukokuussa 2020 yhden datablokin louhimisesta sai palkinnoksi 6.25 bitcoinia, kun taas 2009 louhimisen ollessa vielä uusi ilmiö siitä sai viisikymmentä bitcoinia. Tässä pitää ottaa huomioon, että datablokkien louhiminen vaikeutuu ja hidastuu mitä pidemmälle ajassa mennään, joten yksityishenkilönä louhimisen avulla vaurastuminen on käytännössä mahdotonta nykyään. Marraskuussa 2020 uuden tarkisteen louhimisen todennäköisyys oli yksi 17 biljoonasta. Louhimisen vaikeustasoa säädetään noin kahden viikon välein tavoitteena pitää louhimistyön määrä tasaisena. Mitä enemmän louhitaan, sitä vaikeammaksi louhittava ongelma muodostuu ja toisinpäin louhintamäärän laskiessa. Louhittavien bitcoinien rajallinen kokonaismäärä on 21 miljoonaa ja niistä on louhittu tällä hetkellä noin 18,5 miljoonaa. (Hayes 2020, Kenton 2020, Blockchain www-sivut 2020.)

3.3.3 Tulevaisuus

Bitcoinin tulevaisuutta on hyvin vaikea arvioida tällä hetkellä, mutta on arvioitu, että niiden louhiminen jatkuu noin vuoteen 2140 asti. Louhimisesta saatavat palkinnot pienenevät jatkuvasti, joten herää kysymys, kuinka louhiminen saadaan pidettyä käynnissä palkintojen vähyydestä huolimatta. Louhimisprosessi saattaa muuttua kokonaan erilaiseksi, mikäli louhimismäärät tippuvat dramaattisesti ja tilanne sitä vaatii. Bitcoinyhteisössä olevat kehittäjät ja louhijat ovat joutuneet usein erimielisyyksiin, joista on syntynyt uusia kryptovaluuttoja sekä uusia versiota bitcoinista sen verkoston protokollan muutosten myötä. Tällaisten muutosten myötä on syntynyt vuonna 2017 mm. Bitcoin Cash sekä Bitcoin Gold, joissa on nostettu esimerkiksi louhittavien datablokkien määrää. (Hayes 2020, Frankenfield 2020.)

4 OIKEUDELLISUUDET

Vertaisverkkoteknologiaa hyödynnetään edelleen aktiivisesti kopiosuojattujen tiedostojen jakamiseen laittomasti. Ihmiset ovat alkaneet käyttämään VPN eli Virtual Private Network -yhteyksiä aktiivisemmin ladatessaan sisältöä laittomasti. VPN-yhteyden avulla vaikeutetaan viranomaisten työtä käyttäjien jäljityksessä ja vältetään mahdolliset sakot. VPN-yhteys luo niin sanotun tunnelin lataajan tietokoneen ja ladattavan tiedoston välille, jolloin lataajan IP-osoitetta on vaikea jäljittää. VPN-palveluita tarjoavat yritykset voidaan kuitenkin pakottaa viranomaisten toimesta luovuttamaan lataajien oikeat IP-osoitteet, mikäli yritys on tallentanut käyttäjistään lokit tietokantaan. Monet VPN-palveluntarjoajat väittävät suojelevansa käyttäjiä tallentamatta heidän oikeita IP-osoitteita tietokantoihinsa, mutta käyttäjien on mahdotonta selvittää, että pitääkö tämä oikeasti paikkansa. (Bischoff 2020, Harber-Lamond 2020.)

