HAMK
Hämeen ammatti-
korkeakoulu

LOHKOKETJUTEKNOLOGIAN HYÖDYT JA HAITAT VIDEOPELEISSÄ

Ammattikorkeakoulututkinto opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK)

Syksy, 2023

Waltter Skogberg

HAMK
Hämeen ammatti-
korkeakoulu

Tieto- ja viestintätekniikka, insinööri (AMK) Tiivistelmä
Tekijä Waltter Skogberg Vuosi 2023
Työn nimi Lohkoketjuteknologian hyödyt ja haitat videopeleissä
Ohjaaja Mika Virolainen

Tämän opinnäytetyön tarkoituksena oli koota kirjallisuuskatsaus, joka käsittelee lohkoketjuteknologian eri toimintoja ja miten näiden toimintojen avulla voidaan parantaa pääosin videopelejen yleisiä ongelmia, sekä tuoda niihin uusia hyödyllisiä ominaisuuksia.

Työssä tullaan tarkastelemaan erityisesti lohkoketjuteknologian eri osa-alueita, kuten lohkoketjuteknologian yleistoiminta, lohkoketjuteknologiaan siältyviä eri teknologioita ja miten kyseisten teknologioiden avulla voidaan vastata erinäisiin moderneihin ongelmiin erityisesti videopeleissä.

Opinnäytetyöhön lähteinä käytetty kirjallinen aineisto koostuu hyvin suurelta osin Google Scholar kirjastosta etsityistä tutkimuksellisista kirjoituksista. Lähteitä etsiessä aineisto pyrittiin pitämään mahdollisimman modernina, jotta se olisi ajankohtainen ja vastaisi mahdollisimman hyvin lukijan kysymyksiin.

Kyseisellä opinnäytetyöllä ei ollut ketään ulkoista tilaajaa tai toimeksiantajaa, eikä sitä ole tehty yhteistyössä kenenkään kanssa, joten työ on käytännössä vain kirjoittajalle itselleen toteuttama.

Opinnäytetyö on jaettu kahteen pääteemaan. Ensimmäisessä kerrotaan mahdollisimman tarkasti lukijalle miten lohkoketjuteknologia toimii yleisesti ja tästä edetään opinnäytetyön toiseen vaiheeseen, jossa käydään läpi lohkoketjuteknologian toimintaa videopeleissä ja miten lohkoketjuteknologia pystyy parantamaan niitä.

Lopulta opinnäytetyössä voitiin todeta että lohkoketjuteknologialla voi olla monia hyvinkin suuria parantavia vaikutuksia videopeleissä, mutta myös joitakin tämänhetkisiä rajoituksia. Kuitenkin on hyvin todennäköistä että ajan kuluessa tässä opinnäytetyössä keskustellut rajoitukset ovat jo monilta osin ratkaistu.

Avainsanat Lohkoketjut, videopelit, NFT
Sivut 35 sivua ja liitteitä 0 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Information and Communication Technology — Abstract
Author Waltter Skogberg — Year 2023
Subject Blockchain technology benefits and restrictions in video games
Supervisor Mika Virolainen

In this thesis the main goal was to create a literature review about blockchain technology and its different features, how those features can solve known issues mainly in video games and even bring some new beneficial features to them.

This literature review especially focuses on different key parts of the blockchain technology, including how blockchain technology mainly works, what different technologies are part of it and how using these technologies different problems in video games can be answered.

The literature of this thesis consists of mainly of academic articles found in the Google Scholar library. When searching for the literature the goal was to make sure that the literature found and used in this thesis is as current and relevant as possible and answers the reader's questions in the best possible way.

The chapters in this thesis are separated into two main themes. The first theme aims to give the reader a very precise understanding about how blockchain technology works overall. The second chapter discusses how blockchain technology works and can be used to solve issues and improve video games.

This thesis was made mainly for the writer himself, without any external co-operations with customers or employers.

Lastly in conclusion of this thesis we could acknowledge that blockchain technology can have great beneficial factors for video games, but that it may currently have some restrictions. However it is very likely that in time the restrictions mentioned in this thesis will mostly be solved.

