Atte Sarkonen

PELITEORIAN VAIKUTUS JULKISTEN LOHKOKETJUJEN TOIMINTAAN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Sarkonen, Atte
Peliteorian vaikutus julkisten lohkoketjujen toimintaan
Jyväskylä: Jyväskylän yliopisto, 2019, 30 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Luoma, Eetu; Palonen, Teija

Tämä tutkielma käsittelee peliteorian vaikutusta julkisten lohkoketjujen toimintaan, ja se on toteutettu kirjallisuuskatsauksena vertaisarvioidun tieteellisen aineiston ja kirjallisuuden avulla. Lohkoketjut ovat herättäneet paljon keskustelua viime vuosien aikana. Vaikka lohkoketjuteknologialla on potentiaalia kasvaa aikamme yhdeksi suurimmista keksinnöistä, sisältää kyseinen teknologia vielä paljon ratkaisemattomia ongelmia. Lohkoketjuteknologian yksi olennaisimmista ominaisuuksista on sen tuoma mahdollisuus luopua luotettavan kolmannen osapuolen käytöstä. Koska kyseessä on hajautettu järjestelmä, jonka oikeellisuudesta ei päätä kolmas osapuoli, löytyy motiivi yhteisymmärryksen saavuttamiseen lohkoketjujen käyttäjien mielten syvyyksistä. Peliteoria näyttelee suurta roolia lohkoketjujen toiminnassa, mutta sen lisäksi sen avulla on mahdollista havaita lohkoketjujen vielä toistaiseksi ratkaisemattomia riskitekijöitä. Nashin tasapaino on peliteorian suosituin konsepti, ja sen avulla käydään läpi lohkoketjujen toimintaa selvittämällä, mikä motivoi lohkoketjujen toimijoita toimimaan oikealla tavalla. Vangin dilemma puolestaan on yksi peliteorian tunnetuimmista esimerkeistä, ja sitä käytetään hyväksi lohkoketjujen ongelmien havaitsemisessa. Tutkielmassa käydään myös läpi, miten teknologian kehittyminen on lisännyt riskiä lohkoketjujen väärinkäytölle. Tutkimalla lisää peliteorian vaikutusta lohkoketjuihin voidaan lohkoketjujen kehitystä jatkaa oikeaan suuntaan ja sen turvallisuutta parantaa entisestään.

Asiasanat: lohkoketju, peliteoria, Nashin tasapaino, vangin dilemma, konsensusalgoritmit

ABSTRACT

Sarkonen, Atte
The effect of Game theory on the functionality of public blockchains
Jyväskylä: University of Jyväskylä, 2019, 30 pp.
Information systems, bachelor's thesis
Supervisor(s): Luoma, Eetu; Palonen, Teija

This thesis is about the effect of Game theory on the functionality of public blockchains, and it has been conducted as a literature review using peer reviewed papers and academic literature. Blockchain technology has awoken a lot of conversation during the last few years. Even though blockchain technology does have a lot of potential to become one of the biggest inventions of our time, it still has a lot of unresolved problems. One of the main features of the blockchain is the opportunity to cut out the use of any centralized third parties. Because blockchain technology is a distributed system in which validity is not verified by any trusted third party, the motive to achieve a consensus is formed from the vast body of blockchain users. Game theory plays a big part in the functionality of the blockchain, but it can also be used to detect the as of yet unsolved risks of blockchains. Nash Equilibrium is the most popular concept of Game theory, and in this thesis it's used to find out what motivates actors within the blockchain to make ethically sound decisions. Prisoner's dilemma is one of the most well known examples of blockchain decision-making, and it can be used in detecting the possible problems in blockchains. In this thesis it'll be discussed how the advance of blockchain technology has increased the risk for its abuse. By doing more research on the effect of Game theory on the functionality of the blockchain, the development of the blockchain can be continued in a positive direction and its security may be improved.

Keywords: blockchain, Game theory, Nash equilibrium, prisoner's dilemma, consensus algorithms

KUVIOT

SISÄLLYS

1 JOHDANTO

Lohkoketju on hajautettu lista validoituja sekä kryptograaffisesti turvattuja lohkoja, jotka on linkitetty toisiinsa kronologisessa järjestyksessä (Beck, Müller-Bloch & King, 2018). Koska lohkoketju pohjautuu hajautettuun ratkaisuun, ei sen oikeellisuudesta voi päättää vain yksi keskitetty toimija. Kun oikeellisuudesta on päättämässä useampi osapuoli, voi joukossa olla myös pahaenteisiä toimijoita. Mahdollisuus pahaenteiseen toimintaan voi osoittautua ongelmaksi, kun tavoitteena on päästä yhteisymmärrykseen lohkoketjun oikeellisuudesta. Tämä ongelma on ratkaistu konsensusalgoritmeilla, jollainen on esimerkiksi konsensusalgoritmeista yleisimmin käytetty Proof-of-Work (Salviotti, De Rossi & Abbatemarco, 2018). Kyseisessä konsensusalgoritmissa lohkoketjun oikeellisuudesta vastaa joukko niin kutsuttuja louhijoita, jollaiseksi kuka tahansa voi ryhtyä halutessaan. Nämä louhijat käyttävät tietokoneidensa laskentatehoa ratkaistakseen heille annettuja matemaattisia pulmia, josta heitä palkitaan lohkoketjun omalla kryptovaluutalla (Riasanow, Setzke, Burckhardt, Böhm & Kremar, 2018). Tämän niin sanotun louhinnan avulla lohkoketjua ylläpitävät solmut voivat varmentaa lohkoketjun oikeellisuuden. Louhinnasta palkintona annettavat kryptovaluutat ovat lohkoketjujen päällä toimivia virtuaalisia valuuttoja.

Peliteoria on sovelletun matematiikan osa-alue, jossa tarkastellaan toimijoiden välistä strategista kanssakäymistä (Myerson, 1991, s. 1). Se on eri tilanteisiin soveltuva teoreettinen ja metodologinen lähestymistapa, jonka avulla voidaan luoda ennusteita ja strategioita suotuisan tuloksen saavuttamiseksi (Krishnan, Balu, Smith & Pang, 2015). Koska lohkoketjun käyttäjäkunnan voi yleisesti uskoa koostuvan rationaalisista toimijoista, on lohkoketjun toimintaa mahdollista tutkia peliteorian avulla. Peliteoria mahdollistaa lohkoketjujen louhimisen, mikä taas mahdollistaa lohkoketjujen toiminnan. Asiaa tutkittaessa pidemmälle huomataan lohkoketjujen louhimisen sisältävän myös riskejä, jotka ovat hyötyjen tavoin mahdollista todistaa peliteorian avulla.

Hajautettuun ratkaisuun pohjautuvat lohkoketjut ovat tuoneet tullessaan uusia mahdollisuuksia toteuttaa erilaisia tietoteknisiä ratkaisuja (Nakamoto, 2008). Tämän teknologian avulla on mahdollista poistaa luotetun kolmannen osapuolen tarve, jonka ansiosta sillä on potentiaalia kasvaa aikamme suurim-

maksi muutokseksi heti internetin jälkeen. Koska kyseessä on hajautettu järjestelmä, jonka oikeellisuudesta ei päätä luotettu kolmas osapuoli, löytyy motiivi yhteisymmärryksen saavuttamiseen lohkoketjun käyttäjien mielten syvyyksistä. Peliteoriaa on mahdollista käyttää tämän tutkimiseen, ja se näytteleekin suurta roolia lohkoketjujen toiminnassa. Vaikka lohkoketjujen nähdään olevan yksi aikakautemme suurimmista muutoksista (Puthal, Malik, Mohanty, Kougianos & Yang, 2018), sisältää lohkoketjuteknologia vielä tällä hetkellä paljon toistaiseksi ratkaisemattomia ongelmia. Peliteorian avulla on mahdollista tutkia myös näitä lohkoketjun vielä toistaiseksi ratkaisemattomia riskitekijöitä.

Lohkoketjuteknologia jakaa myös paljon mielipiteitä meneillään olevan kryptovaluuttabuumin johdosta, jonka takia teknologian nimelle on kertynyt paljon stigmaa. Tässä kirjallisuuskatsauksessa on tarkoituksena lähestyä asiaa neutraalista näkökulmasta, käyden peliteorian avulla läpi lohkoketjujen toimintaa sekä riskitekijöitä. Tavoitteena on myös saada realistinen käsitys teknologian tämänhetkisestä tilasta.

Tutkielmassa pyritään vastaamaan seuraavaan tutkimuskysymykseen:

- Miten peliteoria liittyy julkisiin lohkoketjuihin?

Päätutkimuskysymystä avustavat seuraavat tutkimuskysymykset:

- Miten peliteoria mahdollistaa julkisten lohkoketjujen toiminnan?
- Miten peliteorian avulla voidaan havaita mahdollisuus julkisten lohkoketjujen väärinkäyttöön?

Tutkielma toteutettiin kirjallisuuskatsauksena vertaisarvioidun tieteellisen aineiston ja kirjallisuuden avulla. Tutkielman kehittämisessä käytettiin avuksi Okolin ja Schabramin (2010) opasta kirjallisuuskatsauksen luomiseen. Lähdekirjallisuus etsittiin käyttäen Google Scholaria, Scopusta sekä AIS eLibrarya. Lohkoketjuihin liittyvä aineisto haettiin pääosin hakusanoilla “blockchain”, “public blockchain”, “cryptocurrency”, “bitcoin” ja itse lohkoketjujen louhimiseen liittyvillä hakusanoilla “Proof-of-Work” sekä “Proof-of-Stake”. Peliteoriaan liittyvä aineisto haettiin hakusanoilla “game theory”, “Nash equilibrium” sekä “prisoner’s dilemma”. Yksittäisiä lähteitä löytyi myös yhdistämällä kirjallisuuskatsauksen aiheet. “Game theory and blockchain” hakusanalla löytyi myös muutamia aiheeseen liittyviä lähteitä. Löydetystä aineistosta pyrittiin rajaamaan pois vähiten lainatut tekstit. Sopivan aineiston puutteen vuoksi tutkielmassa ei pystytty täysin välttämään vertaisarvioimatonta aineistoa. Viimeinen sisältöluku myös sisältää verrattavan vähän lähteitä samaisen aineiston puutteen vuoksi.