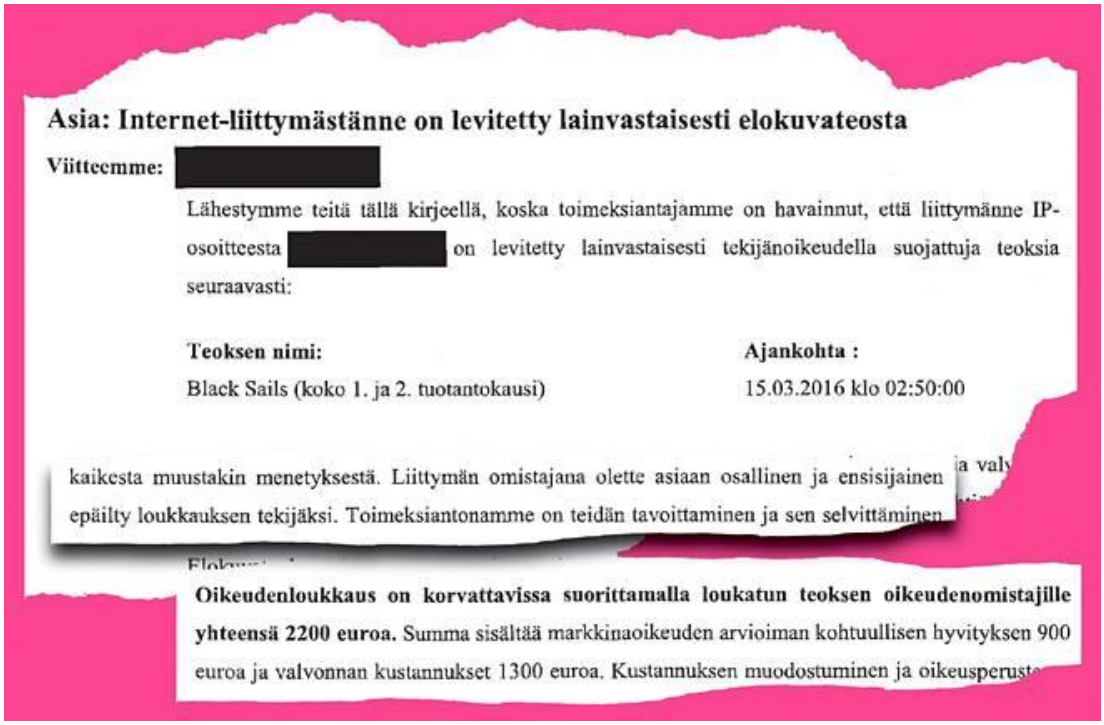
4.1 The Pirate Bay

Yksi tunnetuimmista vertaisverkkoteknologiaa käyttävistä verkkosivustoista on vuonna 2003 perustettu The Pirate Bay. Vuosi sen perustamisen jälkeen sivustoa käytti miljoona käyttäjää ja siellä jaettiin yli 60,000 torrent-tiedostoa. Tämä ruotsalainen BitTorrent-tracker kasvoi maailmanlaajuiseksi piratismin ikoniksi. Palvelussa oli ladattavissa torrentteja esimerkiksi musiikkilevyistä, elokuvista ja peleistä. Pirate Bayn kasvava liikennemäärä ei jäänyt viihdeteollisuuden huomiotta, sillä kopiosuojattujen tiedostojen tekijänoikeuksien omistajat lähettivät useita pyyntöjä torrenttien poistamiseksi sivustolta. Pirate Bayn ylläpitäjät eivät välittäneet kyseisistä pyynnöistä, jolloin paine sivuston sulkemiseksi kasvoi Hollywoodin ja USA:n puolelta. Toukokuun 31. päivänä vuonna 2006 poliisit menivät datakeskukseen Ruotsissa tavoitteena sammuttaa Pirate Bayn palvelimet. Sivusto oli pois käytöstä kolme päivää, kunnes se ilmestyi verkkoon uuden ”The Police Bay” -nimen alla. Poliisien suorittama tehtävä Pirate Bayn sulkemiseksi sai maailmanlaajuisen mediahuomion ja julkisuuden myötä vierailijamäärä Pirate Bayn uudella sivustolla kasvoi valtavasti. Sivuston kolmea perustajaa kohtaan aloitettiin rikostutkinta, jolloin vuonna 2009 alkoi oikeudenkäynti heitä ja rahoittaja Carl Lundstromia vastaan. Heidät tuomittiin vuodeksi vankilaan ja

yhteensä 3 620 000 dollarin sakoin. Tuomitut valittivat tuomioistaan 2010 ja saivat lyhennettyä niitä, mutta sakot nousivat yli 6,5 miljoonaan dollariin. (Van Der Sar 2013, Williams 2019, De Looper 2014, Seppala 2014.)

