Matias Vuorio

BITCOIN FIAT-VALUUTTOJEN KORVAAJANA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Vuorio, Matias
Bitcoin Fiat-valuuttojen korvaajana
Jyväskylä: Jyväskylän yliopisto, 2022, 26 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Halttunen, Veikko

Kryptovaluuttojen ja niitä hyödyntävän lohkoketjuteknologian yleistyessä on niitä tutkittu paljon positiivisten vaikutusten ja mahdollisuuksien näkökulmasta. Tämä tutkimus toteutettiin, sillä kaikesta ”hehkutuksesta” ja teknologisista saavutuksista huolimatta, tulisi teknologiaa kryptovaluuttojen takana tarkastella myös kriittisestä näkökulmasta. Tämä tutkimus on toteutettu kirjallisuuskatsauksena, jonka tarkoitus on selvittää riskejä, joita käytössä olevien valuuttojen korvaaminen bitcoinilla toisi tullessaan. Tutkimuksessa esiin tulleet riskit voidaan jakaa kolmeen kategoriaan, jotka liittyvät niiden skaalautuvuuteen, rahatalouteen sekä ympäristövaikutuksiin. Osa tutkimuksessa ilmenneistä riskeistä voisi olla minimoitavissa, mutta toisiin ei toistaiseksi löydy yksiselitteistä ratkaisua. Tutkimuksessa tunnistettiin bitcoinin vakavimman riskin olevan sen käyttämä konsensusmekanismi proof-of-work, joka pyrkii varmistamaan verkon solmujen toimivan protokollan mukaisesti. Proof-of-work mekanismin käyttö on suoraan tai epäsuoraan liitettävissä kaikkiin aiemmin mainittuihin riskikategorioihin.

Asiasanat: Fiat-raha, lohkoketju, bitcoin, konsensusmekanismi, proof-of-work, solmu

ABSTRACT

Vuorio, Matias
Bitcoin as a substitute for fiat-currencies
Jyväskylä: University of Jyväskylä, 2022, 26 pp.
Information Systems Bachelor's thesis
Supervisor: Halttunen, Veikko

Increasing popularity of cryptocurrencies and blockchain technology has led to a lot of research regarding possibilities of these technologies. This research was conducted to provide critical perspective despite all the technological accomplishments and hype surrounding the subject. This literature review aims to point out the risks of replacing fiat-currencies with bitcoin. The results of this research can be divided into three categories which are scalability-, monetary economy- and environmental risks. Part of the risks could be minimized but for now there is no simple solution to all of them. This research found out that the greatest risk was consensus mechanism proof-of-work that bitcoin utilizes. The goal of proof-of-work is to make sure that nodes act according to protocol. Utilization of proof-of-work is either directly or indirectly linked to all previously mentioned risk categories.

Keywords: Fiat-currency, blockchain, bitcoin, consensus mechanism, proof-of-work, node

TERMILUETTELO

Fiat-raha	Valtion liikkeelle laskevaa valuuttaa, jonka arvo perustuu kysyntään ja tarjontaan eikä se ole sidottu esimerkiksi kultaan (Suomen-kultareservi, 2021)
Transaktio	Valuutan siirto osoitteesta toiseen
Volatiliteetti	Arvon vaihtelu
Solmu	Verkossa toimiva käyttäjän laite
Hash	Lohkoketjun lohkon vahvasti yksilöivä tiiviste
Dark web	Anonyymi verkko, jota voidaan käyttää mm. valtioiden sensuurin kiertämiseen ja rikoksiin
Latenssi	Verkon viive. Kuvastaa esimerkiksi transaktion prosessointiin vaadittavaa aikaa
Konsensus	Solmujen välinen yhteisymmärrys tai yksimielisyys

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Erilaiset kryptovaluutat (engl. cryptocurrencies) ovat tulleet kansan tietoisuuteen viimeisen vuosikymmenen aikana. Tietoisuus aiheesta on lisääntynyt muun muassa mediassa esiintyvän kauhistelun sekä rikastumistarinoiden seurauksena. Kauhistelun ja rikastumistarinoiden taustalla on kryptovaluutoille tyypillinen poikkeuksellisen korkea volatilisuus eli arvon vaihtelu. Erilaisia kryptovaluuttoja on olemassa tuhansia, mutta niistä tällä hetkellä tunnetuimpia, vaihdetuimpia ja merkittävimpiä ovat Bitcoin ja Ethereum (Royal, 2022).

Kryptovaluutat tai toiselta nimeltään virtuaalivaluutat ovat digitaalisia arvonkantajia, joita vaihdetaan ja ansaitaan tietoverkkojen välityksellä (Johansson, 2021). Kryptovaluuttojen ansainta- ja vaihdanta prosesseihin liittyy olennaisesti 2000-luvun merkittävimmäksi keksinnöksi kutsuttu lohkoketjuteknologia, joka vastaa tietojen virheettömyydestä ja muuttumattomuudesta. Virtuaalivaluutoilla voidaan teoriassa ostaa palveluja ja hyödykkeitä, mutta tällä hetkellä ne useimmiten nähdään spekulatiivisena sijoituskohteena, millä tarkoitetaan, että Fiat-valuutalla ostetut kryptovaluutat on useimmiten myöhemmin tarkoitus vaihtaa takaisin Fiat-valuutaksi taloudellisten voittojen toivossa (Johansson, 2021: Pernice & Scott, 2021). Toisin kuin Fiat-raha, virtuaalivaluuttoja ei ole laskettu kiertoon keskuspankin tai muun viranomaisentahon toimesta, eikä näin ollen niihin kohdistu samankaltaista valvontaa tai lainsäädäntöä kuin Fiat-valuuttoihin (Johansson, 2021). Luotettavan kolmannen osapuolen puuttuminen arvontakaajana sekä maksunvälittäjänä sallii valuuttojen käyttäytymisen uniikilla tavalla, mihin perehdytään tarkemmin tässä tutkielmassa.

Tutkimus toteutetaan kirjallisuuskatsauksena ja siinä pyritään lähdekirjallisuuden avulla vastaamaan alla esitettyyn tutkimuskysymykseen.

1. Minkälaisia riskejä Fiat-rahan korvaamiseen bitcoinilla liittyy?

Tutkimuksen tekeminen tästä näkökulmasta on perusteltua, sillä viime aikoina tehdyt tutkimukset ovat keskittyneet pääosin vain kryptovaluuttojen ja lohkoketjuteknologian mahdollisuuksiin. Tutkimuksessa käytetyt lähteet ovat vertaisarvioituja ja Julkaisufoorumin luokituksen mukaan pääosin vähintään tasoa

2, mikä viittaa lähteiden olevan luotettavia. Julkaisufoorumin luokitus on tarkistettu osoitteesta. https://www.tsv.fi/julkaisufoorumi/haku.php. Tutkielmassa käytettyjä lähteitä on etsitty Jykdokista ja Google Scholarista hakusanoilla ”bitcoin sustainability”, ”future of cryptocurrencies”, ”bitcoin environmental factors” sekä ”bitcoin scalability”. Tutkielmassa viitataan osaan käsitteistöstä niiden englannin kielisillä nimillä, sillä niille ei ole olemassa asianmukaista suomennosta. Lisäksi tutkielmassa kryptovaluutta bitcoinin valuuttayksikköön (BTC) viitatessa käytetään pientä alkukirjainta, kun taas Bitcoin verkkoon tai järjestelmään viitatessa käytetään isoa alkukirjainta.

Tutkielma koostuu kolmesta luvusta, joista ensimmäisessä tarkastellaan kryptovaluuttojen ja erityisesti bitcoinin ominaisuuksia ja niiden käytön mahdollistavia teknologioita. Toisessa luvussa tarkastellaan riskejä, joita tällä hetkellä käytössä olevien Fiat-valuuttojen, kuten euron ja Yhdysvaltain dollarin korvaaminen kryptovaluutta bitcoinilla toisi tullessaan. Riskejä tarkastellaan muun muassa yhteiskunnan, ympäristön, käytön skaalautuvuuden ja rikollisuuden näkökulmista. Viimeisessä luvussa kerrataan ja kootaan yhteen tutkielman kannalta keskeisin asiasisältö.