Tämän tutkielman alussa käydään läpi lohkoketjuteknologian perusteet, ja esitellään kaksi suosituimpaa kryptovaluuttaa. Lohkoketjujen jaottelun ja perusperiaatteiden lisäksi keskitytään lohkoketjujen louhimiseen, konsensusmekaniikkaan sekä louhintayhtymiin, sillä kyseisiä aiheita tullaan viimeisessä sisältöluvussa tutkimaan peliteorian avulla. Kolmannessa luvussa perehdytään peliteoriaan käymällä läpi suosituin peliteorian konsepti, sekä yleisesti käytetty peliteorian esimerkki. Kolmannessa sisältöluvussa selvitetään miten nämä kaksi

liittyvät toisiinsa, eli miten peliteoria käytännössä ohjaa lohkoketjujen toimintaa ja miten peliteoriaa hyväksi käyttäen on mahdollista väärinkäyttää lohkoketjua sen nykyisessä tilassa. Lisäksi tutkielmassa selvitetään, miksi lohkoketjujen toiminnassa rehellisyys kannattaa ja miksi niiden väärinkäyttö puolestaan ei. Lopuksi tutkielmassa selvitetään myös, mitä ongelmia lohkoketjujen nykyisessä teknologiassa on, sekä miten tulevat teknologiat tulevat mahdollisesti ratkaisemaan nämä ongelmat.

2 LOHKOKETJUT JA KRYPTOVALUUTAT

Hajautettuun ratkaisuun pohjautuvat lohkoketjut ovat tuoneet tullessaan uusia mahdollisia tapoja toteuttaa erilaisia tietoteknisiä ratkaisuja. Lohkoketjujen käyttäminen on kannattavaa tilanteissa, joissa toisiinsa luottamattomat toimijat eivät halua käyttää luotettua kolmatta osapuolta, mutta haluavat silti pystyä muokkaamaan yhteisen järjestelmän tilaa (Würst & Gervais, 2017). Yksinkertaisesti selitettynä lohkoketjuteknologian avulla on mahdollista poistaa luotetun kolmannen osapuolen tarve pystyen silti tekemään esimerkiksi luottovapaita valuuttasiirtoja henkilöltä toiselle niin kutsuttujen kryptovaluuttojen avulla. Nämä kryptovaluutat ovat tämän hetken näkyvin lohkoketjuteknologiaa hyödyntävä keksintö, mutta lohkoketjuteknologian hyödyt eivät kuitenkaan lopu tähän. Tässä luvussa käydään läpi, mitä lohkoketjut ovat ja selitetään samalla kryptovaluutat niiden toimiessa erinomaisena esimerkkinä lohkoketjuteknologian potentiaalista. Lohkoketjujen jaottelun ja perusperiaatteiden lisäksi käydään tarkemmin läpi lohkoketjujen louhintaa, konsensusmekaniikkaa ja louhintayhtymiä, sillä kyseinen aihe on eräs tämän kirjallisuuskatsauksen olennaisimmista asioista.

2.1 Lohkoketjut

Tässä alaluvussa käydään läpi, mitä erilaisia lohkoketjuja on olemassa, sekä miten lohkoketjut yleisesti toimivat. Nakamoton (2008) kirjoittamassa paperissa Bitcoinin selitettiin käyttävän teknologiaa, joka myöhemmin ristittiin lohkoketjuksi. Bitcoinin lisäksi on olemassa useita muita kryptovaluuttoja, joista varteenotettavimmilla on usein omat lohkoketjunsa. Tällä hetkellä yleisin ja esimerkeissä eniten käytetyin on Bitcoinin lohkoketju, mutta esimerkiksi aiemmin mainittu Ethereum käyttää myös omaa lohkoketjuaan. Ethereumin lohkoketju mahdollistaa lohkoketjujen käytön muutenkin kuin vain vaihdon välineenä kryptovaluuttojen muodossa. Lisäksi on myös olemassa monia muita erilaisia lohkoketjuja, joiden toimintatavat saattavat poiketa huomattavasti edellä mainituista.

2.1.1 Lohkoketjujen jaottelu

Lohkoketjut voidaan jaotella yleisesti kolmeen osaan: julkisiin lohkoketjuihin, yksityisiin lohkoketjuihin sekä konsortiolohkoketjuihin (Kruijff & Weigand, 2017), joita myös luvallisiksi tai hybridilohkoketjuiksi välillä kutsutaan. Yksityiset lohkoketjut kulkevat myös joskus nimellä luvanvaraiset lohkoketjut. Ero näillä lohkoketjuilla on siinä, kuka hallinnoi lohkoketjun solmuja.

Julkisissa lohkoketjuissa solmuja pystyy ylläpitämään kuka tahansa. Julkinen lohkoketju on täysin läpinäkyvä, eli kenen tahansa on mahdollista päästä näkemään kaikki kyseisessä lohkoketjussa tapahtuneet siirrot aina alkulohkosta lähtien. Julkiset lohkoketjut ovat myös avoimia kaikille, eli kuka tahansa voi ottaa osaa niiden toimintaan esimerkiksi lähettämällä ja vastaanottamalla valuuttasiirtoja tai osallistumalla konsensuksen tekemiseen. (Kruijff & Weigand, 2017.) Julkisia lohkoketjuja kuvataan yleisesti julkisina tilikirjoina (Swanson, 2015). Tämä tarkoittaa sitä, että esimerkiksi Bitcoinin lohkoketju on kaikille avoin lista, jossa pidetään kirjaa kaikista Bitcoinien siirroista Bitcoinlompakoiden väleillä. Kryptovaluutat toimivat useimmiten julkisten lohkoketjujen päällä, sillä näiden käyttäminen johtaa parempaan informaation läpinäkyvyyteen.

Yksityisissä lohkoketjuissa solmujen ylläpidosta huolehtii yksi organisaatio (Kruijff & Weigand, 2017). Tämä omalla tavallaan vesittää lohkoketjujen perimmäisen idean luotettavan kolmannen osapuolen poistosta, sillä yksityiset lohkoketjut pakottavat käyttäjänsä luottamaan yhteen keskitettyyn toimijaan. Useat uskovat, etteivät yksityiset lohkoketjut ole varsinaisia lohkoketjuja, vaan enemmänkin hajautettuja tilikirjatekniikoita. (O'Connell, 2016.) Kun yksi toimija hallitsee koko lohkoketjua, pystyy tämä halutessaan muuttamaan lohkoketjun lohkojen sisältöä. Iansitin ja Lakhanin (2017) listanneista lohkoketjujen perusperiaatteista yksi on tietojen peruuttamattomuus, jota yksityiset lohkoketjut eivät edistä. Tämän takia esimerkiksi kryptovaluuttojen rakentamista yksityisten lohkoketjujen päälle ei nähdä järkevänä vaihtoehtona.

Useiden organisaatioiden ylläpitämät **konsortiolohkoketjut** nähdään osittain keskitettyinä, sillä vain pieni osa solmuista valitaan määrittämään konsensus (Zheng, Xie, Dai, Chen, Wang, 2017). Konsortiolohkoketjuja ei voida yksityisten lohkoketjujen tapaan nähdä yhtä luotettavina julkisessa käytössä kuin julkisia lohkoketjuja, sillä ne eivät toimi yhtä hajautetusti. Tästä huolimatta yksityisillä lohkoketjuilla sekä konsortiolohkoketjuilla on omat vahvuutensa, toimien julkisia lohkoketjuja paremmin esimerkiksi yrityksien sisällä, kun luottamattomuudelle ei ole varsinaista tarvetta. Konsortiolohkoketjuja kutsutaan myös hybridilohkoketjuiksi.

2.1.2 Julkisten lohkoketjujen viisi perusperiaatetta

Vaikka julkisia lohkoketjuja on mahdollista kuvata yksinkertaisina hajautettuina tietokantoina, on lohkoketjuteknologia todellisuudessa kompleksinen teknologia. Lohkoketjuteknologiaa on sanottu tukevan viisi perusperiaatetta: hajautuneisuus, vertaisverkkosiirrot, läpinäkyvyys peitettynä, tietojen korjautumat-

tomuus ja laskennallinen logiikka (Iansiti & Lakhani, 2017). Hajautuneisuus selittyy sillä, että lohkoketjujen verkot koostuvat erillisistä solmuista. Jokainen solmu omistaa kopion lohkoketjun nykyisestä tilasta, sisältäen tiedon kaikista lohkoketjun sisällä tapahtuneista transaktioista sekä kaikista osoitteista ja niiden saldoista. (Swan, 2015.) Yhdessä nämä solmut muodostavat lohkoketjun verkon. Lohkoketjujen hajautetun verkon olemus suojelee sitä, sillä vahingot on mahdollista kiertää (Bradbury, 2013). Eli vaikka jokin lohkoketjun toimija toimisi pahaenteisesti, ei tästä koidu lohkoketjulle haittaa enemmistön toimiessa pahaenteistä toimijaa vastaan.