Laittomasti torrentteja lataavia käyttäjiä on harvoin sakotettu, mutta annetut sakot ovat olleet mittavia. Tekijänoikeuksien omistajat haastoivat käyttäjiä eniten oikeuteen 2000-luvun loppupuolella. Käyttäjiltä pyydettiin jättimäisiä summia ja suurin osa tapauksista soviteltiin oikeudessa. Nykyään käyttäjiä harvemmin haastetaan oikeuteeen, mutta työ laittomuuksia vastaan jatkuu edelleen ja yksittäisiä käyttäjiä vastaan tehdyt haasteet on ulkoistettu pienemmille toimijoille, joita kutsutaan niin sanotuiksi tekijänoikeustrolleiksi. Nämä toimijat jäljittävät käyttäjiä, jotka lataavat torrentteja oikeiden IP-osoitteidensa kautta ja lähettävät heille sovittelukirjeitä, joissa käyttäjiä pyydetään maksamaan esimerkiksi kolmen tuhannen dollarin sakot välttääkseen sadan tuhannen sakot tapauksen mennessä oikeuteen. Nämä kirjeet eivät ole laillisesti pitäviä dokumentteja. (Bischoff 2020, Maxwell 2017.)

4.2 Suomessa tapahtunutta



Asia: Internet-liittymästänne on levitetty lainvastaisesti elokuvateosta

Viitteemme: [redacted]

Lähestymme teitä tällä kirjeellä, koska toimeksiantajamme on havainnut, että liittymänne IP-osoitteesta [redacted] on levitetty lainvastaisesti tekijänoikeudella suojattuja teoksia seuraavasti:

Teoksen nimi:	**Ajankohta :**
Black Sails (koko 1. ja 2. tuotantokausi)	15.03.2016 klo 02:50:00

kaikesta muustakin menetyksestä. Liittymän omistajana olette asiaan osallinen ja ensisijainen epäilty loukkauksen tekijäksi. Toimeksiantonamme on teidän tavoittaminen ja sen selvittäminen

Oikeudenloukkaus on korvattavissa suorittamalla loukatun teoksen oikeudenomistajille yhteensä 2200 euroa. Summa sisältää markkinaoikeuden arvioiman kohtuullisen hyvityksen 900 euroa ja valvonnan kustannukset 1300 euroa. Kustannuksen muodostuminen ja oikeusperust

Kuva 8. Leikkaus Hedman Partnersin lähettämästä kiristyskirjeestä. (Helsingin Sanomat 2017.)

Suomen tunnetuin kiristyskirjeitä lähettänyt yritys kulki nimellä Hedman Partners. Hedman Partners sai ulkomailta tiedon, että esimerkiksi jotakin elokuvaa jaetaan laittomasti internetissä. Ulkomailta tulevat todisteet on saatu tekijänoikeusrekistereistä ja torrent-sovellusten seurantaohjelmien lokitiedostoista. Lakitoimisto ei siis hankkinut todisteita itse, vaan ne tulivat heille ulkomailta. Lakifirmat voivat vaatia Markkinaoikeudelta tekijänoikeusrikkomuksesta epäillyn henkilön IP-osoitteen tunnistamista, jolloin Markkinaoikeus voi velvoittaa teleoperaattorin luovuttamaan IP-osoitteeseen liitettävät yhteystiedot. Hedman Partners lähetti kiristyskirjeitä (kuva 8) noin 100–200 käyttäjälle kerralla, mutta vain pieni osa tapauksista vietiin oikeuteen, vaikka käyttäjät jättivät uhkasakot maksamatta. Vuonna 2015 eräs käyttäjä oli saanut kirjeen Hedman Partnersilta, jossa vaadittiin käyttäjää maksamaan 2100 euron sakot Hedman Partners Oy:n pankkitilille. Käyttäjä ei suostunut maksamaan sakkoja ja lähetti vastauksen Hedman Partnersille, jolloin käyttäjä haastettiin markkinaoikeuteen. Vuonna 2016 markkinaoikeus julkaisi päätöksen, jossa Hedman Partners voitti oikeudenkäynnin. Käyttäjä joutui maksamaan vahingonkorvauksia sekä oikeudenkäyntikuluja, koska markkinaoikeus katsoi kantajien esittäneen uskottavan näytön siitä, että vastaaja oli