2 KRYPTOVALUUTAT

Kryptovaluutat, tai toiselta nimeltään virtuaalivaluutat, ovat digitaalisia arvonkantajia, joita vaihdetaan ja ansaitaan tietoverkkojen välityksellä (Johansson, 2020). Niiden toiminta perustuu täysin teknologisiin ratkaisuihin, eikä taustalla ole luotettavia kolmansia osapuolia, kuten instituutiota tai pankkeja. Valuuttojen ollessa puhtaasti teknologiapohjaisia, vältytään ylimääräisiltä kaupankäynnin kustannuksilta etenkin valtioiden välisessä kaupankäynnissä. Transaktiot eli valuutan siirrot ovat Fiat-valuuttoihin verraten anonyymejä, mikä mahdollistaa tasa-arvoisen kaupankäynnin ja muun muassa valtiolliselta sensuurilta välttymisen. Tällä hetkellä kryptovaluuttoja käytetään suurimmilta osin sijoituskohteena ja ne soveltuvat teoriassa hyvin sijoitussalkun hajautukseen. Tämä johtuu siitä, että indeksien ja arvopapereiden hinnanmuutokset eivät suoraan heijastu kryptovaluuttoihin ja talouden kärsimisellä voi olla jopa positiivinen vaikutus kryptovaluuttojen kursseihin.

Ensimmäinen kryptovaluutta syntyi vuonna 2009, mutta kierrossa olevien kryptovaluuttojen sekä niiden omistajien määrä on kasvanut räjähdysmäisesti viime vuosikymmenen aikana. Esimerkiksi tammikuussa vuonna 2017 tehdyssä tutkimuksessa kryptovaluutta bitcoinia oli kierrossa 16 miljardin Yhdysvaltain dollarin arvosta (Vranken, 2017). Ja marraskuussa 2019 bitcoin oli maailman kuudenneksi suurin kierrossa oleva valuutta (Saiedi, 2021). Viime vuosikymmenen räjähdysmäisen kasvun osasyynä on uudelle teknologialle tyypillinen ”hehkutus” sekä aiheeseen liittyvien ääritapauksien kuten äkkirikastumisten ja huijausten saama mediasuosio. Tässä luvussa tarkastellaan kryptovaluuttojen ominaisuuksia, mahdollisia käyttötarkoituksia sekä motiiveja niiden omistamiselle. Luvussa tarkastellaan myös kryptovaluuttojen historiaa ja nykytilannetta, konsensusmekanismeja sekä monikäyttöistä lohkoketjuteknologiaa kryptovaluuttojen näkökulmasta.

2.1 Kryptovaluuttojen määritelmä ja ominaisuudet

Kryptovaluutoiksi luetaan tyypillisesti valuutat, jotka sijaitsevat hajautetussa (engl. decentralized) vertaisverkossa (engl. peer-to-peer) (P2P), eivätkä ole käsin kosketeltavissa (Vranken, 2017). Hajautetulla vertaisverkolla tarkoitetaan verkkoa, jonka toiminta ei perustu yksittäisiin keskuspalvelimiin. Sen sijaan tietokannan hallinnasta vastaavat toisiinsa nähden tasavertaiset, maantieteellisesti hajautetut verkossa toimivat laitteet, joita kutsutaan solmuiksi (engl. node) (Vermaak, 2021). Solmujen tehtävä on todentaa transaktioiden oikeellisuus ja säilyttää tilikirjaa aiemmista transaktioista. Tällaisella verkon hajautetulla mallilla saavutetaan keskitettyjä järjestelmiä parempi vikasietoisuus sekä tietoturva hyökkäyksiä vastaan, mitkä ovat olleet kriittisiä menestystekijöitä ensimmäisen kryptovaluutan bitcoinin ”onnistumiselle” (Franco, 2015).

Merkittävin ero Fiat-rahaan nähden on, etteivät kryptovaluutat ole valtion, muun viranomaisentahon tai edes niiden kehittäjien hallinnassa, mikä tekee niiden käytön seuraamisesta ja kontrolloinnista lähes mahdotonta (Extance, 2015). Kryptovaluuttoja ei siis omista kukaan ja samanaikaisesti ne omistavat kaikki, jotka ovat päättäneet sijoittaa niihin. Kryptovaluuttoja koskeva säännöstelyn puute onkin syynä kryptovaluuttojen poikkeuksellisen suurelle volatilisuudelle, mikä on saanut monet sijoittamaan niihin rikastumisen toivossa. Yksittäisen kryptovaluutan hinta voi markkinoilla ilmenneen uuden tiedon, kuten esimerkiksi suuren osto- tai myynti toimeksiannon seurauksena moninkertaistua tai muuttua arvottomaksi.

Kryptovaluuttojen arvoa voi olla hankala määrittää, sillä niiden fundamentaalinen eli reaaliarvo on nolla. (Cheah & Fry, 2015; Corbet ym., 2018) Tämä tarkoittaa, ettei niiden arvoa ole sidottu mihinkään konkreettiseen kuten velkaan tai arvometalliin, eivätkä ne myöskään tuota osinkoja osakesijoittamisen tavoin. Kryptovaluuttojen hinta kuitenkin määräytyy niiden tunnettavuuden ja omistajien määrän mukaan eli toisin sanoen kysynnän ja tarjonnan mukaan. Täysin vapaasti vaihteleva hinta tekee kohteesta erittäin riskipitoisen sijoituskohteen, sillä valuutan ostovoimaa ei ole millään tavalla taattu. Lisäksi kaikenlaisten valuuttamuotojen arvo perustuu niukkuuteen eli rajattuun saatavuuteen. Kryptovaluuttojen tapauksessa tämäkin on toteutettu teknisesti, mikä tarkoittaa, että valuuttaa tulee kiertoon vain tietty määrä tarkastellulla aikavälillä, eikä määrää kyetä edes tarvittaessa säätelemään.

Kryptovaluuttoihin kuten bitcoiniin liittyvässä keskustelussa tulee usein esiin anonymiteetti ja rikollisuus, mistä asiantuntijoilla on tutkimusaineistosta riippuen eriäviä näkemyksiä. Erimielisyydet johtuvat siitä, että kryptovaluutoilla kuten bitcoinilla toteutetuista transaktiosta jää aina jälki lohkoketjuun, jota käsittelen seuraavassa alaluvussa, jolloin transaktiota ei voida piilottaa tai poistaa. (McCallum, 2015.) Toisaalta transaktioiden suorittamiseen käytetään nimimerkkejä ja kryptovaluuttalompakoita, joiden liittäminen yritykseen tai yksityishenkilöön voi olla haastavaa, sillä lompakon luominen ei vaadi henkilöllisyyden todentamista (Bohme ym., 2015). Tilanteessa, joissa rahoja on siirretty maiden

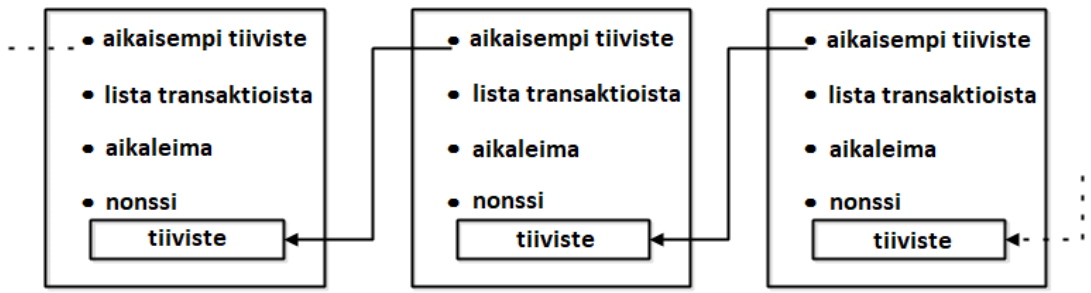
välillä lompakosta toiseen useaan kertaan, ei esimerkiksi Suomen poliisilla ole riittävästi resursseja transaktion osapuolten henkilöllisyyksien selvittämiselle (Johansson, 2021).