Vertaisverkkosiirrot puolestaan viittaavat vapautukseen luotettavasta kolmannesta osapuolesta, jolloin toimijat voivat suorittaa siirtoja ilman välikäsiä. Tietojen läpinäkyvyys peitettynä tarkoittaa sitä, että käyttäjien lohkoketjussa käyttävät osoitteet ovat täysin satunnaiset, eikä niitä ole mahdollista yhdistää henkilöön, mikäli tämä on pitänyt osoitteensa salassa muilta. (Iansiti & Lakhani, 2017.)

Tietojen korjaamattomuudella viitataan siihen, ettei lohkoketjuun tallennettua tietoa ole mahdollista päästä enää jälkikäteen muokkaamaan. Lohkoketju on lista validoituja lohkoja, jossa jokainen lohko on linkitetty sen edeltäjään aina ensimmäiseen louhittuun lohkoon eli alkulohkoon (engl. genesis block) asti (Antonopoulos, 2015, s. 29). Lohkoketjun koko kasvaa jatkuvasti, sillä louhijat lisäävät siihen jatkuvasti lohkoja tallentaen viimeisimmät tapahtumat ja transaktiot lohkoketjuun. Nämä lohkot lisätään lohkoketjun jatkeeksi lineaarisessa, kronologisessa järjestyksessä (Beck ym., 2018).

Lohkoketju koostuu nimensä mukaisesti lohkoista. Jokainen lohko sisältää vapaamuotoisen datan, eli esimerkiksi tiettynä aikajaksoina suoritettujen valuuttasiirtojen lisäksi yksilöllisen tunnisteen (engl. hash). Lohkon oman tunnisteen lisäksi lohkoon liitetään myös edeltävän lohkon yksilöllinen tunniste. Lohkon tunnisteen luomisessa otetaan aina huomioon myös edeltävän lohkon yksilöllinen tunniste, jolloin onnistutaan luomaan turvallinen ketju. Lohkon yksittäinen tunniste muuttuu, jos yhdenkään aikaisemman lohkon sisältöä muokataan. Tämä todistaa lohkoketjun oikeellisuuden, ja sen ettei vanhempia lohkoja pysty muokkaamaan jälkikäteen. (Antonopoulos, 2015, s. 163.)

Laskennallisella logiikalla viitataan matemaattisiin haasteisiin pohjautuvaan hajautettuun konsensukseen. Nakamoton (2008) mukaan luottaminen kolmanteen osapuoleen ei ole enää tarpeellista vaan tärkeintä on, että elektroninen rahajärjestelmä perustuu kryptografisiin perusteisiin. Lohkoketjujen yksi olennaisimmista asioista on se, miten luottovapauteen päästään. Tämä ongelma on ratkaistu konsensusmekaniikalla, joka käydään tarkemmin läpi seuraavassa alaluvussa.

2.1.3 Louhiminen ja konsensusmekaniikka

Lohkoketjuun tallennetun informaation tarkastelu on mahdollista jokaiselle lohkoketjun toimintaan osallistuvalle toimijalle, mutta muutoksia lohkoketjuun on mahdollista tehdä ainoastaan saavuttamalla konsensus, eli lohkon luomi-

seen vaadittava yhteisymmärrys (Albrecht, Reichert, Schmid, Strüker, Neumann & Fridgen, 2018). Koska lohkoketjujen tarkoituksena on toimia hajautetusti, ei mikään toimija voi yksin varmentaa lohkojen oikeellisuutta. Konsensuksen luomiseen tarvitaan enemmistö lohkoketjun vertaisverkon solmuista, joilla kaikilla on oma käsitys lohkoketjun sen hetkisestä tilasta. Useamman käyttäjän ollessa päätöksenteossa on haasteellista päästä konsensukseen, sillä joukossa saattaa olla pahaenteisiä toimijoita. Tähän ratkaisuna käytetään erilaisia konsensusalgoritmeja, joista lohkoketjujen keskuudessa suosituin on tällä hetkellä esimerkiksi Bitcoinin ja Ethereumin käyttämä Proof-of-Work -menetelmä. (Salviotti, De Rossi & Abbatemarco, 2018.) Kyseisessä menetelmässä lohkoja tarkistaa louhijouksi (engl. miners) kutsuttu joukko. Nämä louhijat takaavat lohkoketjujen turvallisuuden käyttämällä esimerkiksi tietokoneen komponenttien laskentatehoa ratkaistakseen erilaisia kryptografisia arvoituksia (Eyal & Sirer, 2018). Louhinnan motiivina toimii rahallinen hyöty, sillä lohkoketjut kannustavat louhijoita palkitsemalla nopeiten oikein vastanneen louhijan uudella louhitulla valuutalla sekä louhitun lohkon sisältämien siirtojen siirtomaksuilla (Tsabary & Eyal, 2018). Louhiminen on siis laskentatehon myymistä palkkiota vastaan. Louhinnan seurauksena eniten laskentatehoa kerryttänyt lohko valitaan seuraavaksi lohkoksi ja lisätään ketjuun. Jos enemmistö laskentatehosta on rehellisten solmujen kontrolloimaa, kasvaa rehellinen ketju nopeammin kuin kilpailevat ketjut (Nakamoto, 2008).

Hyvä esimerkki havainnollistamaan louhintaa on ajatella tuhansien pelaajien kilpailullinen sudokukisa, jossa nopeiten sudokun selvittänyt pelaaja voittaa. Uusi sudoku aloitetaan aina, kun jokin pelaaja on läpäissyt pelin. Pelin vaikeustaso on asetettu dynaamisesti sellaiseksi, että pelaajilta menee keskimäärin noin kymmenen minuuttia ratkaisun löytämiseen. Tätä vaikeustasoa säädellään muuttamalla kentän rivien ja sarakkeiden lukumäärää. Sudokun ratkaisun oikeellisuuden tarkistaminen on paljon nopeammin tarkastettavissa, kun itse tehtävän ratkaisun päätteleminen. (Antonopoulos, 2015, s. 27.) Lohkoketjujen louhiminen voidaan nähdä samanlaisena tämän esimerkin kanssa: louhijoille annetaan matemaattinen lasku, jonka ratkaiseminen vaatii paljon laskentatehoa, mutta ratkaisun tarkistaminen on helppoa ja nopeaa. Vaikeustason määrittäminen on myös helposti säädeltävissä.

Proof-of-Workin ongelmana on sen suuri energiankulutus (Kiayias, Russell, David & Oliynykov, 2017), jonka vuoksi esimerkiksi Ethereumin lohkoketjun on tarkoitus siirtyä käyttämään vaihtoehtoista Proof-of-Stake konsensusalgoritmia (Buterin & Griffith, 2017). Proof-of-Stakessa varmentajien täytyy tehdä vakuustalletus pystyäkseen osallistumaan konsensuksen luomiseen (Buchman, 2016, s. 51). Käyttäjien mahdollisuus päästä varmentamaan lohko on suoraan verrannollinen heidän vakuustalletuksensa suuruuteen (Christidis & Devetsikiotis, 2016). Tehty vakuustalletus velvoittaa käyttäjiä toimimaan oikein lohkoketjussa, sillä heidän asettamansa talletus toimii panttina mahdollisuudelle osallistua konsensuksen luomiseen (Zheng, Xie, Dai, Chen & Wang, 2018).

2.1.4 Louhintayhtymät

Lohkopalkkioiden löytämisestä on tullut louhinnan haastavuuden lisäännyttyä entistä vaikeampaa vähemmän laskentatehoa omaaville louhijoille, jonka seurauksena enemmistö lohkoketjujen louhintatehosta tulee nykyään louhintayhtymiin (engl. mining pool) osallistuvilta louhijoilta (Schrijvers, Bonneau, Boneh & Roughgarden, 2017). Louhintayhtymät ovat kolmannen osapuolen hallinnoivia ryhmiä, jossa joukko louhijoita yhdistää ryhmäloton tavoin voimansa saadakseen enemmän laskentatehoa. Louhintayhtymän hallitsija koordinoi yhtymän louhijoiden laskentatehoa ja ulkoistaa louhimisen lähettämällä kryptografiset arvoitukset suoraan louhintayhtymän louhijoille (Gervais, Karame, Capkun & Capkun, 2014). Suurempi laskentateho kasvattaa yhtymän louhijoiden todennäköisyyttä lohkopalkkioiden saamiselle, mikä näkyy yksittäiselle louhijalle vakaampana tulonlähteenä. Etenkin pienille tekijöille louhintayhtymät ovat nykyään välttämättömyys, sillä yksin toimiessa todennäköisyydet lohkopalkkioiden saamiselle ovat lähestulkoon olemattomat. Osallistumalla louhintayhtymiin nämä pienemmätkin tekijät voivat olla osa suurempaa toimijaa, jolloin osuus tulevista lohkopalkkioista jaetaan samaan louhintayhtymään osallistuvien kanssa suhteessa heidän antamaa laskentatehoa vastaan. (Schrijvers ym., 2017.) Louhintayhtymät siis madaltavat kynnystä louhinnan aloittamiselle tekemällä siitä kannattavampaa pienemmille toimijoille, joka edesauttaa lohkoketjun ekosysteemin kasvamista.

Louhintayhtymät aiheuttavat kiistanalaisuutta lohkoketjujen yhteisössä, sillä enemmistön lohkoketjujen laskentatehosta tullessa keskittyneiltä louhintayhtymiltä vie tämä pohjan hajautetulta teknologialta (Schrijvers ym., 2017). Kuten aiemmin mainittiin, on hajautuneisuus eräs lohkoketjuteknologian tärkeimmistä ominaisuuksista sen mahdollistaessa demokratian toteutumisen louhinnassa. Lohkoketjujen louhimisen keskittyminen louhintayhtymille keskittää lohkoketjujen toimintaa, joka vie hyödyn hajautetulta järjestelmältä. Louhinnan keskittymisestä seuraa myös se, että mahdolliset vahingot ovat liian suuria kierrettäviksi.