itse ladannut kantajien teokset ja jakanut niitä eteenpäin. Tämä perustui Hedman Partnersin tekemään tekniseen selvitykseen käyttäjän internet-liittymän lokitiedoista, sillä käyttäjän yhteydenotot Hedman Partnersin asiamieheen liittyivät ajallisesti suoraan heidän harjoittamaan valvontatoimintaan käyttäjän avoimessa langattomassa verkossa. Tuomiota ei siis langetettu pelkästään käyttäjän IP-osoitteen perusteella, vaan käyttäjän omat kertomukset internetissä vahvistivat käsityksen syyllisyydestä. Vuonna 2017 markkinaoikeus taas hylkäsi Hedman Partnersin nostaman kanteen toista henkilöä kohtaan, koska puutteellisen näytön takia ei voitu todistaa käyttäjän suorittaneen lataukset henkilökohtaisesti. Käyttäjän langaton verkkoasema oli suojaamaton, jolloin kuka tahansa lähellä oleva on voinut ottaa yhteyden siihen. Lisäksi käyttäjän kovalevyistä ja verkkolevyistä ei löytynyt asiantuntijan tarkastuksessa viitteitä BitTorrent-ohjelmistoihin tai laittomasti ladattuihin tiedostoihin. (Raeste 2017, Piraattipuolue 2017, Markkinaoikeus 2017, MuroBBS www-sivut 2016).

Toinen taho, jolta suomalaiset ovat saaneet kiristyskirjeitä liittyen tekijänoikeuksilla suojatun sisällön laittomaan lataamiseen on tanskalainen NjordLaw-lakifirma. Tekijänoikeustrollit toimivat aktiivisimmin vuonna 2015 kun ilmiö oli Suomessa uusi, jolloin luovutuspyyntöjä tehtiin yhteensä 211 kappaletta. Kiristyskirjebisnes itsessään on maailmanlaajuinen ilmiö, josta esimerkkejä löytyy mm. Australiasta, Iso-Britanniasta, Yhdysvalloista sekä Ruotsista. Samat henkilöt ja yritykset löytyvät usein taustalta, kuten Tecxipio GmbH, Guardaley Ltd sekä Maverick Eye Ltd nimien alla toimivat Crystal Bay Corporation, Crystalis Entertainment, Interallip LLP ja Copyright Collections Ltd. Nämä niin sanotut pöytälaatikkoyritykset ostivat yksittäisiin elokuviin tai tv-sarjoihin tekijänoikeuksia, joiden avulla he saivat kirjeitä lähetettyä, vaikka yrityksellä ei ollut mitään muuta liiketoimintaa. Iso-Britanniassa valtio antoi virallisen toimintaohjeen kansalaisille kiristyskirjeitä varten. (MuroBBS www-sivut 2017, Rantanen 2016.)

5 POHDINTA

Internet itsessään on mullistanut tiedon jakamisen ja leviämisen uskomattomalla tavalla, jota ihmiset itseni mukaan lukien pitävät liikaa itsestäänselvyytenä. Sen kehitys on jo päässyt niin pitkälle, että mikään taho ei pysty enää kunnolla kontrolloimaan tai sensuroimaan siellä jaettavaa sisältöä. Valtioiden kuten esimerkiksi Kiinan tekemien sensurointitoimenpiteiden on huomattu aiheuttavan vastareaktion suuressa osassa käyttäjiä varsinkin tilanteissa, joissa ihmisillä ei ole korvaavaa vaihtoehtoa sensuroitavalle alustalle. Kiellettäessä ihmisten suosiossa olleita ja hankalasti korvattavia alustoja niiden käyttäjät, joilla aikaisemmin ei ole ollut aikaa tai kiinnostusta opetella kiertämään sensuurin aiheuttamia rajoituksia on sen myötä vahvemmat motiivit päästä käsiksi sensuroituun sisältöön. Esimerkiksi Iranissa Google Readerin käyttö kasvoi valtavasti, kun valtio sensuroi kansalaisiltaan tiettyjä verkkosivuja ja ihmiset kiersivät sensuurin avaamalla sivut tekstimuotoisena Google Readerissa. Se mitä ihmisiltä yritetään kieltää, niin sitä seuraavaksi halutaan eniten. (Hobbs, Roberts 2018, Laurenson 2014, King, Pan, Roberts 2013.)