2.2 Lohkoketjuteknologia

Kryptovaluutalla toteutettujen transaktioiden toteutuessa ilman pankkeja tai muita kolmansia osapuolia, täytyi tilalle kehittää järjestelmä, joka takaisi tietojen virheettömyyden ja oikeellisuuden. Syntyi uusi teknologia, joka tunnetaan nimellä lohkoketju (engl. blockchain). On huomion arvoista mainita, etteivät lohkoketjuteknologian mahdollisuudet suinkaan rajoitu kryptovaluuttoihin, mutta ne ovat tällä hetkellä teknologian merkittävin käyttötarkoitus. Tulevaisuudessa teknologiaa voitaisiin hyödyntää esimerkiksi joukkorahoitukseen ja älysopimuksiin (engl. Decentralized Finance).

Lohkoketjuteknologia Li ym., (2018) mukaan tarkoittaa hajautettua julkista tietokantaa, jossa tieto kaikista transaktioista on järjestyksellisesti varastoitu lohkoihin, ja julkisesti saatavilla. Tämä määritelmä osoittautui kuitenkin melko suppeaksi uudemmassa (Low & Mik, 2020) tutkimuksessa, jossa todettiin lohkoketjujen jakautuvan julkisiin- ja esimerkiksi yritysten hyödyntämiin yksityisiin lohkoketjuihin, mikä tarkoittaa, etteivät kaikki lohkoketjut ole Bitcoinin tavoin julkisesti saatavilla. Sen sijaan tutkielmassa määriteltiin lohkoketjun olevan tietokantalajike, jossa tietokannan hallinnasta vastaavat maantieteellisesti hajautetut ja toisiinsa nähden tasavertaiset tietokoneet (Low & Mik, 2020).

Lohkoketju edustaa täydellistä muuttumatonta digitaalista tilikirjaa (engl. digital ledger), joissa tieto transaktioista ja omistajuuksista on kronologisesti kirjattu lohkoihin. Jokainen uusi transaktioista koostuva lohko liitetään viimeisimpänä validiksi todettuun lohkoon vahvasti yksilöivällä, sormenjälkeen verrattavissa olevalla tiivistellä (engl. hash) (Vranken, 2017). Tiiviste on ainutkertainen ja muuttuu, mikäli lohkon tietoja muutetaan. Tiiviste yhdessä aikaleiman ja satunnaisesti luodun tarkistusluvun nimeltä nonssin (engl. nonce) kanssa mahdollistaa lohkoketjun eheyden tarkastamisen aina ensimmäiseen lohkoon (engl. genesis block) asti. Alle oleva kuva (Kuvio 1) havainnollistaa lohkoketjun lohkojen sisältämiä tietoja ja niiden välistä liitosta.



KUVIO 1 Hiding Bitcoins in Steganographic Fractals. (Hosam, 2018)

Merkittävä peruste lohkoketjuteknologian hyödyntämiselle kriittisissä järjestelmissä on se, että se kykenee tarjoamaan suuren määrän dataa samanaikaisesti suurelle määrälle ihmisiä, kuitenkin ilman, että yksittäinen käyttäjä kykenee väärentämään tietoja (Low & Mik, 2020). Tämä johtuu siitä, että jokaisella verkon solmulla on kopio koko lohkoketjusta, jolloin yksittäinen väärennetty kopio ei kykene syrjäyttämään alkuperäistä (Vranken, 2017).

Lohkoketjuteknologian, kuten kaikkien uusien teknologioiden ympärillä on jo vuosikymmenen ajan merkittävää trendin omaista ”hehkutusta”. Aihe on todella mediaseksikäs ja sen mahdollisuuksista uutisoidaan jatkuvasti. Lohkoketjuteknologia ei kaikista hyvistä puolista huolimatta ole virheetön. Teknologian hyödyt ovat selkeästi nähtävissä, mutta teknologian heikkoudet konkretisoituvat vasta käyttäjämäärien kasvaessa moninkertaiseksi. Joka tapauksessa, lohkoketjuteknologia on osoittautunut erinomaiseksi työkaluksi datan tarjoamiseen suurelle määrälle ihmisiä vaarantamatta tietokannan turvallisuutta, mistä johtuen Tomić ym (2020) uskovat lohkoketjuteknologian olevan osa tulevaisuuden maksujärjestelmiä.

2.3 Louhiminen

Lohkoketjuteknologiaan ja sen turvallisuuteen liittyy olennaisesti käsite louhiminen (engl. mining). Uuden lohkon syntyessä sitä ei suoraan lisätä lohkoketjun jatkeeksi, vaan sen sisältö täytyy ensin todentaa validiksi. Validoinnin tarkoituksena on estää väärennettyä dataa sisältämien lohkojen lisäys lohkoketjuun, mistä vastaavat louhijat (engl. miner). Louhijat ovat verkossa toimivia käyttäjän laitteita, joka käyttävät tietokoneen komponenttien, kuten prosessorin, näytönohjaimen tai jopa kovalevyn laskentatehoa lohkojen sisältämien transaktioiden varmentamiseen palkkiota vastaan (Extance, 2015). Vaikka louhimiseen voidaan käyttää muitakin komponentteja, ovat näytönohjaimet osoittautuneet energiatehokkaimmaksi vaihtoehdoksi.

Ensimmäisten lohkojen louhimiseen käytettiin lähes jokaiselta löytyvää perinteistä pöytätietokonetta, mutta kilpailun kiihtyessä, alettiin louhimiseen käyttää siihen tarkoitettua laitteistoa. (Vranken, 2017) Louhimiseen tarkoitettu laitteisto (engl. mining rig) sisältää parannellun komponenttien viilennyksen sekä yhden tai useamman markkinoiden tehokkaimmista näytönohjaimista. Laitteisto liitetään kryptovaluuttaverkkoon lohkoketjusovelluksella, jonka jälkeen se jätetään työskentelemään ilman käyttäjän toimia. Vuonna 2017 louhiminen yleistyi niin merkittävästi, että näytönohjainten hinnat nousivat kahden kuukauden aikana jopa 80 euroa lisääntyneen kysynnän vuoksi (Laine, 2017). Lisäksi energiatehokkaiden näytönohjainten hankkiminen oli tuohon aikaan lähes mahdotonta. Nykyään hintataso ja saatavuus ovat kuitenkin palannut normaalille tasolle.

Louhimisprosessiksi kutsuttu transaktioiden varmentaminen koostuu datan salauksen purkamisesta ratkaisemalla matemaattisia pulmia (Extance, 2015). Transaktion tapahtuessa, ensimmäinen salauksen purkanut louhija julkaisee ratkaisun matemaattiseen pulmaan ja todentaa transaktion validiksi. Ratkaisu

julkaistaan muille solmuille tarkasteltavaksi, mikäli solmut ovat yksimielisiä ratkaisun oikeellisuudesta, lisätään lohko lohkoketjun jatkeeksi ja ensimmäinen salauksen purkanut louhija saa palkaksi kryptovaluuttaa (Extance, 2015). Tätä prosessia kokonaisuudessaan kutsutaan louhimiseksi, ja sitä kritisoidaan erityisesti siihen liittyvästä suuresta energiankulutuksesta. Nature lehden (2018) tutkimusartikkelin mukaan kryptovaluuttojen tuotanto loi saman määrän hiilidioksidipäästöjä kuin miljoona autoa tarkastellulla aikavälillä. Louhimisen yleistyminen aiheuttaisi siis merkittävän uhkan ympäristölle, jota tarkastellaan myöhemmin luvussa 3.3.

2.4 Konsensusmekanismit

Konsensusmekanismin tehtävä on varmistaa, että solmut toimivat protokollan mukaisesti sekä ovat yksimielisiä lohkoketjun rakenteesta. Ne pyrkivät estämään denial of service (DoS) hyökkäykset, rahojen kaksinkertaisen kulutuksen sekä muunlaiset väärinkäytökset (Vranken, 2017: Khalilov ym., 2018.) Käytetyimpiä konsensusmekanismeja ovat proof-of-work (PoW) sekä myöhemmin kehitetty proof-of-stake (PoS). Tutkielmassa viitataan edellä mainittuihin teknologioihin englanninkielisillä nimillä, sillä niille ei ole olemassa asianmukaista suomennosta.