Louhintayhtymät kasvattavat myös riskiä lohkoketjun tahalliselle vandalisoinnille. Pahaenteisen toimijan on mahdollista toteuttaa niin sanottu 51 % -hyökkäys lohkoketjussa, jos kyseinen toimija saa käsiinsä yli puolet lohkoketjun laskentatehosta (Zhao, Fan & Yan, 2016). Esimerkiksi Bitcoin Gold -kryptovaluutta koki vuonna 2018 51 % -hyökkäyksen, jonka ansiosta hyökkäyksen toteuttanut toimija tienasi 18 miljoonaa dollaria (Roberts, 2018). Aikana ennen louhintayhtymiä tämän hyökkäyksen onnistuminen olisi ollut erittäin epätodennäköistä, sillä onnistunut hyökkäys olisi vaatinut enemmistön louhijoista vannomaan tietyn väärän vastauksen oikeellisuutta. Vaikka louhijoiden tarkkaa lukumäärää on lähes mahdotonta saada selville, lohkoketjuista tilastoja vuodesta 2012 kerännyt Andrew Geyl (2015) arvioi vuonna 2015 pelkän Bitcoinin louhijoita olleen noin 100 000. Mikäli jokainen louhija omaisi saman verran laskentatehoa, olisi 51 % -hyökkäyksen toteuttaminen tuohon aikaan vaatinut yli 50 000 louhijan kontrolloimista. Vuoden 2015 jälkeen lohkoketjujen suosio on vain jatkanut kasvuaan, joten myös louhijoiden lukumäärän on syytä olettaa kasvaneen.

Louhintayhtymien ansiosta 51 % -hyökkäyksen toteutuminen on nykyään paljon todennäköisempää kuin ennen. Tällä hetkellä viiden suurimman louhintayhtymän yhteenlaskettu laskentateho ylittää 50 % Bitcoinin louhijoiden yhteenlasketusta laskentatehosta (Blockchain.info, 2019). Mikäli näiden louhintayhtymien ylläpitäjät päättäisivät väärinkäyttää Bitcoinin lohkoketjua, olisi se täysin mahdollista. Louhintayhtymien kautta louhiminen tapahtuu yleisesti erillisen sovelluksen kautta. Mikäli tämän sovelluksen lähdekoodi ei ole avointa, voisi louhintayhtymän ylläpitäjä käyttää louhijoita hyväksi 51 % -hyökkäyksen toteuttamisessa.

2.2 Kryptovaluutat

Tässä alaluvussa käydään läpi tämän hetken suosituimmat kryptovaluutat, Bitcoin ja Ethereum. Kryptovaluuttojen kirjo on laaja: CoinMarketCap.com (2018) -sivuston mukaan virallisia kryptovaluuttoja on tällä hetkellä yli 2000, mutta tässä tutkielmassa keskitymme ainoastaan kahteen suosituimpaan kryptovaluuttaan.

Kryptovaluutat ovat lohkoketjuteknologian päällä toimivia digitaalisia valuuttoja, joiden siirtelyyn verkossa ei tarvita luotettavaa kolmatta osapuolta. Luotettavan kolmannen osapuolen, esimerkiksi pankin tai muun palveluntarjoajan sijaan elektronisia varojen siirtoja on mahdollista tehdä suoraan yksityisten henkilöiden välillä.

2.2.1 Bitcoin

Ensimmäisen kryptovaluutan eli Bitcoinin kehittäjänä toimi nimimerkkiä Satoshi Nakamoto käyttävä yksittäinen henkilö tai ryhmä, jonka identiteetti on vielä tähän päivään asti pysynyt salassa aiheuttaen kiihkeää spekulointia (Taylor, 2013). Vuonna 2008 Satoshi Nakamoto julkaisi paperin vertaisverkkoa hyödyntävästä elektronisesta rahajärjestelmästä nimeltä Bitcoin (Nian & Chuen, 2015, s. 11), joka on lohkoketjuksi nimetyn luottovapaan hajautetun julkisen tilikirjan päällä toimiva internetissä siirreltävä digitaalinen valuutta (Swan, 2015, s. 7). Bitcoin on täysin elektroninen valuutta, jota on mahdollista siirtää verkon yli ilman kolmatta osapuolta (Antonopoulos, 2015, s. 1).

Koko Bitcoinia Nakamoto ei kuitenkaan ole rakentanut yksin, vaan tähän päivään mennessä Bitcoinin lohkoketjua on ollut kehittämässä vajaa 600 kehittäjää (github.com/bitcoin, 2018). Bitcoin perustuu avoimeen lähdekoodiin, jota kukaan ei omista tai kontrolloi. Tämän lisäksi myös kuka tahansa voi ottaa osaa Bitcoinin toimintaan monin eri tavoin (bitcoin.org, 2018). Näitä tapoja on esimerkiksi Bitcoinien käyttäminen, Bitcoinin solmun ylläpitäminen, jo edellä mainittu osanottaminen Bitcoinin kehitykseen sekä Bitcoinien louhiminen.

2.2.2 Ethereum

Kryptovaluuttojen toteutustapa vaihtelee: Monet niin sanotuista vaihtoehtovaluutoista (engl. altcoin) ovat ottaneet mallia Bitcoinin lähdekoodista sisältäen samoja ominaisuuksia kuin Bitcoin, mutta jotkut järjestelmät on suunniteltu täysin erilaisiksi (Bonneau, Miller, Clark, Narayan, Kroll & Felten, 2015). Erinomainen esimerkki Bitcoinista eroavasta suunnittelusta on Ethereum.

Ethereum laajentaa Bitcoinin toimintamallia luomalla käyttäjilleen mahdollisuuden ohjelmoida älysopimuksia (Nofer, Gomber, Hinz & Schiereck, 2018). Nämä älysopimukset ovat Ethereumin lohkoketjun käyttäjien kirjoittamia lohkoketjuun säilöttyjä ohjelmia, joita voi ajaa anonyymisti ilman riskiä häiriöajoista, sensuurista tai petoksista (Beck, Avital, Rossi & Thatcher, 2017). Ethereumin keksijä Vitalik Buterin (2013) on itse maininnut Ethereumin julkaisupaperissa älysopimusten olevan järjestelmiä, jotka siirtävät digitaalisia varoja ennalta määriteltyjen sääntöjen mukaan.

Bitcoinin tapaan myös Ethereumin toimintaan voi kuka tahansa ottaa halutessaan osaa. Vaikka Ethereumin lohkoketjussa tärkeimpänä uudistuksena ja ominaisuutena pidetäänkin älysopimuksia, on Ethereumilla Bitcoinin tavoin myös oma kryptovaluuttansa, jota kutsutaan Etheriksi. Vaihdon välineenä käytön lisäksi Ether on tärkeä siksi, että se on välttämätöntä älysopimuksia ajettaessa. Mikäli Ethereumin lohkoketjuun halutaan tallentaa dataa älysopimuksen kautta tai jo olemassa olevaa tietoa halutaan muokata, joudutaan tästä maksamaan pieni summa Etheriä (Buterin, 2013). Tätä pientä maksua kutsutaan kaasuksi (engl. gas). Kun kaasua on käytetty ohjelman ajamiseen, kulkeutuu maksuna otettu kaasu Ethereumin lohkoketjun kiertokulussa aina lohkon louhijoille asti.

Ethereum siis laajentaa Bitcoinin lohkoketjua luomalla alustan hajautettujen sovellusten luomiselle. Vaikka Bitcoinin ja Ethereumin ensisijaiset ominaisuudet poikkeavat toisistaan, ovat niiden päällä toimivat vaihdon välineenä toimivat valuutat niitä yhdistävä tekijä. Molemmissa lohkoketjuissa rahanarvoiset valuutat ovat päteviä toimimaan louhinnan motiivina.

3 PELITEORIA

Tässä sisältöluvussa käydään läpi, mikä peliteoria on ja otetaan lähempään tarkkailuun peliteorian suosituin konsepti, Nashin tasapaino sekä yleisesti käytetty peliteorian esimerkki, vangin dilemma. Nashin tasapainon ja vangin dilemman avulla peliteorian ja lohkoketjujen välistä suhdetta tarkkaillaan seuraavassa sisältöluvussa. Peliteoriaan aiheena ei paneuduta tarkemmin matemaattisesti, vaan asiat käydään läpi yleisemmällä tasolla. Lopuksi käydään läpi myös analyysin laatimista, jonka avulla ymmärretään paremmin, mitä asioita on otettava huomioon sovellettaessa peliteoriaa oikean elämän tilanteisiin, esimerkiksi lohkoketjuihin.

Ernst Zermelo kirjoitti 1900-luvun alkupuolella artikkelin shakista, jossa hän loi ensimmäisen peliteorian konseptin (Schwalbe & Walker, 2001). Kiinnostus peliteoriaa kohtaan lähti suurempaan nousuun vasta Von Neumannin ja Morgensternin esiteltyä enemmistön peliteorian piirteistä vuonna 1944, jonka jälkeen peliteoriaa ollaan aloitettu käyttämään hyväksi esimerkiksi yhteiskunta- ja taloustieteessä (Camerer, 2003, s. 2). Nykyään peliteoriaa käytetään yleisesti monella alalla.