Vuonna 2011 52 prosenttia Yhdysvaltojen verkkoliikenteen lähetyskaistasta oli BitTorrent -protokollassa jaettua sisältöä, mutta vuoteen 2015 mennessä tämä verkkoliikenne oli vähentynyt noin 27 prosenttiin laadukkaiden ja kohtuuhintaisten striimauspalveluiden kuten Netflix yleistyessä. Striimauspalveluiden ongelmaksi on kuitenkin muodostunut sisällön eksklusiivisuus eri palveluissa, jolloin sisällön jakautuessa nykyään useaan eri palveluun käyttäjän tulisi maksaa niistä jokaisesta erikseen per kuukausi nähdäkseen kaikkea haluamaansa sisältöä. Tämä ongelma on tuonut ihmisiä takaisin laittoman lataamisen pariin. Mielestäni tv-viihteen laiton lataaminen vähenisi huomattavasti, mikäli kaikki sisältö keskittyisi yhteen kuukausimaksulliseen palveluun. Tämä on toki vain spekulointia omalta osaltani, mutta on vaikea uskoa, että läheskään yhtä suuri osa ihmisistä jaksaisi nähdä vaivaa sisältöjen lataamisessa laittomasti, kun kaikki olisi helposti saatavilla yhdestä kohtuuhintaisesta palvelusta. (Bode 2018, Sandvine 2018.)

Vertaisverkkojen toimintaperiaate on teorian tasolla toimiva ja lupaava vaihtoehto nykyiselle keskitetylle internetille ja esimerkiksi BitTorrent -protokollan käyttö jatkuu

tälläkin hetkellä aktiivisena siellä jaetun laittoman sisällön sakottamisesta huolimatta. Ihmiset ovat ottaneet entistä aktiivisemmin VPN-yhteyksiä käyttöön kiertääkseen mahdolliset sakot, jolloin laitonta sisältöä lataavaan IP-osoitteen jäljittäminen vaikeutuu. Todellisuudessa esimerkiksi IPFS-protokolla vaatii vielä huomattavan paljon kehitystä toimiakseen laajemmin nykyisten toimintamallien rinnalla tai niiden korvaajana. Vertaisverkkoratkaisujen kehitys ja tuki varmasti lisääntyy, mikäli valtiot haluavat tulevaisuudessa kontrolloida verkon käyttäjiä ja sisältöä enemmän. Mitä enemmän internetin sisältöä yritetään sensuroida, sitä voimakkaamman vastareaktion se aiheuttaa verkon käyttäjissä. Maailmassa vallitseva markkinatalous ei myöskään tue vertaisverkkomallien toimintaperiaatetta, koska suurin osa sisällöstä on voittoa tavoittelevien yksityisomisteisten yritysten hallussa.

Pilvipalveluiden kasvattaessa valtaansa internetissä niiden muovautuessa enemmän vertaisverkkomalleista hybridimallin mukaiseksi palvelinten sijainnin hajautumisen myötä herää kysymys, mikä on itse vertaisverkkoteknologian tulevaisuus. Tarvitaanko vertaisverkkoteknologiaa tulevaisuudessa muuhun, kuin käyttäjien väliseen tiedostojen jakamiseen, jos pilvipalveluiden infrastruktuurit hajautuvat tarpeeksi tehokkaasti mahdollistaen tehokkaat yhteydet ja lyhyet vasteajat kaikille käyttäjille ympäri maailmaa. Vastauksena tähän pitää kuitenkin sanoa, että pilvipalveluiden taustalla hyödynnetään vertaisverkon teknologiaa edelleen huomattavissa määrin datan tallennuksen ja big datan yhteydessä. Voisiko tulevaisuudessa olla mahdollista jonkinlainen vertaisverkkojen ja pilvipalveluiden yhdistyminen, mikäli datamäärät jatkavat kasvuaan esimerkiksi entistä korkearesoluutioisemman videostriimauksen myötä. Tästä esimerkkinä Netflix, jossa jokainen käyttäjä sitoutuisi katsoessaan sisältöä myös jakamaan sitä muille. Tämä vaatisi toki valtavaa kehitystyötä yritysten osalta, koska jaettava sisältö pitäisi jakaa palasina kaikille käyttäjille ja sen koordinointi tuottaisi varmasti haasteita. (Kisembe, Jeberson 2017.)