Yleisimmin käytössä oleva Proof-of-work mekanismi nimensä mukaisesti vaatii todistuksen tehdystä työstä. Työ voidaan todentaa, kun siihen on käytetty resursseja kuten prosessointiaikaa (Khalilov, ym 2018). Resursseja käytetään lohkon tiivisteen yhteydessä satunnaisesti luodun tarkistusluku nonssin (engl. nonce) löytämiseksi. Nonssi voi olla mikä vain luku 0 ja $2^{256} - 1$ väliltä, minkä löytämiseen kuluu yleensä aikaa noin 10 minuuttia (Vranken, 2017). Louhijat kisaavat tämän proof-of-work:in eli ratkaisun löytämisestä kokeilemalla lukuja satunnaisesti (Extance, 2015). Ratkaisun löytyessä, lisätään uusi lohko lohkoketjuun ja louhija julkaisee päivitetyn version lohkoketjusta muille solmuille (Khalilov ym., 2018). Satunnaisten lukujen kokeileminen ei ole kovinkaan nopeaa, eikä varsinkaan energiatehokasta. Tutkimuksessa huomattiin, että merkittävimmän Proof-of-work:iä hyödyntävän lohkoketju Bitcoinin energiankulutus on noin. 45,8 TWh vuodessa, mikä verrattavissa kokonaisten valtioiden, kuten Itävallan ja Irlannin energiankulutukseen (Saleh, 2020).

Modernimpi vaihtoehto toteuttaa konsensusta on nimeltään proof-of-stake, joka on kehitetty ratkaisuna proof-of-work:in liialliselle energiankulutukselle. Puhtaan laskentatehon käyttämisen sijasta tässä mallissa valitaan lohkoketjuun lisäävä solmu satunnaisesti solmujen joukosta, joilla on hallussaan riittävän suuri määrä kyseisen lohkoketjun valuuttaa. (Saleh, 2020). Tämä kannustaa solmuja toimimaan protokollan mukaisesti, sillä väärinkäytöksistä saatava hyöty jäisi hyvin marginaaliseksi. Tämän lisäksi kryptovaluutan arvo laskee toistuvista lohkoketjun rakenteeseen liittyvistä erimielisyyksistä solmujen välillä, mikä vähentäisi myös väärinkäyttäjän oman osuuden arvoa. (Saleh, 2020)

Proof-of-stake ei kokonaan poista energiankulutuksen ja hiilidioksidipäästöjen ongelmaa, mutta sen avulla haittavaikutukset saataisiin kuitenkin kohtuullisemmaksi. Tästä johtuen toiseksi merkittävin kryptovaluutta ethereum onkin siirtymässä käyttämään uudempaa konsensusmekanismia, minkä on arvioitu kasvattavan valuutan arvoa ja merkityksellisyyttä. Proof-of-stake mekanismi on kuitenkin suhteellisen uutta teknologiaa, jonka tehokkuudesta, turvallisuudesta ja skaalautuvuudesta ei ole vielä pitkän aikavälin näyttöä.

2.5 Kryptovaluuttojen historia ja nykytilanne

Ensimmäinen kryptovaluutta ja samalla ensimmäinen lohkoketju bitcoin syntyi vuonna 2009, mikä käynnisti lohkoketjuteknologian kehityksen (Johansson, 2021). Bitcoin sai alkunsa tähän päivään asti anonyyminä pysyneen henkilön tai ryhmän nimeltä Satoshi Nakamoton vuonna 2008 julkaisemasta artikkelista ”Bitcoin: A Peer-To-Peer Electronic Cash System”. Artikkelissa esitetään, kuinka valuutta toimisi täysin teknologiapohjaisesti hyödyntäen lohkoketjuteknologiaa, mikä tarjoaisi taloudellista turvaa inflaatiokriiseissä. Kryptovaluuttojen suurena etuna nähtiin myös kustannusten pieneneminen etenkin maiden välisessä kaupankäynnissä, sillä transaktioiden suorittamiseen ei tarvita välikäsiä, kuten pankkeja (Härdle ym., 2020). Välikäden poistaminen tarjoaisi myös kehitysmaissa asuville pankittomille mahdollisuuden moderniin kaupankäyntiin.

Uuden kryptovaluutan kiinnostavuutta ja kasvua kiihdytti vuosien 2007–2009 aikana vallitseva maailmanlaajuinen finanssikriisi, jolloin luottamus perinteiseen pankkijärjestelmään oli vaakalaudalla (Senner, & Sornette, 2019). Vain vuosi myöhemmin vuonna 2009 käynnistyi avoin Bitcoin-verkko, johon kuka tahansa pystyy liittämään oman laitteensa ja tulla osaksi konsensuksen toteutusta. Valuutan merkityksellisyys ei kuitenkaan syntynyt hetkessä ja ensimmäisinä vuosina bitcoinin hinta sekä omistajien määrä olivat todella alhaiset. Tästä kertoo muun muassa se, että ensimmäinen bitcoinilla ostettu hyödyke oli kaksi kappaletta pizzoja toukokuussa 2010 hintaan 10 000 BTC (Extance, 2015). Kaupanteossa käytettyjen bitcoinien arvo olisi tänä päivänä noin. 191 750 000 euroa (Coindesk, 2022).

Uusia bitcoinin kaltaisia altcoineiksi kutsuttavia kryptovaluuttoja syntyy ja poistuu markkinoilta jatkuvasti, mutta bitcoin on säilyttänyt asemansa merkittävimpänä kryptovaluuttana. Merkittävästä asemasta ja tunnettavuudesta huolimatta ei bitcoinia tai muitakaan kryptovaluuttoja käytetä päivittäistavaroiden hankkimiseen, eikä suurin osa valtioista tunnista niitä virallisiksi maksuvälineiksi. Pääosin bitcoiniin ja muihin kryptovaluuttoihin sijoitetaan taloudellisen hyödyn toivossa ja valuutat on tarkoitus myöhemmin vaihtaa takaisin Fiat-valuutaksi paremmalla kurssilla.

Kryptovaluutat nähdään sijoituskohteen lisäksi eräänlaisena anonyyminä valuuttana, sillä kauppaa ei käydä henkilöiden oikeilla nimillä, vaan pseudonyymeillä eli nimimerkeillä ja kryptovaluuttalompakoilla (Khalilov, & Levi, 2018). Tämä houkuttelee rikollisia, sillä vaikka jokaisen transaktion tiedot tallentuvat

julkisesti saatavilla olevaan lohkoketjuun, voi oikein toteutettuna osapuolten henkilöllisyys olla lähes mahdoton selvittää (Johansson, 2021). Tästä syystä kryptovaluuttoja käytetään lähes poikkeuksetta maksuvälineenä dark webissä, jossa käydään kauppaa muun muassa laittomista hyödykkeistä ja palveluista.

Saiedin ym. (2021) mukaan vuonna 2019 tehdyssä tutkimuksessa huomattiin, että 25 % bitcoinilla tehdyistä, ja 44 % muilla kryptovaluutoilla tehdyistä transaktioista liittyy rikolliseen toimintaan, kuten rahanpesuun tai huumekauppaan. Kryptovaluuttojen käyttö ei läheskään aina liity rikolliseen toimintaan, mutta osa asiantuntijoista pelkää kryptovaluuttojen ajan myötä muuttuvan rikolliseksi rahaksi (Badea & Mungiu-Pupazan, 2021). Kryptovaluuttasijoittamiseen liittyy myös huijauksia, joiden uhriksi on joutunut myös suomalaisia. Huijaukset perustuvat siihen, että asiaan perehtymättömille luvataan salkunhoitoa, mutta tosiasiassa sijoitetut rahat päätyvät ulkomaille huijareiden tileille (Johansson, 2021). Kryptovaluuttoihin liittyvästä kyberrikollisuudesta keskustellaan tarkemmin luvussa 3.4.