3.1 Peliteoria yleisesti

Peliteoriassa tutkitaan matemaattisten mallien avulla älyllisten ja rationaalisten päätöksentekijöiden välillä tapahtuvia konflikteja sekä yhteistyötä. Mikäli päätöksentekijöiden valinnat vaikuttavat muiden rationaalisten päätöksentekijöiden valintoihin, kutsutaan peliteorian pelitilannetta strategiaa vaativaksi pelitilanteeksi. Yleinen käsitys on, että tällaisessa strategisessa tilanteessa pelaajat tekevät valintansa yrittäen maksimoida heidän saamansa hyödyn, mikä tekee päätöksentekijöistä rationaalisia. Peliteoriassa samassa pelitilanteessa olevat pelaajat voivat myös olettaa vastapuolen olevan heidän tavoin älyllinen ja rationaalinen päätöksentekijä. Peliteoriassa mietitään miten päätöksentekijän kannattaa toimia strategiaa vaativassa tilanteessa, kun hänen päätöksentekonsa

riippuu siitä, mitä vastapuoli ajattelee päätöksentekijän tekevän. (Myerson, 1991, s. 1.)

Peliteorian teho tulee sen matemaattisen tarkkuuden lisäksi myös sen yleisyydestä (Camerer, 2003, s. 2). Yleisyydellä tässä tilanteessa tarkoitetaan sitä, että peliteoriaa voidaan käyttää hyväksi monenlaisissa tilanteissa monenlaisten toimijoiden kesken. Pelitilanteella ei esimerkiksi välttämättä tarkoiteta aina varsinaista peliä, kuten enemmistö ihmisistä kuvittelee (Krishnan ym., 2015), vaan kyseessä voi esimerkiksi olla kaupan strategiointi tuotteiden hinnoittelussa. Toimijat voivat myös tilanteesta riippuen vaihdella yksittäisestä henkilöstä aina kokonaisiin valtioihin, jolloin pelitilanne voi vaihdella aina shakki- tai tennisottelusta useamman maan välisiin poliittisiin toimiin. Erinomainen tosielämän esimerkki on myös pokeri: kannattaako pelaajan bluffata riippuu täysin siitä, uskooko hän vastapuolensa ajattelevan pelaajan tekevän niin.

3.2 Nashin tasapaino

Muutama vuosi Von Neumannin ja Morgensternin esiteltyä enemmistön peliteorian piirteistä amerikkalainen matemaatikko John Nash esitti ratkaisun ongelmaan rationaalisten pelaajien käyttäytymisestä. Tämä ratkaisu nimettiin myöhemmin Nashin tasapainoksi (engl. Nash equilibrium). (Camerer, 2003, s. 2.) John Nashin kehittämä Nashin tasapaino on yleisimmin käytetty peliteorian konsepti (Osborne & Rubinstein, 1994).

Nashin tasapainon ideana on, että pelaajat muuttavat strategiaansa, kunnes yksikään pelaaja ei voi enää hyötyä muutoksesta (Camerer, 2003, s. 2). Tasapaino saavutetaan sillä hetkellä, kun yhdelläkään päätöksentekijällä ei ole syytä poiketa käyttämästään strategiasta. Nashin tasapainoja on mahdollista olla pelitilanteessa useampia ja jotkut näistä voivat olla ristiriidassa pelaajan intuitiivisen käsityksen kanssa (Myerson, 1978).

Nashin tasapaino toteutuu useimmiten pelitilanteen toistuessa tarpeeksi monta kertaa (Pearce, 1984). Mikäli tilanne toistuu tarpeeksi monta kertaa, pelaajat pyrkivät parantamaan lopputulemaansa aina tasapainon saavuttamiseen asti, jolloin pelaajien tuloksen hyöty on maksimoitu. Nopealla varoitusajalla mahdollisuus epäsuotuisalle valinnalle on suurempi, joten pelaajan on mahdollista päätellä paras mahdollinen strateginen valinta yhdelläkin kerralla, mikäli hänellä on tarpeeksi aikaa.

3.3 Vangin dilemma

Yksi peliteorian suosituimmista esimerkeistä on vangin dilemma (engl. prisoner's dilemma). Vangin dilemmassa kahden henkilön on päätettävä samanaikaisesti, tekevätkö he yhteistyötä toisen henkilön kanssa vai pettävätkö he tä-

män. Vangin dilemman pulmana on, että kumpikaan henkilö ei voi tietää parasta ratkaisua kahden vaihtoehdon välillä tietämättä toisen henkilön valintaa (Heylighen, 1993).

Vangin dilemma on saanut nimensä seuraavasta hypoteettisesta tilanteesta: Kaksi henkilöä on pidätetty epäiltynä pienestä rikoksesta. Poliisi tietää heidän molempien osallistuneen myös suurempaan rikokseen, mutta tästä rikoksesta viranomaisilla ei ole tarpeeksi todisteita heidän tuomitsemiseen. Epäillyt eristetään toisistaan ja heitä kuulustellaan erikseen. Kuulustelutilanteessa molemmille tarjotaan sopimusta: mikäli epäilty lupaa todistaa rikoskumppaniaan vastaan, päästetään hänet vapaaksi. Molemmat syytetyt voivat siis joko hylätä tarjouksen ja vaieta tai hyväksyä tarjouksen ja todistaa rikoskumppaniaan vastaan. Mikäli kumpikaan epäilty ei ota tarjousta vastaan, tuomitaan heidät molemmat todisteiden puuttuessa vuoden vankeusrangaistukseen pienestä rikoksesta. Mikäli vain toinen epäillyistä hyväksyy tarjouksen, pääsee hän vapaaksi välttyen täysin tuomiolta. Hänen rikoskumppaninsa puolestaan saa viiden vuoden vankeustuomion isommasta rikoksesta, sillä häntä vastaan on riittävää todistusaineistoa ja hän kieltäytyi tekemästä yhteistyötä poliisin kanssa. Mikäli molemmat syytetyt hyväksyvät tarjouksen, tuomitaan heidät molemmat suuremmasta rikoksesta kolmeksi vuodeksi vankeuteen. Tuomiota on kuitenkin lievennetty tässä tilanteessa, sillä molemmat epäillyt toimivat yhteistyössä poliisin kanssa todistettuaan rikoskumppaniaan vastaan (kuvio 1).

		Henkilö A	
		Hylkää tarjouksen	Hyväksyy tarjouksen
Henkilö B	Hylkää tarjouksen	(1,1)	(5,0)
	Hyväksyy tarjouksen	(0,5)	(3,3)

KUVIO 1 Vangin dilemma

Ottamatta huomioon mitä toinen osapuoli valitsee, on vastapuolen pettäminen aina henkilölle itselleen parempi vaihtoehto, mutta yhteisen hyvän vuoksi paras vaihtoehto molemmille on yhteistyön tekeminen (Lönnqvist, Verkasalo & Walkowitz, 2011). Mikäli molemmat hylkäävät tarjouksen ja toimivat yhteisen hyvän vuoksi yhteistyössä, on heidän yhteenlaskettu vankeusrangaistuksensa kaksi vuotta. Muissa tilanteissa yhteenlaskettu vankeusrangaistus on suurempi, mutta yksilöillä on mahdollisuus selvitä pienemmällä rangaistuksella. Mikäli yksilö pettää, selviää hän itse aina pienemmällä rangaistuksella kuin yhteistyössä olisi ollut mahdollista. Tämän takia yksilölle vastapuolen pettäminen on aina paras vaihtoehto. Ainoa vahva Nashin tasapaino saavutetaan vangin dilemmassa tilanteessa, jossa molemmat osapuolet pettävät vastapuolen. Tällöin kummankaan pelaajan ei ole mahdollista parantaa omaa asemaansa muuttamalla vain omaa strategiaansa.

Pelaajien ratkaisut riippuvat monista tekijöistä, esimerkiksi heidän välisestä suhteestaan (Axelrod, 1980, s. 5). Mikäli esimerkin pelitilanteessa olevat päätöksentekijät luottavat toisiinsa täysin, on yhteistyö epäiltyjen välillä jopa todennäköistä. Mikäli henkilöt eivät luota toisiinsa on yksilölle aina varminta pettää vastapuoli. Yksilön dilemmaan vaikuttaa paljon hänen kyky luottamaan vastapuoleen vankeusrangaistuksen uhalla.

3.4 Analyysin laatiminen

Toimijoiden välisen suhteen lisäksi tasapainoa tutkiessa täytyy ottaa huomioon monia muitakin asioita. Jackson (2011) listasi kirjoittamassaan paperissa neljä eri kohtaa, jotka täytyy huomioida peliteoriaa analysoitaessa. Ensimmäiseksi pitää tietää, keitä pelaajat ovat: ovatko he yksittäisiä henkilöitä, vaiko esimerkiksi yrityksiä? Mitä sukupuolta pelaajat edustavat tai mihin etniseen ryhmään he kuuluvat?

Toinen huomioitava seikka on tietää, mitä mahdollisia toimintoja pelaajilla on käytettävissään. Toisin kuin vangin dilemmassa, oikean elämän peliteorian tilanteissa toimijoilla voi olla enemmän kuin kaksi vaihtoehtoa, joten kaikki vaihtoehdot on otettava huomioon. Niin sanotuissa täydellisen informaation peleissä (engl. perfect information) pelaajat tietävät kaikki omat ja muiden mahdolliset toimintavaihtoehdot sekä aiemmat valinnat. (Khomskii, 2010.)

Kolmanneksi on tiedettävä, miten vuorovaikutus ajoitetaan. Tehdäänkö toiminnot samaan aikaan, toistuuko vuorovaikutus ja missä järjestyksessä pelaajien toiminnot suoritetaan? Tieto edellisen pelaajan valinnasta voi asettaa jälkimmäisen pelaajan etulyöntiasemaan. Tämän lisäksi tapahtuman toistuessa useasti pelaajat voivat oppia pelaamaan optimaalisesti. Mikäli peliä toistetaan loputtomiin, saavuttavat pelaajat todennäköisesti lopulta jonkin Nashin tasapainon (Pearce, 1984). Analyysia laatiessa pitää myös olla tietoinen, mitä tietoa eri pelaajilla on toiminnan hetkellä. Mikäli pelaajat ovat valintojen jälkeen tietoisia toisen pelaajan valinnoista, voi lopputulos muuttua täysin. Esimerkiksi mikäli vangin dilemmassa toinen pelaaja saisi ensin tietää toisen päätöksen, voisi hän riskittömästi valita itselleen parhaimman vaihtoehdon syyttämisen tai syyttämättä jättämisen välillä. Neljäntenä täytyy tietää, mikä on lopputulos eri pelaajille minkäkin toiminnan seurauksena. Vangin dilemman tilanteessa pelaajien valinnat voivat vaihdella riippuen siitä, onko tuomiona ainoastaan sakko vaiko vankeusrangaistus.