Bitcoinin noustessa kirjoitushetkellä joulukuun alussa 2020 kaikkien aikojen ennätyslukemiin lähelle 17,000 dollaria se herättää edelleen mielenkiintoa rankasti kritisoitua ja Warren Buffetin tyrmäämää lohkoketjun voimin toimivaa kryptovaluuttaa kohtaan. Vuoden 2020 aikana bitcoinin arvo on noussut 170 %, joka kertoo sen arvon epävakaisuudesta, mutta myös sen taustalla olevan lohkoketjun potentiaalista. Bitcoinin ollessa vain yksi esimerkki lohkoketjun hyödynnettävyydestä herää kysymys, että mihin

kaikkeen sitä oikeastaan voidaan käyttää ja mikä sen todellinen potentiaali on, sillä se kuitenkin mahdollistaa käytännössä minkä tahansa arvoa omaavan asian tallennuksen, seurannan ja vaihtokaupan vähentäen riskejä ja leikaten kuluja kaikilta osapuolilta. Onkin ennustettu, että tulevaisuudessa entistä suuremmat yritykset ja jopa pankit ja valtiot ottavat vertaisverkkoteknologiaan perustuvan lohkoketjun käyttöönsä palveluiden kehittyessä. (Schlapkohl 2020, Jolly 2020.)

Tämän työn kautta sain itse lisää konkreettisia esimerkkejä vertaisverkkoteknologian käyttökohteista ja pääsin perehtymään sen toimintaan pintaa syvemmältä. Bitcoinin hyödyntämä lohkoketju oli sanana tuttu, mutta en ollut koskaan perehtynyt siihen sen syvällisemmin ja olin hieman yllättynyt sen perustuessa samaan teknologiaan kuin itselläni käytössä olleiden VoIP (Voice over Internet Protocol) -puheviestintäohjelmien arkkitehtuuri. Tulevaisuudessa eniten herättää mielenkiintoa vertaisverkkoteknologian mahdollistama laiton toiminta, ottavatko yritykset entistä kovempia toimia rikollisuuden estämiseksi, mikäli striimauspalveluiden käyttö vähenisi entisestään ja ihmiset alkaisivat lataamaan sisältöä kasvavissa määrin laittomasti. MuroBBS-verkkofoorumilla käyttäjä kirjoitti 23. päivä marraskuuta 2020 saaneensa Hedman Partnersilta kiristyskirjeen kolmen vuoden tauon jälkeen, joka laittaa miettimään niin sanottujen tekijänoikeustrollien toimintaa tulevaisuudessa sikäli moraalisesti väärin olevan laittoman toiminnan valvontatoimijana, kuitenkin vääriä keinoja käyttäen ja ihmisiä kohtuuttomilla summilla kiristäen. Mikäli tällaista toimintaa halutaan ruveta valvomaan ja rankaisemaan tulevaisuudessa, tulee sitä hoitavan toimijan olla omasta mielestäni valtion virallistama eikä jokin hämärästi tietoja keräävä pöytälaatikkoyritys. Kuten aikaisemmin työssä mainitsin, tällainen toiminta aiheuttaa käyttäjissä tunnetusti vastareaktion, ja mitä enemmän kiristyskirjeitä lähetetään, sitä enemmän käyttäjät tulevat parantamaan omaa yksityisyyttään vapaasti tietoa liikuttavassa verkossa sen ollessa hyvinkin avoin ja sensuroimaton Suomessa. (MuroBBS www-sivut 2020.)

LÄHTEET

Addaquay, K. 2018. A Beginner's Guide to IPFS. Viitattu 21.9.2020.

https://hackernoon.com/a-beginners-guide-to-ipfs-20673fedd3f

Binance Academy. 2020. Peer-to-Peer Networks Explained. Viitattu 26.11.2020.

https://academy.binance.com/en/articles/peer-to-peer-networks-explained

Bischoff, P. 2020. What is Torrenting? Is it Safe? Is it illegal? Are you likely to be caught? Viitattu 18.11.2020.

https://www.comparitech.com/blog/vpn-privacy/is-torrenting-safe-illegal-will-you-be-caught/

Bitcoinin www-sivut. 2020. Frequently Asked Questions. Viitattu 27.11.2020.

https://bitcoin.org/en/faq

Blockchainin www-sivut. 2020. Network Difficulty. Viitattu 27.11.2020.

https://www.blockchain.com/charts/difficulty

Bode, K. 2018. The Rise of Netflix Competitors Has Pushed Consumers Back Toward Piracy. Viitattu 2.12.2020.