3 FIAT-RAHASTA BITCOINIIN SIIRTYMINEN

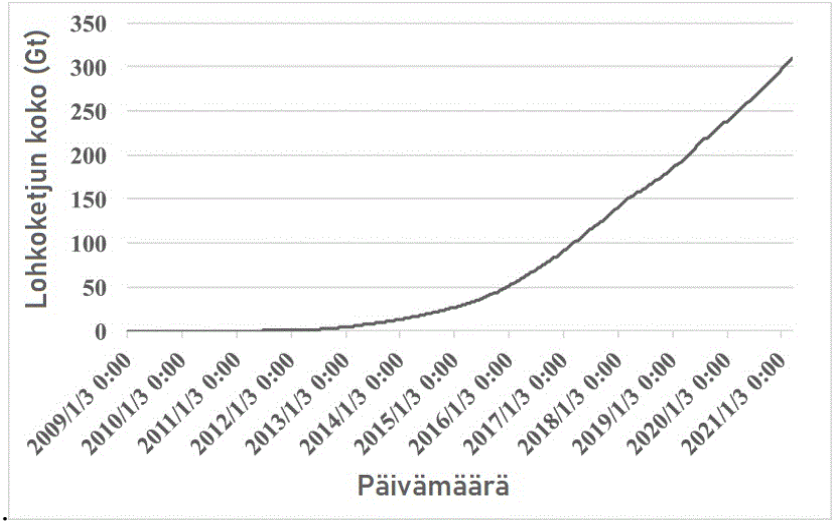
Kryptovaluutat ovat suuri teknologinen edistysaskel kohti tulevaisuuden rahataloutta ja Bitcoinlohkoa onkin kuvailtu, jopa kaksituhattaluvun merkittävimmäksi keksinnöksi (Extance, 2015; Badea & Mungiu-Pupazan, 2021). Kaikille avoin ja tasa-arvoinen kaupankäynti, matalat kustannukset sekä tietojen muuttumattomuus puhuvat kryptovaluuttojen käytön puolesta, mutta kolikolla on aina kaksi puolta. Tutkielman lähdekirjallisuuksia yhdisti kaikkia sama lopputulos, jossa bitcoin ei ole nykyisessä muodossaan valmis korvaamaan käytössä olevia valuuttoja, sillä se ei täytä valuutan määritelmälle välttämättömiä kriteerejä. Valuutan määritelmän ongelmallisuuden ja sitä seuraavien rahatalouden haasteiden lisäksi, lähdekirjallisuudesta havaitut merkittävimmät haasteet liittyivät skaalautuvuuteen, ympäristöhaittoihin ja rikollisuuteen, joiden suuremman mittakaavan vaikutuksia käsitellään tässä luvussa.

3.1 Skaalautuvuuden ongelmat

Skaalautuvuuden ongelmat ovat yksi keskeisimmistä haasteista lohkoketjuteknologian hyödyntämiselle reaalimaailman liiketoimintaympäristöissä (Xie ym., 2019). Ongelmat ilmenevät verkon solmujen ja transaktioiden määrän lisääntyessä, sillä solmujen täytyy varastoida ja validoida erikseen jokainen transaktio (Khan ym., 2021). Tällä hetkellä bitcoinia rajoittavina tekijöinä nähdään transaktioiden suoritusteho, tallennustilavaatimukset sekä tiedonsiirtonopeus (Xie ym., 2019). Eniten keskustelua herättänyt skaalautuvuuden ongelma on transaktioiden suoritusteho, jonka heikkous liittyy suoraan käytössä olevaan konsensusmekanismiin. Yleisimmin kryptovaluuttojen hyödyntämälle ja bitcoinilla käytössä olevalle proof-of-work konsensusmekanismille on tyypillistä, että louhijoilla on aika ajoin erimielisyyksiä lohkoketjun rakenteesta. (Hinzen ym., 2022) Erimielisyydet täytyy ratkaista ja solmujen tulee olla yksimielisiä, jotta transaktio voidaan kirjata suoritetuksi ja lisätä lohkoketjuun.

Solmujen määrän lisääntyessä myös erimielisyyksien määrät kasvavat, mikä pidentää yksimielisyyden saavuttamiseen vaadittua aikaa. Tämä johtaa korkeaan latenssiin eli transaktioiden suorittamiseen vaadittuun aikaan. Bitcoinilla toteutettujen transaktioiden latenssi on jo tällä hetkellä merkittävästi nykyisiä luottoyhtiötä korkeampi. (Khan ym., 2021) Esimerkiksi Visa kykenee prosessoimaan 400 transaktiota joka sekunti, kun taas Bitcoinin transaktioiden prosessointi on rajoitettu seitsemään transaktioon sekunnissa. Transaktioiden prosessoinnin määrä on rajoitettu, sillä pienempi latenssi vähentäisi turvallisuutta ja lisäisi Forkin muodostumisen, eli lohkoketjun kahtiajakautumisen riskiä. (Khan ym., 2021) Lisääntynyt transaktioiden määrä vaatisi myös solmuilta kohtuuttoman suuren tiedonsiirtonopeuden korkean latenssin ehkäisemiseksi (Xie ym., 2019). Tämän seurauksena Khan ym., (2021) uskovat, etteivät tällä hetkellä käytössä olevat konsensusmekanismit kykene tarjoamaan riittävää transaktioiden suoritustehoa kriittisten toimialojen käyttötarkoituksiin.

Korkean latenssin tuomien haittojen lisäksi, lohkoketjujen pidentyessä jatkuvasti, kasvavat myös niiden solmuille asettamat tallennustilavaatimukset. Lohkoketjun turvallisuuden kannalta on välttämätöntä, että suurella osalla solmuista on täydellinen kopio koko lohkoketjusta. Lohkoketjun lohkojen jatkuva lisääntyminen kasvattaa tallennustilavaatimuksia, mikä puolestaan johtaa siihen, ettei solmujen ole kannattavaa tai edes mahdollista säilyttää kokonaista kopiota laitteillansa. Tätä seuraa verkossa olevien solmujen määrän vähentyminen ja lohkoketjun turvallisuuden heikentyminen. (Wang ym., 2022) Solmujen määrän vähentyminen muuttaisi järjestelmän keskittyneemmäksi, mikä on ristiriidassa teknologian ydinhyötyjen kanssa. Alla oleva graafi esittää Bitcoin lohkoketjun kumulatiivisten tallennustilavaatimusten kasvua vuodesta 2009 vuoteen 2021 asti.



KUVIO 2 ESS: An Efficient Storage Scheme for Improving the Scalability of Bitcoin Network (Wang ym., 2022)

3.2 Talouden haasteet

Jotta hyödykettä voidaan pitää valuuttana, tulee sen täyttää valuutan määritelmälle asetetut ehdot. Valuutan tulee toimia vaihdonvälineenä, laskentayksikönä sekä arvonsäilyttäjänä (Tomic, 2020). Näiden lisäksi tulee valuutan kurssin olla riittävän stabiili sekä käyttäjämäärän riittävän suuri (Selimović ym, 2021). Bitcoin kykenee toimimaan hyvin vaihdonvälineenä, mutta se ei ole paras mahdollinen laskentayksikkö eikä myöskään arvonsäilyttäjä suuren volatilisuutensa vuoksi. Kuvitellaan, että bitcoinin käyttäjämäärä saataisiin riittävän suureksi, ja tarkastellaan, millaisia ongelmia tai haasteita bitcoinin ominaisuudet aiheuttaisivat taloudelle ja yhteiskunnalle.

Kryptovaluutta bitcoinin mahdollisesti merkittävin taloudellinen haaste on kiinteä tarjonta (engl. fixed supply). Kiinteällä tarjonnalla tarkoitetaan, että jokaisesta louhitusta lohkosta saa saman määrän valuuttaa palkaksi tarkastellulla aikavälillä, eikä kierrossa olevan valuutan määrää kyetä säätelemään. Tämä on ristiriidassa rahan määräteorian kanssa, jonka mukaan ”Talouden rahan tarjonnan ja myytyjen tuotteiden hintatason välillä on suora yhteys.” (Greenlane, 2019.) Esimerkiksi, jos elintarvikkeiden valmistuskustannukset nousevat, täytyy elintarvikkeiden hankintahinta nousta myös kuluttajille. Tämä ei ole mahdollista, jos kierrossa olevan valuutan määrää ei kyetä säätelemään. Ongelma konkretisoituu erityisesti rahoitusmarkkinoilla, koska markkinoilla ei ole tarpeeksi valuuttaa yritysten reaali-investointien rahoittamiseen eikä taloudellisen kasvun edistämiseen. Tutkijoista Gronwald (2019) onkin sitä mieltä, että bitcoin muistuttaa valuutan sijasta enemmän uusiutuvia luonnonvaroja.