Reinhard Selten (1975) esitteli artikkelissaan vapisevan käden tasapainon (engl. trembling hand equilibrium), jonka ideana on se, että mikään ei ole koskaan täysin varmaa. Vapisevan käden tasapainon mukaan on aina mahdollista, että pelaaja tekee virheen ja valitsee odottamattoman vaihtoehdon. Tämä voisi toteutua esimerkiksi tilanteessa, jossa pelaaja painaa vapisevalla kädellään vahingossa väärää nappia. Vapisevan käden tasapainot ovat vakaita siinä mielessä, että pienet muutokset pelin rakenteessa eivät muuta pelaajien käyttäytymistä tasapainossa (Kultti, 1994).

4 PELITEORIAN VAIKUTUS JULKISIIN LOHKOKETJUIHIN

Koska lohkoketjun käyttäjät ovat älyllisiä ja rationaalisia päätöksentekijöitä, voidaan peliteorialla matemaattisia malleja hyväksi käyttäen tutkia näiden välistä vuorovaikutusta. Nashin tasapainoa hyödyntäen on mahdollista selvittää, mikä mahdollistaa lohkoketjun jatkuvan toiminnan, eli erityisesti sen, miten lohkoketjun louhijoita kannustetaan rehellisyyteen ja miksi pahaenteinen toiminta lohkoketjussa ei ole kannattavaa louhijalle.

Teknologioiden kehittyessä ajan myötä myös lohkoketjujen on täytynyt mukautua. Tästä seuranneiden muutosten johdosta on syntynyt uusia tapoja väärinkäyttää lohkoketjuja. Kuten lohkoketjun toiminnan mahdollistavat tekijät, on myös lohkoketjun väärinkäytön riskit mahdollista todistaa peliteorian avulla. Lohkoketjuteknologioissa on tiettyjä riskitekijöitä, joten on myös hyvä käydä läpi, miten tulevat lohkoketjun uudistukset pystyvät mahdollisesti ratkaisemaan tämänhetkisiä ongelmia.

4.1 Lohkoketjun toiminnan mahdollistaminen

Lohkoketjujen louhimisessa motivoijana toimii rahallinen hyöty, sillä louhijoita palkitaan lohkojen louhinnasta. Koska palkkio annetaan oikean vastauksen nopeiten laskijalle, kannustaa lohkoketjun toiminta luonnostaan louhijaa löytämään oikean vaihtoehdon virheellisen sijaan. Louhimisen merkitys hallinnan työkaluna on merkittävä sen ohjatessa louhijoiden yhteisön käytöstä (Ziolkowski, Miscione & Schwabe, 2018).

Yleinen käsitys on, että louhijat ovat rationaalisia päätöksentekijöitä, eli he yrittävät maksimoida saamansa hyödyn. Tässä tilanteessa hyödyn on luontevaa olettaa olevan taloudellinen, sillä louhimista motivoi rahallinen hyöty (Tsabary & Eyal, 2018). Mikäli käyttäjät eivät olisi rationaalisia, voisi lopputulos olla toista eikä lohkoketjun toiminta välttämättä toteutuisi odotetulla tavalla.

Käyttäjälle on siis kannattavinta toimia oikealla tavalla. Väärästä vastauksesta louhija ei hyödy, vaan käyttää ainoastaan aikaa ja laskentatehoa hukkaan. Koska louhimisessa tarvitaan suuria määriä laskentatehoa, kuluttaa louhiminen suuria määriä sähköä (Kiayias ym., 2017). Mikäli käyttäjä yrittää tahallisesti laskea lohkoja väärin, ei hän menetä ainoastaan mahdollisuuttaan ansaita lohkopalkkioita vaan jää hän myös taloudellisesti tappiolle louhinnasta koituvan sähkönkulutuksen myötä. Tämän lisäksi myös komponenttien kuluminen on syy sille, minkä takia louhiminen olisi palkitsemattomana taloudellisesti kannattamatonta. Lohkoketjujen louhimisessa käytetyt tietokoneen komponentit ovat kulutusosia, jotka kuluvat käytössä. Louhimisessa komponentit joutuvat koville laskentatehoa vaativien suurten laskutoimitusten takia, joka yhdessä kovassa käytössä olemisesta johtuvan korkean lämpötilan kanssa kuluttaa komponentteja pitkässä juoksussa. Proof-of-Workin nerokkuus piilee siinä, että louhimisesta on tehty mahdollisimman tehotonta. Tehottoman louhimisen ansiosta lohkoketjujen väärinkäyttö olisi pahaenteiselle toimijalle taloudellisesti kannattamatonta, joka taasen motivoi louhijoita toimimaan oikein. Louhija saavuttaa Nashin tasapainon toimiessaan oikein, sillä muuttamalla strategiaansa hänen ei ole mahdollista saada enempää hyötyä.

Lohkoketjun louhijat ovat kaikki yksilöitä, ketkä tekevät päätöksensä tarkoituksenaan maksimoida oma hyöty. Louhijat luovat oman päätöksensä sen pohjalta, mitä he odottavat muiden louhijoiden tekevän. Enemmistö louhijoista odottaa muiden louhijoiden toimivan oikein, mikä motivoi myös yksittäisiä louhijoita toimimaan oikein. Tämän takia myös muut louhijat olettavat enemmistön toimimaan oikein louhiessaan. Tätä kutsutaan itseään ruokkivaksi Nashin tasapainoksi. (Buterin, 2015.) Suurin osa lohkoketjun louhijoista päätyy toimimaan odotettavasti sen maksimoidessa käyttäjien saaman hyödyn. Pahaenteiset toimijat jäävät puolestaan vähemmistöksi, päätyen näin ollen taloudellisesti tappiolle yrittäessään väärinkäyttää lohkoketjua.

4.2 Riskit lohkoketjujen toiminnassa

Vaikka lohkoketjujen väärinkäyttö on tehty lähes mahdottomaksi, on sen riski aina olemassa. Peliteorian avulla on mahdollista todistaa lohkoketjujen toiminta, mutta ainoastaan mikäli lohkoketjun toimintaan osallistuvat toimijat ovat rationaalisia päätöksentekijöitä. Todellisuudessa näin ei kuitenkaan välttämättä ole. Päätöksentekijä ei välttämättä ole rationaalinen, eikä rationaalisenkaan päätöksentekijän toimet ole välttämättä aina odotettuja, kuten vapisevan käden tasapaino osoitti. Vaikka päätöksentekijä on rationaalinen, ei tämä siltikään välttämättä tarkoita hänen motiivinsa olevan taloudellisen hyödyn maksimoimisessa.

Kuten aiemmin mainittiin, kasvattavat louhintayhtymät riskiä lohkoketjun väärinkäytölle. Kuten lohkoketjun toiminnan mahdollistaminen, on myös riskit lohkoketjun väärinkäytölle mahdollista todistaa peliteorian avulla. Vangin di-

lemmaa hyväksi käyttämällä on mahdollista löytää Nashin tasapaino tilanteisiin, jossa toimijoilta vaaditaan strategista ajattelua. Lohkoketjun toimijoiden ollessa rationaalisia päätöksentekijöitä on luontevaa ajatella heidän yrittävän maksimoida taloudellinen hyötynsä, sillä se toimii louhinnan motiivina. Mikäli pahaenteinen toimija luo oman louhintayhtymänsä, jossa louhijalle tarjotaan rehellistä yhteisöä enemmän voittoa, rationaaliset louhijat valitsevat hyökkääjien yhteisön rehellisten sijaan paremman taloudellisen voiton toivossa, näin ollen kasvattaen yhteisön kokoa, kunnes yhteisöstä kasvaa louhijoiden enemmistö (Eyal & Sirer, 2018). Tämän skenaarion tapahtuessa pahaenteisen louhintayhtymän hallitsijan maksettavaksi jää ainoastaan louhimisen lisäksi maksettava ylimääräinen summa, minkä hän maksaa louhijoille jokaisen lohkon louhimisen yhteydessä tai louhintayhtymän saadessa lohkopalkkion. Nashin tasapaino löytyy tilanteessa kohdasta, jossa yksittäinen louhija louhii pahaenteisessä louhintayhtymässä, sillä tällöin louhijan ei ole mahdollista parantaa lopputulemaansa muuttamalla omaa strategiaansa. Mikäli enemmistö louhijoista siirtyy pahaenteisen louhintayhtymän käyttöön, jää yksittäinen louhija tappiolle louhiessaan hyväntahtoisesti (kuvio 2).