https://www.vice.com/en/article/d3q45v/bittorrent-usage-increases-netflix-streaming-sites

De Looper, C. 2014. History of The Pirate Bay: Internet Outlaw or Internet File-Sharing Freedom Fighter? Viitattu 19.11.2020.

https://www.techtimes.com/articles/22362/20141217/history-pirate-bay.htm

Educative.io. 2020a. What are P2P and client-server networks? Viitattu 12.10.2020.

https://www.educative.io/edpresso/what-are-p2p-and-clientserver-networks

Educative.io. 2020b. Kuva vertaisverkkojen ja asiakas-palvelin periaatteen toiminta-mallista. Viitattu 12.10.2020.
https://www.educative.io/edpresso/what-are-p2p-and-clientserver-networks

Frankenfield, J. 2020. Bitcoin. Viitattu 27.11.2020.
https://www.investopedia.com/terms/b/bitcoin.asp

Freitas, C. 2020. Bitcoin explained simply: everything you need to know. Viitattu 27.11.2020.
https://currency.com/bitcoin-explained-simply

Frystyk, H. 1994. Kuva internetprotokollapinosta. Viitattu 21.9.2020.
https://www.w3.org/People/Frystyk/thesis/TcpIp.html

Harber-Lamond, M. 2020. How to use a VPN to torrent safely. Viitattu 18.11.2020.
https://www.tomsguide.com/features/how-to-use-a-vpn-to-torrent-safely

Hayes, A. 2020. What Happens to Bitcoin After All 21 Million Are Mined? Viitattu 27.11.2020.
https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/

Hobbs, W.R., Roberts, M.E. 2018. How Sudden Censorship Can Increase Access to Information. Viitattu 2.12.2020.
https://www.cambridge.org/core/journals/american-political-science-review/article/how-sudden-censorship-can-increase-access-to-information/A913C96E2058A602F611DFEAC43506DB

IPFS.IO. 2020a. What is IPFS? Viitattu 9.10.2020.
https://docs.ipfs.io/concepts/what-is-ipfs/

IPFS.IO. 2020b. How IPFS works. Viitattu 9.10.2020.
https://docs.ipfs.io/concepts/how-ipfs-works/

Jolly, J. 2020. Bitcoin price hits all-time high of almost $20,000. Viitattu 2.12.2020.

https://www.theguardian.com/technology/2020/nov/30/bitcoin-price-hits-all-time-high-of-almost-20000

Kenton, W. 2020. Bitcoin Mining. Viitattu 27.11.2020.

https://www.investopedia.com/terms/b/bitcoin-mining.asp

King, G., Pan, J., Roberts, M.E. 2013. How Censorship in China Allows Government Criticism but Silences Collective Expression. Viitattu 2.12.2020.

https://gking.harvard.edu/files/gking/files/censored.pdf

Kisembe, P., Jeberson, W. 2017. Future of Peer-To-Peer Technology with the Rise of Cloud Computing. Viitattu 2.12.2020.

https://www.researchgate.net/publication/319579735_Future_of_Peer-To-Peer_Technology_with_the_Rise_of_Cloud_Computing

Laurenson, L. 2014. The Censorship Effect. Viitattu 2.12.2020.

https://techcrunch.com/2014/05/03/business-and-censorship

Li, J. 2007. A Survey of Peer-to-Peer Network Security Issues. Viitattu 27.11.2020.

https://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/

Markkinaoikeus. 2016. MAO:419/16. Viitattu 19.11.2020.

https://www.markkinaoikeus.fi/fi/index/paatokset/teollisjatekijanoikeudelli-setasiat/teollisjatekijanoikeudellisetasiat/1467628378764.html

Markkinaoikeus. 2017. MAO:55/17. Viitattu 18.11.2020.

https://www.markkinaoikeus.fi/fi/index/paatokset/teollisjatekijanoikeudelli-setasiat/teollisjatekijanoikeudellisetasiat/1486457257268.html

Maxwell, A. 2017. Finnish Government Investigates as Tens of Thousands Face Piracy ‘Fines’. Viitattu 19.11.2020.

https://torrentfreak.com/finnish-government-investigates-as-tens-of-thousands-face-piracy-fines-170126/