Kiinteän tarjonnan lisäksi bitcoiniin ei kohdistu tällä hetkellä juuri minkäänlaista lainsäädäntöä. (Badea & Mungiu-Pupazan, 2021) Tutkimuksessa todetaan, että bitcoinia ja muita kryptovaluuttoja koskevan lainsäädännön laatiminen voisi vähentää niille ominaista suurta volatilisuutta sekä niihin kohdistuvaa epävarmuutta. Toisaalta osa tutkijoista uskoo, että lainsäädännönlaatiminen voisi tahattomasti luoda turvallisuudentunnetta ja eräällä tavalla kannustaa kryptovaluuttoihin sijoittamiseen. Kryptovaluuttojen välittömästi reagoidessa uuteen tietoon markkinaehtoisen järjestelmän tavoin, ei kryptovaluuttasijoittamiseen haluta kannustaa ihmisiä, etenkin kun valuutan ostovoimaa ei ole millään tavalla taattu. Esimerkiksi vuoden 2022 tammikuussa bitcoiniin sijoittanut olisi marraskuussa menettänyt 62 % sijoituksensa arvosta, mikä indikoi valuutan olevan tällä hetkellä aivan liian volatiili käytettäväksi globaalina maksuvälineenä (Google Finance, 2022). Lisäksi suurin osa valtioista ei tällä hetkellä tunnusta bitcoinia maksuvälineeksi tai ulkomaan valuutaksi, mikä vaikeuttaa välttämättömien verotulojen saantia.

Bitcoinilla toteutetut transaktiot ovat peruuttamattomia, mikä nähdään usein kryptovaluuttojen etuna, mutta voidaan nähdä myös heikkoutena ongelmatilanteissa. (Böhme ym., 2015) Perinteiset luottoyhtiöt kykenevät riitatilanteissa peruuttamaan esimerkiksi vahinko-ostot tai tilanteet, jossa maksoit hyödykkeestä, jota et ikinä saanutkaan. Tämänkaltaisissa tilanteissa on transaktion

peruuttaminen kryptovaluutoilla mahdotonta, mikä osaltaan mahdollistaa huijauksia ja rikollisuutta, joita käsitellään myöhemmin alaluvussa 3.4.

3.3 Ympäristöriskit

Edellä mainittujen ongelmien ja haasteiden lisäksi, myös kryptovaluuttojen ympäristövaikutukset ovat ajankohtainen ja merkittävä huolenaihe. Kryptovaluuttojen louhimisprosessiin vaadittavan energiamäärän oletetaan kasvavan tulevaisuudessa, mikä on saanut tutkijoiden lisäksi myös Euroopan komission tarkkailemaan tilannetta. (Badea & Mungiu-Pupazan, 2021.) Energiankulutuksen näkökulman merkitystä korostaa myös talveksi 2022 Eurooppaan ennustettu energiakriisi.

Kryptovaluuttojen louhimisella on huomattu olevan vaikutuksia myös ilmaston lämpenemiseen. Badean ja Mungiu-Pupazanin (2021) artikkelissa yksi tutkijoista uskoo kryptovaluuttojen louhimisen aiheuttavan kahden celsius asteen lämpenemisen maapallolla seuraavan 11–22 vuoden aikana. Eräs toinen artikkelin tutkijoista ei pidä tällaista kuitenkaan täysin mahdollisena, mutta ei kuitenkaan kiistä valtavan energiankulutuksen määrän negatiivista vaikutusta ympäristöön. Louhimiseen käytettävän energiankulutuksen määrän vastatessa jo tällä hetkellä kokonaisten valtioiden energiankulutusta, täytyisi bitcoinin tuotantoprosessin rakennetta muuttaa merkittävästi ekologisemmaksi, mittavien ympäristöhaittojen ehkäisemiseksi.

Mielenkiintoista on myös tarkastella, kuinka edellisessä kappaleessa keskusteltu lainsäädännön puute kannustaa kryptovaluuttojen louhimiseen maissa, joissa sähkönhinta on alhainen. (Badea & Mungiu-Pupazan, 2021.) Noin 58 % kaikesta bitcoinin louhimisesta tapahtuu jo valmiiksi ilmansaasteista kärsivässä Kiinassa, koska sähkön hinta on siellä alhainen. Bitcoinin muuttuessa valtavirtavaluutaksi, korostuisi valtioiden välisten energian hintaerojen merkitys entisestään, josta kehittyneemmät uusiutuvaa energiaa hyödyntävät valtiot kuten Suomi kärsisivät eniten. Tämä voisi pahimmassa tapauksessa kannustaa valtiota edullisempiin ympäristölle haitallisempiin energiamuotoihin.

Louhimisesta keskusteltaessa nousee usein esiin ajatus, että louhimiseen käytettäessä vain esimerkiksi tuuli- tai vesienergiaa, saataisiin hiilidioksidipäästöjen vaikutukset minimoitua. Tämä on todettu teoriassa mahdolliseksi, mutta louhijoille on tyypillistä altruistinen ajatusmalli, joka tarkoittaa sitä, että louhimisesta halutaan saada mahdollisimman suuri taloudellinen hyöty, vaikka se tarkoittaisi fossiilisten energiamuotojen käyttöä louhimiseen. (Badea & Mungiu-Pupazan, 2021.) Kuten aikaisemmin todettiin, louhiminen on kaikista kannattavinta, silloin kun käytetyn energian hinta on mahdollisimman alhainen, jolloin uusiutuvien energiamuotojen käyttö fossiilisten sijaan ei olisi louhijoiden näkökulmasta kannattavaa.

Skaalautuvuuden ongelmien tavoin, bitcoinin ympäristöriskien taustalla on käytössä oleva konsensusmekanismi proof-of-work. Proof-of-workin matala energiatehokkuus ja suuret hiilidioksidipäästöt johtavat siihen, ettei Bitcoinia

nykyisessä muodossaan Badean ja Mungiu-Pupazan (2021) mukaan voida käyttää globaalina maksuvälineenä. Lähdekirjallisuudesta käy kuitenkin ilmi, että tulevaisuudessa lohkoketjuteknologiaan perustuvat valuutat voisivat teoriassa toimia maan- tai maailmanlaajuisena maksuvälineenä, mikäli louhimisprosessi ja siihen käytettävät komponentit toimisivat energiatehokkaammin.

3.4 Kyberrikollisuus

Kryptovaluuttojen hankkimisesta ovat suurimmilta osin kiinnostunut kaksi ryhmää, jotka ovat pääomasijoittajat ja rikolliset (Lapuh-Bele, 2021.) Miksi bitcoinia ja muita kryptovaluuttoja hyödynnetään maksuvälineenä rikollisessa toiminnassa? Ongelman taustalla on sekä kryptovaluutoille tyypilliset ominaisuudet, että puutteellinen lainsäädäntö. Tässä alaluvussa viitataan kyberrikollisuuteen käsitteenä, joka käsittää kaiken verkossa tapahtuvan rikollisen toiminnan.

Kryptovaluuttoja hyödynnetään kyberrikollisuuteen pääosin kolmella tavalla. Lohkoketjuun hyökkäämällä, laittomien hyödykkeiden tai palveluiden maksamiseen sekä muuhun rikolliseen toimintaan, kuten rahanpesuun ja kiristykseen. (Lapuh-Bele, 2021) Hyvä esimerkki kiristyksestä on WannaCry 2.0 kiristyshaittaohjelma, joka salasi kaikki käyttäjän laitteen tiedostot. Uhrilla oli viikko aikaa maksaa 300–600 Yhdysvaltain dollarin arvoinen maksu bitcoineina tiedostojen palauttamiseksi. Myös erilaiset Ponzi-huijaukset eli sijoittamiseen liittyvät pyramidihuijaukset, ovat yleistyneet viime vuosien aikana.