Keywords Blockchains, video games, NFT
Pages 35 pages and appendices 0 pages

Sisällys

Kuvat, taulukot ja kaavat

1 Johdanto

Lohkoketjuteknologia on monin osin mullistava teknologia, sillä se voi mahdollistaa avoimuutta, turvallisuutta ja itsenäisyyttä monissa asioissa, kuten vaikka rahan siirtämisessä tai tallettamisessa. Tässä opinnäytetyössä tarkastellaan lohkoketjun eri toimintoja yleisesti, kuten älysopimuksia, eri lohkoketjukategorioita, eri lohkoketjun yksimielisyysmalleja ja epäsymmetristä avain kryptografiaa, sekä miten kyseiset toiminnot voivat olla hyödyllisiä erityisesti videopelien toimialalla.

Maailmassa eletään aikaa, jossa tietomurrot ja kyberhyökkäykset eivät ole todellakaan mahdottomuuksia ja tappiot niiden tapahtumisesta ovat niiden uhreille suuret niin rahallisesti, kuin myös luottamuksellisesti. Tämän vuoksi lohkoketjuteknologian hyödyntäminen muissa teknologioissa aiheena on hyvinkin ajankohtainen, sillä sen avulla voidaan tuoda turvaa ja luottamusta kyseisiä ongelmia kohtaan esimerkiksi juuri hajautetun rakenteensa vuoksi.

Lohkoketjuteknologia yleisesti mahdollistaa esimerkiksi tilisiirtojen tallentamisen jokaisen tapahtumaketjun välisen muutoksen jälkeen ja näitä muutoksia on käytännössä mahdoton väärentää tai muuttaa ulkopuolisten tahojen toimesta. Se mahdollistaa myös vaihtoehdon missä ei tarvita kolmansia osapuolia, kuten rahan vaihtamisessa pankkeja, jotta rahansiirto saadaan turvallisesti ja varmennetusti tehtyä.

Lohkoketjuteknologian yleistiedon lisäksi opinnäytetyössä pääosin käydään läpi, miten kyseisiä lohkoketjuteknologian toimintoja voidaan soveltaa myös videopelejen toiminnassa. Esimerkiksi videopelien välisten vaihtojen varmentamisessa ja tallentamisessa, sekä miten lohkoketjuteknologian avulla voidaan parantaa monia tiedettyjä heikkouksia videopeleissä, kuten pelien sisäiset huijaukset, pelien ylläpitäjiin kohdistuvia hyökkäyksiä ja pelien laittomien lataamisten torjumista.

Opinnäytetyössä tullaan myös puhumaan lohkoketjun tuomista hyödyistä videopeleissä, kuten eri pelien välisten esineiden vaihtojen tekemisen mahdollisuus, sekä miten pelaajat pystyvät lohkoketjuteknologian avulla vaikuttamaan lohkoketjuvideopelien tulevaisuuteen.

Tässä opinnäytetyössä ei käydä läpi metaversumejen toimintaa vaikka nekin ovat yksi osa web3.0 ja lohkoketjupelien kokonaisuutta, sillä työn aihepiiri on pyritty rajaamaan enemmän kyberturvallisuuteen ja luottamukseen.

Lopputuloksena opinnäytetyön lukemisen jälkeen tarkoituksena on että lukija saa hyvän perustiedon ja käsityksen lohkoketjuteknologiaan kuuluvista eri teknologioista, sekä toiminnoista. Näihin mukaan lukeutuen, miten lohkoketjuteknologia toimii pääosin, mikä sen toimintaketju on, mitä eri osia siihen kuuluu ja miten lohkoketjuteknologian avulla voidaan parantaa videopelejen suojausta, luottamusta ja toimintaa.

2 Lohkoketjuteknologia

Lohkoketju on jaettu digitaalinen tilikirja, jossa sen käyttäjät voivat toteuttaa esimerkiksi tilisiirtoja toistensa kanssa kaikille jaetussa yhteisessä tilikirjassa. Lohkoketju on myös hajautettu, mikä tarkoittaa ettei sitä hallitse mikään keskeinen yritys tai taho. (Yaga ym., 2018, s. 1) Tämän vuoksi lohkoketjulla on mahdollisuus mullistaa verkossa käytävä kanssakäyminen antamalla mahdollisuus varmentaa tämänhetkisiä ja tulevia digitaalisten varojen siirtoja milloin tahansa (Crosby, 2016, s. 8).