MuroBBS www-sivut. 2016. Hedman Partnersilta kiristyskirje. Viitattu 18.11.2020.

https://murobbs.muropaketti.com/threads/hedman-partnersilta-kiristyskirje.1213329/

MuroBBS www-sivut. 2020. Hedman Partnersilta kiristyskirje, sivu 1752. Viitattu 2.12.2020.

https://murobbs.muropaketti.com/threads/hedman-partnersilta-kiristyskirje.1213329/page-1752

Nakamoto, S. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Viitattu 27.11.2020.

https://bitcoin.org/bitcoin.pdf

Neagu, C. 2019. What are P2P (peer-to-peer) networks and what are they user for? Viitattu 12.9.2020.

https://www.digitalcitizen.life/what-is-p2p-peer-to-peer

Ober, M. 2018. The IPFS Cloud. Viitattu 13.10.2020.

https://medium.com/pinata/the-ipfs-cloud-352ecaa3ba76

Ober, M. 2019. The IPFS Gateway Problem. Viitattu 13.10.2020.

https://medium.com/pinata/the-ipfs-gateway-problem-64bbe7eb8170

Piraattipuolue. 2017. Kiristyskirje.fi. Viitattu 18.11.2020.

http://www.kiristyskirje.fi/

Qureshi, H. 2019. P2P Networking. Viitattu 6.11.2020.

https://nakamoto.com/p2p-networking/

Raeste, J-P. 2017. Juristit vaativat sarjoja ja elokuvia ladanneilta rahaa uhkauskirjeillä – “Lakimieheltä on turha kysyä moraalista”. Viitattu 19.11.2020.

https://www.hs.fi/talous/art-2000005052577.html

Rantanen, A. 2016. Piratismista voi pätkähtää karhukirje – lakifirmat suitsivat laitonta lataamista. Viitattu 19.11.2020.

https://www.ksml.fi/paikalliset/2568594

Rehman, J. 2017. Kuva keskitetystä, hajautetusta ja jaetusta mallista. Viitattu 26.11.2020.

https://www.itrelease.com/2017/11/difference-centralized-decentralized-distributed-processing/

Rosic, A. 2016. What is Blockchain Technology? Viitattu 27.11.2020.

https://blockgeeks.com/guides/what-is-blockchain-technology/

Sandvine. 2018. The Global Internet Phenomena Report. Viitattu 2.12.2020.

https://www.sandvine.com/hubfs/downloads/phenomena/2018-phenomena-report.pdf

Savolainen, P. 2020. Summary of the BitTorrent Protocol. Viitattu 26.11.2020.

https://www.cs.helsinki.fi/webfm_send/1330

Schlapkohl, K. 2020. The future of blockchain. Viitattu 2.12.2020.

https://www.ibm.com/blogs/blockchain/2020/04/the-future-of-blockchain/

Seppala, T. 2014. The Pirate Bay shutdown: the whole story (so far). Viitattu 19.11.2020.

https://www.engadget.com/2014-12-16-pirate-bay-shutdown-explainer.html

Van Der Sar, E. 2013. The Pirate Bay Turns 10 Years Old: The History. Viitattu 11.11.2020.

https://torrentfreak.com/the-pirate-bay-turns-10-years-old-the-history-130810/

Washbourne, L. 2015. A Survey of P2P Network Security. Viitattu 12.10.2020.

https://arxiv.org/ftp/arxiv/papers/1504/1504.01358.pdf

Williams, J. 2019. The Fascinating History of PirateBay. Viitattu 19.11.2020.

https://feedsportal.com/the-fascinating-history-of-piratebay/

Yeferny, T. 2019. Kuva vertaisverkkomallien arkkitehtuureista. Viitattu 30.11.2020.

https://www.researchgate.net/figure/P2P-architectures-at-a-glance-a-Centralized-architecture-b-Pure-P2P-architecture_fig2_332539196

zk Capital. 2018. IPFS Analysis. Viitattu 30.11.2020.

https://ipfs.io/ipfs/QmRU1jJ1kNd9fTzjFwM4X9YtA2wfXN1W2eFK7mgTMJ8xgK

zk Capital. 2018. Kuva IPFS:n toimintaperiaatteesta. Viitattu 30.11.2020.

https://medium.com/zkcapital/ipfs-the-distributed-web-e21a5496d32d