Esimerkkejä lohkoketjuun kohdistuvista hyökkäyksistä ovat varojen kaksinkertainen kulutus (engl. double spending) ja 51 % hyökkäys. Varojen kaksinkertaisessa kulutuksessa hyödynnetään lohkoketjun rakenteen muuttumattomuutta siten, että samat rahat käytetään kahteen eri transaktioon. (Kus & Levi, 2018.) Tilanteessa, jossa varojen kaksinkertainen kulutus onnistuu, käyttäjä saa itselleen ostamansa hyödykkeen sekä hyödykkeen ostamiseen käytetyt varat. Tämä perustuu siihen, että verkon solmut havaitsevat varojen olleen käytetty kahdesti ja näin olleen peruuttaa toisen transaktioista ennen lohkoketjuun lisäämistä.

51 % hyökkäyksessä puolestaan louhija, joka hallitsee yli puolet louhittavan valuutan louhimistehosta (engl. hash rate) kykenee muokkaamaan lohkoketjua oman etunsa mukaisesti. Jos verkossa olevien solmujen määrää pystyttäisiin hetkellisesti laskemaan, voitaisiin 51 % louhimisteho saavuttaa pienelläkin määrällä solmuja. Tämän kaltaisia hyökkäyksiä oli tiedettävästi kohdistunut Bitcoin lohkoketjuun vuoteen 2015 mennessä jopa 40 kertaa, joista osassa oli saatu jopa yli miljoonan Yhdysvaltain dollarin hyöty (Extance, 2015).

Osa uudemmista kryptovaluutoista tarjoaa bitcoiniin verraten paremman anonymiteetin, mutta bitcoin on merkittävyytensä ansiosta edelleen dark webin käytetyin valuutta laittomien palveluiden ja hyödykkeiden ostoon (Lapuh-Bele, 2021). Dark web on internetin osa, jota ei voi saavuttaa perinteisellä verkkoselaimella, ja jossa verkon käyttäjät toimivat anonyymisti. Tämä TOR-verkkona tunnettu palvelu tarjoaa käyttäjille anonymiteetin, mikä mahdollistaa

silkkitien tapaisten sivustojen toiminnan. (Kethineni & Cao, 2020) (Silkkitie on verkkokauppa, jossa käydään kauppaa muun muassa huumeista, aseista tai väärennetyistä henkilöllisyystodistuksista). Dark webissä löytyy myös ohjeita, kuinka bitcoinia voi hyödyntää rahanpesuun. Bitcoinverkko tarjoaa hyvän alustan rahanpesemiselle, sillä se mahdollistaa rahansiirrot maasta toiseen huomaamattomasti. (Lapuh-Bele, 2021) Rahanpesu voi tapahtua hyödyntämällä esimerkiksi verkkokasinoita, verkkohuutokauppoja sekä joukkorahoituksia. (Kethineni & Cao, 2020) Ilmiöstä tekee mielenkiintoisen se, etteivät suurin osa valtioista tunnista bitcoinia valuutaksi, jolloin tekijää ei maan lainsäädännöstä riippuen voida tuomita rahanpesusta. Tällaisia tapauksia on käsitelty oikeudessa ainakin Yhdysvaltain Kaliforniassa vuosina 2014–2017.

Bitcoinia ja muita kryptovaluuttoja hyödynnetään siis rikolliseen toimintaan käteistä rahaa muistuttavien ominaisuuksien vuoksi. Rahat kulkeutuvat helposti maiden välillä, osapuolten pysyessä suurimmilta osin anonyymeinä. Myös puutteellinen lainsäädäntö ja ilmiön uutuudesta johtuva ihmisten tietämättömyys nähdään kryptovaluuttojen osalta kyberrikollisuuteen mahdollistavana tekijänä.

3.5 Haasteiden yhteenveto

Tässä luvussa käsiteltiin nykyisessä muodossa olevan bitcoinin keskeisimpiä haasteita Fiat-valuuttojen korvaajana. Haasteet ovat kuvattu edellä mainittujen näkökulmien mukaisesti tämän luvun lisäksi alla olevaan taulukkoon (taulukko 1). Tarkastelun kohteeksi valikoituivat lähdekirjallisuudessa eniten toistuneet ja vaikutuksiltaan merkittävimmät näkökulmat.

TAULUKKO 1 Bitcoinin riskit Fiat-valuuttojen korvaajana

Bitcoinin riskit Fiat-valuuttojen korvaajana	
Skaalautuvuus	Lisääntynyt verkon solmujen ja transaktioiden määrä hidastaisi jo valmiiksi hidasta transaktioiden suoritusta. Solmuille asetetut tallennustila- ja tiedonsiirtonopeuden vaatimukset kasvaisivat kohtuuttoman suuriksi.
Talous	Ei täytä valuutan määritelmälle asetettuja ehtoja. Suuri arvonvaihtelu, kiinteä tarjonta, puutteellinen lainsäädäntö nähdään hidastavina tekijöinä.
Ympäristö	Heikko energiatehokkuus, suuret hiilidioksidipäästöt, epäekologisten energiamuotojen käyttö. Maiden väliset erot energian hinnassa kannustavat epäekologisten energiamuotojen käyttöön kilpailuedun saavuttamiseksi.
Rikollisuus	Lohkoketjuun kohdistuvat hyökkäykset, anonymiteetin mahdollistama laittomilla tuotteilla ja palveluilla käyty kauppa, rahanpesu, veropetokset sekä sijoitushuijaukset.

4 YHTEENVETO

Tässä tutkielmassa tarkasteltiin bitcoinin ja yleisellä tasolla kryptovaluuttojen ja lohkoketjuteknologian ominaisuuksia. Tutkielman tarkoituksena oli akateemisen lähdekirjallisuuden pohjalta tunnistaa riskit ja haasteet, joita nykyisten käytössä olevien valuuttojen korvaaminen bitcoinilla toisi tullessaan. Johdannon jälkeisessä ensimmäisessä sisältöluvussa käsiteltiin bitcoinin ominaisuuksia, ansaintamallia, sekä lohkoketjuteknologiaa. Tässä luvusta todettiin bitcoinin toiminnan perustuvan täysin teknologisiin ratkaisuihin, mikä vaikuttaa muun muassa turvallisuuteen, valuuttakurssin volatilisuuteen sekä energiankulutukseen. Lohkoketjuteknologia tarjoaa monia etuja keskitettyihin järjestelmiin verrattuna, joista esimerkiksi järjestelmän hajautuksella saavutetaan parempi vikasietoisuus ja tietoturva. Lisäksi välikäden poistaminen kaupankäynnistä vähentää kustannuksia ja on askel kohti tasa-arvoista kaupankäyntiä. Kryptovaluuttojen ja erityisesti bitcoinin rajoittavista tekijöistä tunnistettiin louhintaprosessin heikko energiatehokkuus, anonymiteetti, puutteellinen lainsäädäntö, valuuttakurssin epästabiilisuus sekä fundamenttiarvon ja arvontakaajan puute.

Toisessa sisältöluvussa tarkasteltiin bitcoiniin ja yleisellä tasolla kryptovaluuttoihin liittyviä riskejä kolmesta näkökulmasta. Tarkasteluun valikoituivat skaalautuvuuden, ympäristön ja rahatalouden näkökulmat. Skaalautuvuuden saralla todettiin verkon käyttäjämäärien lisääntymisellä olevan negatiivinen vaikutus transaktioiden suorittamiseen vaadittuun aikaan sekä jatkuvasti kasvavien tallennustilavaatimusten negatiiviset vaikutukset teknologian turvallisuuteen. Ympäristöriskejä tarkastellessa huomattiin bitcoinin louhimisen seurauksena syntyvien hiilidioksidipäästöjen määrän olevan liian suuri, jotta valuuttaa voitaisiin nykyisessä muodossaan hyödyntää maailmanlaajuisena maksuvälineenä. Talouden näkökulman riskeistä tunnistettiin valuutan suuren volatilisuuden ja kiinteän tarjonnan tuomat haasteet sekä maiden välisten eriävien sähkönhintojen synnyttämä kilpailu. Rikollisuuteen mahdollistavina tekijöinä nähtiin puutteellinen lainsäädäntö, kryptovaluuttojen ominaisuudet, kuten vaikeasti jäljitettävissä olevat maiden väliset transaktiot sekä ihmisten tietämättömyys aiheesta.