Lohkoketjua ylläpidetään sen käyttäjien toimesta ja käyttäjiä lohkoketjuverkossa kutsutaan nimellä ”solmu”. Nämä kyseiset solmut ovat yhteydessä toisiinsa P2P (Peer-to-Peer) yhteydellä. Hajautetun rakenteen ansiosta, kuten myös sen että lohkoketjusta on jaettu kopio jokaiselle käyttäjälle lisää lohkoketjun suojaa, sillä näiden kahden ominaisuuden ansiosta lohkoketjussa ei ole yhtä heikkoa kohtaa mihin vaikka hyökkääjä voisi kohdistaa kyberiskun. (Liang, 2020, s. 122) Lohkoketjussa tapahtumien manipulointi on sen hajautetun rakenteen vuoksi vaikeaa, sillä kun esimerkiksi tilisiirto on tehty ja lohko on varmennettu käyttäjien toimesta, sitä ei voi enää peruuttaa tai muuttaa vaikuttamatta koko ketjuun (Yaga ym., 2018, s. 1).

Lohkoketjussa tapahtumat voivat olla muutakin kun pelkästään rahansiirtoja, mutta yleisin vaihdettava esine on yleensä kryptovaluutta. Lohkoketju ei suinkaan ole pelkästään tilikirja, vaan sen avulla voidaan myös suorittaa erilaisten älysopimusten käyttöä, kyseiset älysopimukset kykenevät autonomisesti suorittamaan ehtoja mitä sopimuksiin on kirjattu. (Liang, 2020, s. 121) Lohkoketju voidaan jakaa kuuteen pääosaan, näitä ovat:

1. Hajautettu rakenne, takoittaa ettei lohkoketjussa ole tarvetta keskeisille valvojille esimerkiksi käyttäjien välisien siirtojen tekemisessä ja data voidaan tallentaa yhden keskeisen solmun sijaan monelle solmulle. Lisäten turvaa ja luotettavuutta.
2. Läpinäkyvyys, lohkoketjussa tarkoittaa että data on näkyvissä solmuille ja lisäksi solmut pystyvät vielä itsenäisesti päivittämään dataa.

3. Avoin lähdekoodi, lohkoketju on avoin kaikille uusille käyttäjille ja jokainen voi tehdä siirtoja, sekä tarkistaa niitä julkisesti. Lisäksi kaikki käyttäjät voivat käyttää lohkoketjua uusien applikaatioiden luomiseen.
4. Autonomia, jokainen solmu lohkoketjussa voi siirtää ja päivittää dataa turvallisesti ilman suurempia keskeytyksiä.
5. Muuttamattomuus, lohkoketjussa siirtojen julkistuksen jälkeen niitä ei voi muuttaa ilman ainakin 51% enemmistöä ja ne säilyvät lohkoketjussa ikuisesti.
6. Anonymiteetti, lohkoketjuverkossa ei tarvita luottamusta solmujen välillä tämä antaa mahdollisuuden anonyymisille siirroille käyttäjien välillä ja niihin tarvitaan vain vastaanottavan käyttäjän lohkoketjuosoite. (Niranjanamurthy ym., 2019, ss. 1–2)

2.1 Lohkoketjuteknologian historia

Lohkoketju saavutti suuremman tietoisuuden Bitcoinin kautta vuonna 2008 (Liang, 2020, s. 121), mutta todellisuudessa lohkoketjuteknologian eri osia on tavattu monen eri tahon toimesta jo ennen vuosituhannen vaihdetta. Esimerkiksi tietojen säilytyksestä voidaan tavata merkkejä jo, jopa muinaisen Mesopotamian aikana. Myös merkkejä muuttumattomasta tietolohkojen ketjuttamisesta voidaan löytää Ralph Merklen tutkielmasta vuodelta 1979, jossa hän esittelee Merkle puun. (Sherman ym., 2019, s. 2)

Puolestaan David Chaum esitteli säilöjärjestelmän, joka sisälsi suurimman osan lohkoketjun sisältämistä toiminnoista, kuten hajautettu rakenne ja mahdollisuus ylläpitoon käyttäjien puolesta, jotka eivät välttämättä tunne toisiaan. Lisäksi säilöjärjestelmä sisälsi tuttuja kryptaus primitiivejä, kuten symmetrisen ja epä symmetrisen avain kryptografian, sekä myös kryptograafisen hash funktion ja digitaalisen kirjoituksen. (Sherman ym., 2019, s. 2)

Myös teknologiasta, joka mahdollistaa tuntemattomien käyttäjien luottamuksen toisiinsa voidaan tavata merkkejä vuonna 1989 julkaistussa Leslie Lamportin Paxos protokollassa. Vuonna 2008 pseudonyymi nimeltään Satoshi Nakamoto yhdisti monia näistä teknologioista ja loi niistä lohkoketjuteknologian, sekä ensimmäisen kryptovaluutan Bitcoinin. (Yaga ym., 2018, s. 2)