		Louhija A	
		Hyväntahtoinen louhintayhtymä	Pahaenteinen louhintayhtymä
Muut lohkoketjun louhijat	Hyväntahtoinen louhintayhtymä	(1,1)	(1+n,1)
	Pahaenteinen louhintayhtymä	(0,1)	(1,1)

KUVIO 2 Louhintayhtymän valitseminen

Yhteisön kasvettua louhintatehon enemmistöksi mahdollistaa tämä 51 % -hyökkäyksen suorittamisen (Zhao ym., 2016). Mikäli jokin toimija tai yhteisö saa haltuunsa 51 % kontrollin louhinnasta ja koska lohkoketjuissa lohkoksi valitaan enemmistön valitsema lohko, voisi pahaenteinen toimija enemmistön puolelleen saatuaan syöttää lohkoketjuun väärää dataa sisältäviä lohkoja tavoitellen taloudellista hyötyä (Eyal & Sirer, 2018). Taloudellisen hyödyn lisäksi pahaenteisellä toimijalla voi olla täysin eri motiivit. Hypoteettisessa tilanteessa, jossa Bitcoinista on tullut maailman yleisimmin käytetty valuutta, voi tarpeeksi varakas toimija esimerkiksi vihan tai politiikan motivoivana suorittaa 51 % -hyökkäyksen Bitcoinia vastaan horjuttaen maailmantaloutta. Onnistunut 51 % -hyökkäys antaa lohkoketjun hallinnon pahaenteiselle toimijalle ja tuhoaa sen hajautuneisuuden (Eyal & Sirer, 2018). Tämä vaikuttaa riskin olemassaolo väärjäämättä Bitcoinin sekä muiden kryptovaluuttojen uskottavuuteen ja luotettavuuteen.

Taloudellista hyötyä tavoitellessaan voi pahaenteisen toiminnan yrittäminen olla riski, sillä käyttäjien on mahdollista menettää luottamus lohkoketjuun,

josta on mahdollista seurata lohkoketjun kryptovaluutan arvon tippuminen. Mikäli motiivina on esimerkiksi viha, ei riski taloudellisen hyödyn menettämisestä ole pätevä syy luopua toteutuksesta. Käyttäjä voi myös toimia epärationaalisesti, jolloin motiivia ei välttämättä ole.

Yksi ratkaisu tähän louhintayhtymien aikaansaamaan riskiin on eri konsensusalgoritmiin siirtyminen. Nykyinen Proof-of-Work ottaa huomioon ainoastaan laskentatehon määrän, joten suurella määrällä raakaa laskentatehoa on mahdollista väärinkäyttää kyseistä konsensusalgoritmia käyttäviä lohkoketjuja. Todennäköisimpänä ratkaisuna ollaan pidetty siirtymistä Proof-of-Stake konsensusalgoritmiin, jossa käyttäjät asettavat hetkellisesti jäädytettävän panoksen lohkoketjun kryptovaluutasta. Toisin kuin Proof-of-Workissa, Proof-of-Stake konsensusalgoritmissa lohkon tarkistusta ei pääse tekemään eniten laskentatehoa omaava, vaan suurimman panoksen omaavalla on suurin todennäköisyys päästä validoimaan lohko. Jos lohkon validoija toimii väärin, menettää hän jäädytetyn panoksensa.

Yleisen käsityksen mukaan käyttäjien on epätodennäköisempää väärinkäyttää lohkoketjua, mikäli tämä johtaisi heidän omaan taloudelliseen tappioon (Zheng ym., 2018). Yritykset vahingoittaa Proof-of-Stake konsensusalgoritmia käyttävää lohkoketjua tulisivat pahaenteiselle toimijalle entistä kalliimmaksi (Lin & Liao, 2017) heidän menettäessään lohkoketjuun asettamansa vakuustalletuksen.

5 YHTEENVETO

Tässä tutkielmassa tutkittiin peliteorian vaikutusta julkisiin lohkoketjuihin. Lohkoketju on hajautettuun ratkaisuun pohjautuva teknologia, joka koostuu kronologisessa järjestyksessä toisiinsa linkitetyistä varmennetuista lohkoista. Lohkoketjuteknologian suurin innovaatio on mahdollisuus päästä eroon tarpeesta luottaa kolmanteen osapuoleen, sillä lohkoketjun ansiosta käyttäjien ei tarvitse luottaa muuhun kuin todistettavissa olevaan lohkoketjun protokollaan. Koska lohkoketju on luottovapaa hajautettuun ratkaisuun pohjautuva teknologia, on käyttäjien päästävä yhteisymmärrykseen sen sisällä tapahtuneista transaktioista. Yhteisymmärrykseen pääseminen on luottovapaissa lohkoketjuissa välttämätöntä, vaikka osa toimijoista olisi pahaenteisiä. Tähän yhteisymmärrykseen eli konsensukseen on mahdollista päästä lohkoketjuteknologian käyttämien konsensusalgoritmien avulla. Konsensusalgoritmeista tällä hetkellä yleisin Proof-of-Work hajauttaa konsensukseen pääsemisen luomalla kryptografisia laskutoimituksia, joita niin kutsutut louhijat suorittavat rahallista palkkiota vastaan. Ensimmäiselle oikein vastanneelle louhijalle annetaan palkkioksi lohkopalkkio, joka koostuu uudesta louhitusta valuutasta sekä louhitun lohkon sisältämien siirtojen siirtomaksuista.

Teknologian kehittyminen on johtanut tietokoneiden komponenttien laskentatehon nousemiseen, jonka vuoksi myös louhimisen vaikeustaso on kasvanut. Louhimisen vaikeustason kasvamisen vuoksi vähemmän laskentatehoa omaavilla pienemmillä toimijoilla ei ole enää samanlaista mahdollisuutta päästä käsiksi lohkopalkkioihin. Tämän seurauksena on luotu kolmansien osapuolten ylläpitämiä louhintayhtymiä, joissa useampi tekijä yhdistää voimansa jakaen mahdolliset tuotot yhtymään osallistuneiden louhijoiden kesken. Louhintayhtymät tuovat yksinkertaisemman käyttökokemuksen lisäksi tasaisemman tulonlähteen, jonka vuoksi niiden käyttäminen on yleistynyt louhijoiden keskuudessa. Toisaalta louhintayhtymät ovat myös kasvattaneet väärinkäytöksen riskiä niiden keskittäessä lohkoketjun toimintaa. Louhintayhtymän saadessa käyttöönsä yli 50 % lohkoketjun yhteenlasketusta laskentatehosta heidän on mahdollista väärinkäyttää lohkoketjua hyötyen siitä samalla itse taloudellisesti.

Peliteorian mukaan älylliset ja rationaaliset päätöksentekijät tekevät valintansa yrittäen maksimoida heidän saamansa hyödyn. Peliteorian suosituin kon-

septi on Nashin tasapaino, jonka mukaan pelaajat muuttavat strategiaansa niin kauan kun muutoksesta on mahdollista hyötyä. Kun vastapuolen toimet eivät enää vaikuta pelaajan omiin valintoihin, ollaan saavutettu Nashin tasapaino. Yksi peliteorian suosituimmista esimerkeistä on vangin dilemma, jossa kahden henkilön on päätettävä samanaikaisesti tekevätkö he yhteistyötä toisen henkilön kanssa vai pettävätkö he tämän. Henkilö ei voi tietää kannattavinta ratkaisua tietämättä mitä toinen toimija on valinnut.

Peliteorian avulla on mahdollista kuvata lohkoketjujen konsensukseen pyrkiminen, sekä todistaa mikä mahdollistaa lohkoketjujen toiminnan. Kuten monissa muissakin asioissa, myös lohkoketjussa toimijat ovat älyllisiä ja rationaalisia päätöksentekijöitä, jotka haluavat maksimoida saamansa hyödyn. Lohkoketjussa louhijoiden on kannattavinta toimia oikealla tavalla, sillä siitä palkitaan. Suurin osa louhijoista ajattelee tällä tavalla, mikä mahdollistaa lohkoketjun toiminnan. Kyseessä on siis itseään ruokkiva Nashin tasapaino. Yksittäisten toimijoiden muutokset eivät vaikuta louhijoiden valintoihin, sillä enemmistö louhijoista toimii rationaalisesti.

Peliteorian avulla voidaan myös todistaa mahdolliseksi lohkoketjun väärinkäyttäminen sen nykyisessä tilassa. Vangin dilemmaa apuna käyttäen pystytään todistamaan, että louhijoiden on kannattavampaa siirtyä pahaenteisen louhintayhtymän käyttöön, mikäli sen on mahdollista tarjota louhijoille parempaa voittoa. Nashin tasapaino yksittäiselle louhijalle löytyy myös pahaenteistä louhintayhtymää käyttäessä, sillä strategiaa vaihtamalla louhijan ei ole mahdollista parantaa lopputulemaansa. Uudet konsensusalgoritmit, erityisesti Proof-of-Stake, on toteutettu estämään tämän kaltainen toiminta.

Proof-of-Stake konsensualgoritmia käyttämällä hyökkäyksen yrittämisestä tulisi entistäkin kalliimpaa, sillä pahaenteinen toimija menettäisi panokseksi asettamansa varat. Proof-of-Work konsensusalgoritmia käyttävissä lohkoketjuissa pahaenteinen toiminta louhintayhtymiä hyväksi käyttämällä on helpompaa, sillä louhijat on mahdollista saada heidän tietämättään toimimaan pahaenteisen toimijan agendan mukaisesti. Vangin dilemman avulla todistettiin myös, että louhintaan vaadittujen resurssien sijaan pahaenteisen toimijan tarvitsee ainoastaan maksaa louhinnasta muita louhintayhtymiä enemmän.

Peliteorian ongelmana tutkittaessa niiden vaikutusta julkisten lohkoketjujen toimintaan on se, että peliteoriassa toimijoiden uskotaan olevan rationaalisia päätöksentekijöitä. Vaikka toimijat olisivat rationaalisia päätöksentekijöitä, voi heidän motiivinsa olla taloudellisen hyödyn sijaan esimerkiksi viha. Tällöin pahaenteisen toiminnan aikaansaama taloudellinen tappio ei estäisi suunnitelman toteuttamista.