Tutkimuksessa kuitenkin todettiin, että ottaen huomioon lohkoketjuteknologian maturiteetin on mahdollista, että jossain vaiheessa se voisi vaikuttaa

rahapolitiikkaan etenkin maissa, joiden valuutan kurssi ei ole stabiili. (Tomić, 2020). Mahdollisia jatkotutkimusaiheita tutkimuksessa todetun tiedon perusteella olisi eri konsensusmekanismin käytön vaikutukset. Suurin osa tutkielmassa käsitellyistä bitcoinin heikkouksista liittyvät tavalla tai toisella käytössä olevaan proof-of-work konsensusmekanismiin. Mielenkiintoista olisi tutkia, olisiko esimerkiksi proof-of-stake konsensusmekanismin käyttöön siirtyvä kryptovaluutta ethereum parempi vaihtoehto Fiat-rahan korvaajaksi, sillä aineiston kriittisen tarkastelun ja niiden yhdistelemän tiedon pohjalta on todettavissa, ettei bitcoin ole siihen nykyisessä muodossaan valmis.

Tutkimuksesta jätettiin pois kehitysmaita koskeva näkökulma, jossa kryptovaluuttojen käyttö olisi vaikeaa heikon infrastruktuurin vuoksi. Aiheesta löytyi suhteellisen vähän vertaisarvioitua tieteellistä tietoa, ja suurin osa saatavilla olevasta tutkimusaineistosta perustui kryptovaluutoista saataviin hyötyihin. Heikosti saatavilla olevan tiedon ja aihealueiden laajuuden seurauksena näkökulmien käsittely olisi voinut olla laajempaa.

LÄHTEET

Badea, L. & Mungiu-Pupazan, M. C. (2021). The Economic and Environmental Impact of Bitcoin. IEEE access, 9, 48091-48104. https://doi.org/10.1109/ACCESS.2021.3068636

Bohme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. The Journal of economic perspectives, 29(2), 213-238. https://doi.org/10.1257/jep.29.2.213

Cheah, E. & Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Economics letters, 130, 32-36. https://doi.org/10.1016/j.econlet.2015.02.029

Coindesk. (7.9.2022) Bitcoin. https://www.coindesk.com/price/bitcoin/

Corbet, S., Lucey, B., Peat, M., & Vigne, S. (2018). Bitcoin Futures—What use are they? Economics letters, 172, 23-27. https://doi.org/10.1016/j.econlet.2018.07.031

Extance, A. (2015). The future of cryptocurrencies: Bitcoin and beyond. Nature (London), 526(7571), 21-23. https://doi.org/10.1038/526021a

Franco, P. (2015). Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley

Google Finance, (2022) Bitcoin. https://www.google.com/finance/?sa=X&ved=2ahUKEwi7wvml0NP7AhUDl4sKHU3ZDA8Q6M8CegQIGRAG

Greenlane. (2019) Rahan määräteoria. https://www.greelane.com/fi/science-tech-matematiikka/yhteiskuntatieteet/the-quantity-theory-of-money-1147767

Gronwald, M. (2019). Is Bitcoin a Commodity? On price jumps, demand shocks, and certainty of supply. Journal of international money and finance, 97, 86-92. https://doi.org/10.1016/j.jimonfin.2019.06.006

Hinzen, F. J., John, K. & Saleh, F. (2022). Bitcoin's limited adoption problem. Journal of financial economics, 144(2), 347-369. https://doi.org/10.1016/j.jfineco.2022.01.003

Hosam, O. (2018). Hiding Bitcoins in Steganographic Fractals. 512–519. 10.1109/ISSPIT.2018.8642736

Härdle, W. K., Harvey, C. R. & Reule, R. C. G. (2020). Understanding Cryptocurrencies. *Journal of financial econometrics, 18*(2), 181-208. https://doi.org/10.1093/jjfinec/nbz033Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current opinion in environmental sustainability, 28, 1-9. https://doi.org/10.1016/j.cosust.2017.04.011

Johansson, P. [MOT]. (14.7.2022). Bitcoin-huijareiden jäljillä [video]. Yle Areena. https://areena.yle.fi/1-50654064/

Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International criminal justice review, 30(3), 325-344. https://doi.org/10.1177/1057567719827051

Khan, D., Jung, L. T. & Hashmani, M. A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. Applied sciences, 11(20), 9372. https://doi.org/10.3390/app11209372

Kus Khalilov, M. C. & Levi, A. (2018). A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. IEEE Communications surveys and tutorials, 20(3), 2543-2585. https://doi.org/10.1109/COMST.2018.2818623

Laine, P. (2017) Kryptovaluuttojen louhinta nostanut näytönohjainten kysynnän selvästi yli tarjonnan. https://www.io-tech.fi/uutinen/kryptovaluuttojen-louhinta-nostanut-naytonohjainten-kysynnan-selvasti-yli-tarjonnan/

Lapuh Bele, J. (2021). Cryptocurrencies as facilitators of cybercrime. SHS Web of Conferences, 111, 1005. https://doi.org/10.1051/shsconf/202111101005

Li, J., Li, N., Peng, J., Cui, H., Wu, Z. (2018) Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies, found at: https://www-sciencedirect-com.ezproxy.jyu.fi/science/article/pii/S0360544218322503

Lo, Y. & Medda, F. (2018) Bitcoin mining: converting computing power into cash flow, found at: https://www-tandfonline-com.ezproxy.jyu.fi/doi/full/10.1080/13504851.2018.1540841

McCallum, B. T. (2015). The Bitcoin revolution. The Cato journal, 35(2), 347-356.

Nature (2018). 'Mining' Bitcoin takes more energy than mining gold. Nature (London), 563(7731), 296. https://doi.org/10.1038/d41586-018-07283-3

Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. Internet policy review, 10(2), . https://doi.org/10.14763/2021.2.1561

Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. Internet policy review, 10(2), . https://doi.org/10.14763/2021.2.1561

Royal, J. & Baker, B. (2022) 12 most popular types of cryptocurrency. https://www.bankrate.com/investing/types-of-cryptocurrency/

Saiedi, E., Broström, A., Ruiz, F. (2021) Global drivers of cryptocurrency infrastructure adoption, found at: https://link-springer-com.ezproxy.jyu.fi/article/10.1007/s11187-019-00309-8

Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. The Review of financial studies, 34(3), 1156-1190. https://doi.org/10.1093/rfs/hhaa075

Schilling, L. & Uhlig, H. (2019). Some simple bitcoin economics. Journal of monetary economics, 106, 16-26. https://doi.org/10.1016/j.jmoneco.2019.07.002

Selimović, A., Kozarić, K., Žunić, A., & Dželihodžić, E. Ž. (2021). CRYPTOCURRENCY-ADVANTAGES, DISADVANTAGES, DETERMINANTS: CASE OF BITCOIN. *Sarajevo business and economics review, 39*, 123-144.

Senner, R. & Sornette, D. (2019). The Holy Grail of Crypto Currencies: Ready to Replace Fiat Money? Journal of economic issues, 53(4), 966-1000. https://doi.org/10.1080/00213624.2019.1664235

Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. Joule, 3(7), 1647-1661. https://doi.org/10.1016/j.joule.2019.05.012

Suomen Kultareservi. (14.5.2022) Mikä on fiat raha ja mihin valuutta perustuu? https://suomenkultareservi.fi/fiat-raha-ja-valuutat/

Tomić, N., Todorović, V., & Čakajac, B. (2020). The potential effects of cryptocurrencies on monetary policy. The European Journal of Applied Economics, 17(1), 37-48.

Wang, X., Wang, C., Zhou, K., & Cheng, H. (2022). ESS: An Efficient Storage Scheme for Improving the Scalability of Bitcoin Network. IEEE eTransactions on network and service management, 19(2), 1191-1202. https://doi.org/10.1109/TNSM.2021.3127187

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A Survey on the Scalability of Blockchain Systems. IEEE network, 33(5), 166-173. https://doi.org/10.1109/MNET.001.1800290