2.2 Lohkoketjun älysopimukset

Älysopimukset ovat ohjelmia, joita käytetään yleensä kahden tai useamman henkilön keskeisen tapahtuman suorittamiseen. Älysopimuksiin voidaan asettaa tiettyjä ehtoja, sekä sääntöjä ja joiden toimintahistoriaa voidaan seurata helposti. (Mohanta ym., 2018, s. 2)

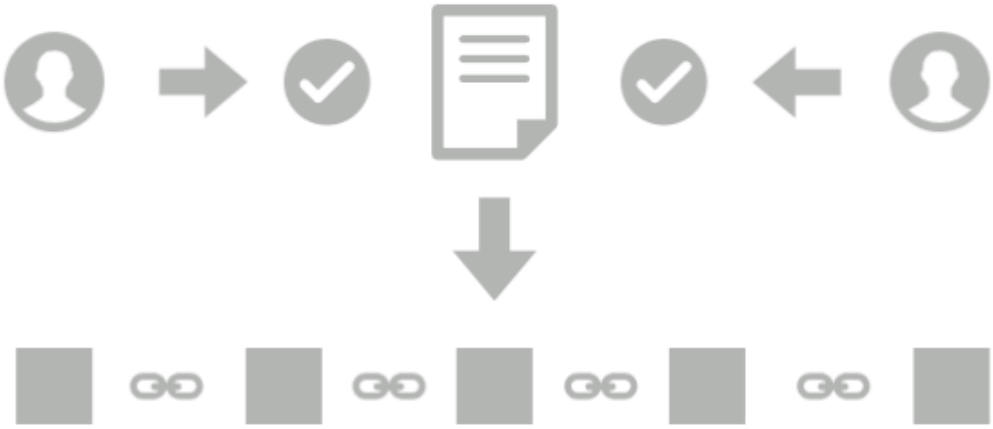
Älysopimukset pystyvät suorittamaan niihin asetetut säännöt itsenäisesti sääntöjen ehtojen täytyttyä. Täten vähentäen tarvetta kolmansien osapuolien tarpeelle. (Mohanta ym., 2018, ss. 2–3) Älysopimuksen rakenne koostuu maksutaseesta, varastosta ja suoritettavasta koodista. Älysopimus päivittää tilaansa, joka perustuu maksutaseen ja varaston toimintaan aina kun käyttäjät kutsuvat sitä lohkoketjussa. (Alharby & Moorsel, 2017, s. 127)

Jokaiselle älysompimukselle niiden luontivaiheessa asetetaan uniikki osoite, joka on noin 20 bittiä pitkä. Kun älysopimus on luotu sen ehtoja, jotka on merkattu koodiin ei voi enää muuttaa. Käyttäjät voivat kutsua älysopimusta lähettämällä siirron sen osoitteeseen, jonka jälkeen tämä siirto varmennetaan solmujen puolesta lohkoketjussa. (Alharby & Moorsel, 2017, s. 128)

Älysopimukset käyttävät Solidity nimistä ohjelmointikieltä toiminnassaan esimerkiksi Ethereum, Zeppelin, erisDB ja Counterparty nimisissä lohkoketjuissa. Esimerkkinä älysopimuksen toimintaa voidaan verrata ohjelmoinnissa funktion toimintaan. Älysopimuksessa ja ohjelmointi funktiossa kumpaankin syötetään jokin syöte, jonka funktio tai älysopimus suorittaa ja antaa ulostulon (Kuva 1). (Mohanta ym., 2018, ss. 2–3)

Idea älysopimuksista syntyi jo vuonna 1994, mutta kunnolla toiminnassa ne tavattiin vasta lohkoketjuteknologian yhteydessä. Älysopimuksia tavataan yleensä lohkoketjualustoilla, kuten Ethereum, mutta sen lisäksi älysopimuksia voidaan käyttää myös esimerkiksi Bitcoin lohkoketjussa. Kuitenkin Bitcoinin alustan ohjelmointikielen rajoitteisuuden, kuten silmukoiden ja nostorajoituksien puutteen vuoksi sen päälle ei voida luoda mitään kovin monimutkaista logiikkaa suorittavaa älysopimusta. (Alharby & Moorsel, 2017, s. 128)

Kuva 1. Älysopumuksien toiminta (soveltaen Zhang & Liu, 2022, s. 3).