Tutkielmassa pyrittiin vastaamaan siihen, miten peliteoria liittyy julkisiin lohkoketjuihin. Peliteoriaa hyväksi käyttämällä selvitettiin taloudellisen hyödyn toimivan motiivina lohkoketjujen toiminnallisuudelle, mikä mahdollistaa lohkoketjujen toiminnan. Nashin tasapainon avulla todistettiin, että lohkoketjun louhijoille kannattavin strategia on toimia oikein. Toimiessaan väärin louhija jäisi taloudellisesti tappiolle, mikä ei ole luonnollinen valinta rationaaliselle päätöksentekijälle. Peliteorian avulla selvitettiin myös, miten julkisia lohkoketjuja on mahdollista väärinkäyttää. Teknologian kehittyessä lohkoketjuteknologian on täytynyt mukautua, joka on johtanut kolmansien osapuolien ylläpitä-

mien louhintayhtymien muodostumiseen. Vaikka louhintayhtymät kasvattavat lohkoketjun ekosysteemiä, muodostavat ne silti suuren riskin lohkoketjun toiminnalle viemällä pohjan lohkoketjujen hajautuneisuudelta. Pahaenteiset toimijat voivat muodostaa uuden louhintayhtymän, jota käyttämällä väärinkäytöstä tietämättömät louhijat saavat muita louhintayhtymiä suuremman palkkion. Nashin tasapainon mukaisesti louhijat siirtyvät pahaenteisen louhintayhtymän käyttöön paremman lopputuleman perässä. Pahaenteisen louhintayhtymän saadessa käyttöönsä yli puolet lohkoketjun laskentatehosta on hänen mahdollista väärinkäyttää lohkoketjua.

Mielenkiintoisia jatkotutkimusaiheita löytyy uuden sukupolven konsensusalgoritmeista sekä niiden tutkimisesta peliteorian avulla. Tässä tutkielmassa jätettiin tutkimatta muita peliteorian esimerkkejä kandidaatin tutkielman laajuuden vuoksi. Toinen peliteorian esimerkki, jolla lohkoketjuteknologiaa voi tutkia on bysanttilaisten kenraalien ongelma. Lohkoketjuissa käytetään yleisesti esimerkkinä myös varmentajan dilemmaa, joka myös jätettiin käsittelemättä tässä kirjallisuuskatsauksessa. Lohkoketjuteknologiaan ja peliteoriaan liittyviä jatkotutkimusaiheita on yleisesti mahdollista löytää erittäin laajasti keskittyen niin teknologiasta yhteiskuntatieteelliseen näkökulmaan.

Peliteoria on yksi olennaisimmista asioista, jotka mahdollistavat julkisten lohkoketjujen toiminnan hajautetusti ilman luotettua kolmatta osapuolta. Yhdessä teknisten ratkaisujen kanssa se muodostaa pohjan hajautettujen ratkaisujen toiminnalle. Peliteoria ei kuitenkaan toimi ympäristössä, jossa toimijat eivät ole täysin rationaalisia ja maksimaalista hyötyä tavoittelevia entiteettejä, vaan perustavat toimintansa esimerkiksi tunnepohjaisiin ratkaisuihin.

LÄHTEET

Albrecht, S., Reichert, S., Schmid, J., Strüker, J., Neumann, D., & Fridgen, G. (2018). Dynamics of Blockchain Implementation - A Case Study from the Energy Sector. *Proceedings of the 51st Hawaii International Conference on System Sciences* (3527-3536).

Antonopoulos, A. M. (2015). Mastering bitcoin: Unlocking digital cryptocurrencies (1. ed.). Sebastopol, CA: O'Reilly Media, Inc.

Axelrod, R. (1980). Effective Choice in the Prisoner's Dilemma. Journal of Conflict Resolution, 24(1), 3–25.

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business and Information Systems Engineering*, 59(6), 381-384.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Technology: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 19(10), 1020-1034.

Bitcoin.org (2018). Bitcoin's website. Haettu osoitteesta https://bitcoin.org/

Blockchain.info. (2019). Bitcoin Mining Pools. Haettu osoitteesta https://blockchain.info/pools

Bonneau, J., Miller, A., Clark, J., Narayan, A., Kroll J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104-121.

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security*, 2013(11), 5-8.

Buchman, E. (2016). Tendermint: *Byzantine fault tolerance in the age of blockchains*. (Pro gradu –tutkielma). University of Guelph

Buterin, V. (2013). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. Haettu osoitteesta http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (28.1.2015). The P + epsilon Attack. Haettu osoitteesta https://blog.ethereum.org/2015/01/28/p-epsilon-attack/

Buterin, V., & Griffith, V. (2017). Casper the Friendly Finality Gadget. Haettu osoitteesta https://arxiv.org/abs/1710.09437

Camerer, C, F. (2003). Behavioral Game Theory: Experiments in Strategic Interactions. New York, US: Russell Sage Foundation.

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

CoinMarketCap. (2018). Cryptocurrency Market Capitalizations. Haettu osoitteesta https://coinmarketcap.com/

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: bitcoin mining is vulnerable. *Communications of the ACM*, 61(7), 95-105.

Gervais, A., Karame, G., Capkun, V., & Capkun, S. (2014). Is Bitcoin a Decentralized Currency? *IEEE Security & Privacy*, 12(3), 54-60.

Geyl, A. (10.5.2015). May 10th 2015 Network Statistics. Haettu osoitteesta http://organofcorti.blogspot.com/2015/05/may-10th-2015-network-statistics.html

github.com/bitcoin (2018). GitHub Bitcoin's repository. Haettu osoitteesta https://github.com/bitcoin

Heylighen, F. (1993). The Prisoners' Dilemma. *Principia Cybernetica Web*. Haettu osoitteesta http://pespmc1.vub.ac.be/PRISDIL.html

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.

Jackson, M, O. (2011). A Brief Introduction to the Basics of Game Theory. SSRN Electronic Journal. Haettu osoitteesta http://ssrn.com/abstract=1968579

Khomskii, Y. (2010). Infinite games. Technical report, University of Sofia Bulgaria, Summer Course.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Advances in Cryptology – CRYPTO 2017: 37th Annual International Cryptology Conference,* 10401, 357-388.

Krishnan, S., Balu, B. K., Smith, S., & Pang, V. (2015). The Development of Theoretical Framework for In-App Purchasing for the Gaming Industry. *Proceedings of the 2015 Pacific Asia Conference on Information Systems*.

Kruijff, J.D., & Weigand, H. (2017). Understanding the Blockchain Using Enterprise Ontology. *International Conference on Advanced Information Systems Engineering*, 29-43.

Kultti, K. (1994). Taloustieteen Nobel peliteorian kehittäjälle. *Kansantaloudellinen aikakauskirja*, 90(4), 520-524.

Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5), 653-659.

Lönnqvist, J-E., Verkasalo, M., & Walkowitz, G. (2011). It pays to pay – Big Five personality influences on co-operative behaviour in an incentivized and hypothetical prisoner's dilemma game. *Personality and Individual Differences*, 50(2), 300-304.

Myerson, R, B. (1978). Refinements of Nash Equilibrium Concept. *International Journal of Game Theory*, 7(2), 73-80.

Myerson, R, B. (1991). Game Theory: Analysis of Conflict. England: Harvard University Press

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Haettu osoitteesta https://bitcoin.org/bitcoin.pdf

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183-187.

Nian, L. P., & Chuen, D. L. K. (2015). Handbook of digital currency: Bitcoin, innovation, financial instruments and big data Chapter 1 Introduction to Bitcoin. Singapore: Elsevier Inc.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electronic Journal*.

O'Connell, J. (20.6.2016). What Are the Use Cases for Private Blockchains? The Experts Weigh In. Haettu osoitteesta https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/

Pearce, D, G. (1984). Rationalizable Strategic Behavior and the Problem of Perfection. *Econometrica*, 42(4), 1029-1050.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework. *IEEE Consumer Electronics Magazine*, 7(2), 18-21.

Riasanow, T., Setzke, D. S., Burckhardt, F., Böhm, M., & Kremar, H. (2018). The Generic Blockchain Ecosystem and its Strategic Implications. *24th Americas Conference on Information Systems* (AMCIS), At New Orleans, LA, USA.

Roberts, J. F. (29.5.2018). Bitcoin Spinoff Hacked in Rare '51 % Attack'. Haettu osoitteesta http://fortune.com/2018/05/29/bitcoin-gold-hack/

Salviotti, G., De Rossi, L. M., & Abbatemarco, N. (2018). A Structured Framework to Assess the Business Application Landscape of Blockchain Technologies. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 3467-3476.

Schrijvers, O., Bonneau, J., Boneh, D., & Roughgarden, T. (2017). Incentive Compatibility of Bitcoin Mining Pool Reward Functions. *Financial Cryptography and Data Security*, 9603, 477-498.

Schwalbe, U., & Walker, P. (2001). Zermelo and the early history of Game Theory. *Games and Economic Behavior*, 34(1), 123-127.

Selten, R. (1975). Reexamination of the Perfectness Concept for Equilibrium Points in Extensive Games. *International Journal of Game Theory*, 4(1), 25-55.

Swan, M. (2015). Blockchain: Blueprint for a New Economy, Sebastopol, CA: O'Reilly Media, Inc.

Swanson, T. (2015). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Haettu osoitteesta https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf

Taylor, M. B. (2013). Bitcoin and The Age of Bespoke Silicon. *2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*, 1-10.

Tsabary, I., & Eyal, I. (2018). The Gap Game. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (713-728).

Würst, K., & Gervais, A. (2017). Do you need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45-54.

Zhao, J.L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2(28).

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557-564.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352-375.

Ziolkowski, R., Miscione, G., & Schwabe, G. (2018). Consensus through Blockchains: Exploring Governance across interorganizational Settings. *International Conference of Information Systems (ICIS)*.