Kuvassa kaksi henkilöä suorittavat sopimuksen mukaiset ehdot ja älysopimus suorittaa vaihdon tapahtuman lohkoketjuun.

2.3 Lohkoketjun hyötyjä ja haittoja

Lohkoketjuteknologia tarjoaa monenlaisia hyötyjä, kuten 100% läpinäkyvyyden tapahtumaketjussa. Lohkoketjun kautta tehdyt tapahtumat myös tallennetaan ja niitä voidaan helposti seurata käyttäjien toimesta. Hajautetun rakenteensa ansiosta, lohkoketjussa ei ole yhtä heikkoa kohtaa, johon esimerkiksi hyökkääjä voisi kohdistaa kyberiskun ja kaataa mahdollisesti koko systeemin toiminnan. Lohkoketjussa ei ole myöskään tarvetta kolmansille osapuolille, sillä lohkoketju toimii käyttäjien välisellä P2P (Peer-to-Peer) tekniikalla. Tämän lisäksi mukaan lukien siirtojen varmennus käyttäjien toimesta mahdollistaa sen ettei lohkoketjussa tarvita välikäsiä siirtojenkaan varmentamiseen. (Niranjanamurthy ym., 2019, ss. 8–13)

Lohkoketjuteknologia mahdollistaa luottamuksen tuntemattomiinkin tahoihin ja yksimeilisyysmallien avulla, jopa täysin tuntemattomatkin tahot voivat tehdä luotettavasti siirtoja keskenään ilman tarvetta käyttäjien väliselle suuremmalle luottamukselle. Lohkoketjuteknologia tarjoaa myös tehokkaan yksityisyyden turvan, sillä lohkoketjussa kuka tahansa voi osallistua tekemään siirtoja anonyymisti ilman tarvetta omien tietojensa luovuttamiselle. (Niranjanamurthy ym., 2019, ss. 8–13)

Kuitenkin lohkoketjussa esiintyy myös joitakin heikkouksia, kuten suuri energiankulutus proof-of-work lohkoketjuissa. Proof-of-work lohkoketjuverkkojen louhijasolmut esimerkiksi Bitcoinissa työstävät noin 450 tuhatta triljoonaa ratkaisua sekunnissa käyttäjien tekemiä siirtoja varten. Suuren energiankulutuksen lisäksi kyseisissä lohkoketjuissa on sen toimintatavan vuoksi hitaampi prosessointinopeus verrattuna esimerkiksi keskitettyihin järjestelmiin, kuten tavanomaiset pankkijärjestelmät. Suurin syy tähän on ylimääräiset vaiheet, kuten siirtojen varmentaminen ja yksimielisyyden saavuttaminen. (Niranjanamurthy ym., 2019, ss. 8–13)

Turvallisuus, vaikka lohkoketjuverkoissa on luotu ratkaisuja, kuten vahva enkryptaus ja yksityislohkoketjut, on kyseisellä teknologialla silti monia ratkaistavia ongelmia ennen kuin siihen uskalletaan täysin luottaa. Esimerkiksi epävarmuus säännöstelyssä, koska lohkoketjulla ja kryptovaluutoilla ei ole tavanomaisen rahan lailla mitään valtiota takaamassa sitä on yritysten vaikea luottaa siihen ja ottaa se käyttöönsä. (Niranjanamurthy ym., 2019, ss. 8–13)

3 Lohkoketjukategoriat

Lohkoketjuverkoista on muutamia erilaisia malleja olemassa. Ne voidaan tunnistaa helposti tavasta millä niitä ylläpidetään. Esimerkiksi jos lohkoketjuverkossa kuka vaan solmu voi julkaista uusia lohkoja on kyseessä useimmiten permissionless eli julkinen lohkoketju. Jos taas vain tietyt solmut voivat tehdä lohkojen julkistuksen on kyseessä usein permissioned eli yksityinen lohkoketju. (Yaga ym., 2018, s. 5)

3.1 Permissionless lohkoketju

Permissionless tai julkinen lohkoketju on lohkoketju missä ei ole keskeistä hallintoa, kuten vaikkapa jokin tietty yritys. Permissionless lohkoketjut ovat yleensä avoimen lähdekoodin ohjelmia minkä kuka tahansa voi ladata ja tätä kautta osallistua sen käyttöön. Niissä voi myös kuka tahansa julkaista ja lukea lohkoja ilman erityislupien kysymistä (Kuva 2). Kuitenkin tämä vapaus lisää riskejä, koska kuka tahansa voi liittyä verkkoon, lukea ja julkaista lohkoja tämä lisää mahdollisuuksia ei niin ystävällisille käyttäjille. Tämän ongelman julkiset lohkoketjut kuitenkin pyrkivät ratkaisemaan käyttämällä yksimielisyysmalleja, jotka vaativat käyttäjiltä jonkin verran resursseja kun he haluavat julkaista lohkoja, mutta myös palkitsevat käyttäjiä jos he varmistavat onnistuneesti lohkon. Kyseisiä yksimielisyysmalleja on monenlaisia, kuten proof-of-work ja proof-of-stake. (Yaga ym., 2018, s. 5) Permissionless

lohkoketjuja ovat esimerkiksi Bitcoin ja Ethereum lohkoketjut (Niranjanamurthy ym., 2019, s. 10).

Julkisen eli permissionless lohkoketjun hyödyt ja haitat:

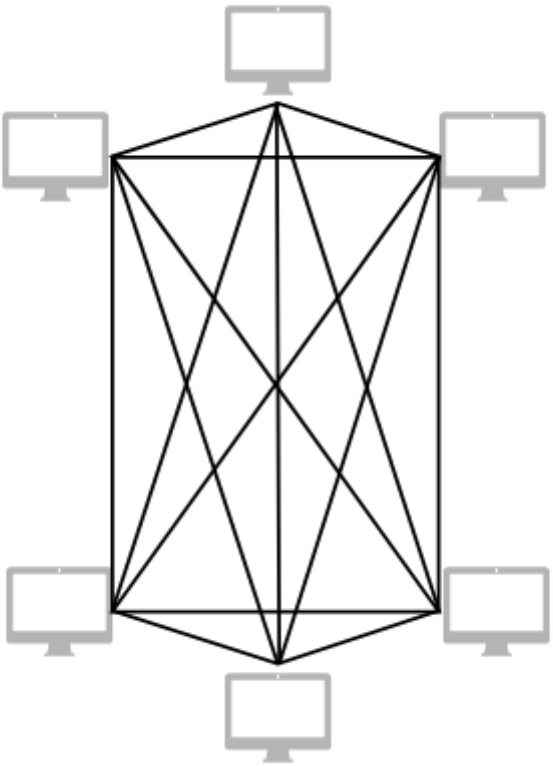
- Avoimuus, jokaisella käyttäjällä eli solmulla on sama oikeus tehdä ja varmentaa siirtoja toisten solmujen kanssa ilman rajoituksia

- Luotettavuus, jokainen solmu voi luottaa toiseen solmuun ilman aikaisempaa kanssakäymistä

- Laajenemisongelmat, koska julkiset lohkoketjut sallivat kenen tahansa osallistumisen tarvitsee se yksimeilisyysmallin turvallisuuden säilyttämiseksi

- Hitaus, koska julkiset lohkoketjut käyttävät toimintaansa yksimielisyysmalleja toimivat ne hitaammin permissioned eli yksityisiin lohkoketjuihin verrattuna (Solat ym., 2020, ss. 96–97)

Kuva 2. Permissionless lohkoketju (soveltaen BitYoga team, 2020).



Kuvassa nähdään että solmut voivat vapaasti toimia toistensa kanssa varmentaen ja tehden siirtoja.

3.2 Permissioned lohkoketju

Permissioned tai yksityinen lohkoketju on jonkin tahon hallittu lohkoketju, sitä voidaan käyttää esimerkiksi yrityksissä. Kyseisessä lohkoketjumallissa esimerkiksi yritys voi laatia kuka saa julkaista lohkoketjuun ja kuka voi lähettää siirtoja (Kuva 3). Yksityiset lohkoketjut yleensä toimivat nopeammin julkisiin tai permissionless lohkoketjuihin verrattuna, sillä ne eivät tarvitse proof-of-workin tai proof-of-staken tapaisia yksimielisyysmalleja toimintaansa (Sherman ym., 2019, s. 2). Syy tähän on se että lohkoketjussa hallinnoivat solmut yleensä tuntevat toisensa, jonka vuoksi ongelmat voidaan selvittää helposti lohkoketjun sisällä. Esimerkiksi poistamalla väärin käyttäytyvältä solmulta oikeudet julkaista lohkoja. (Yaga ym., 2018, ss. 5–6) Permissioned lohkoketjualustoja ovat esimerkiksi Quorum ja Parity lohkoketjut.

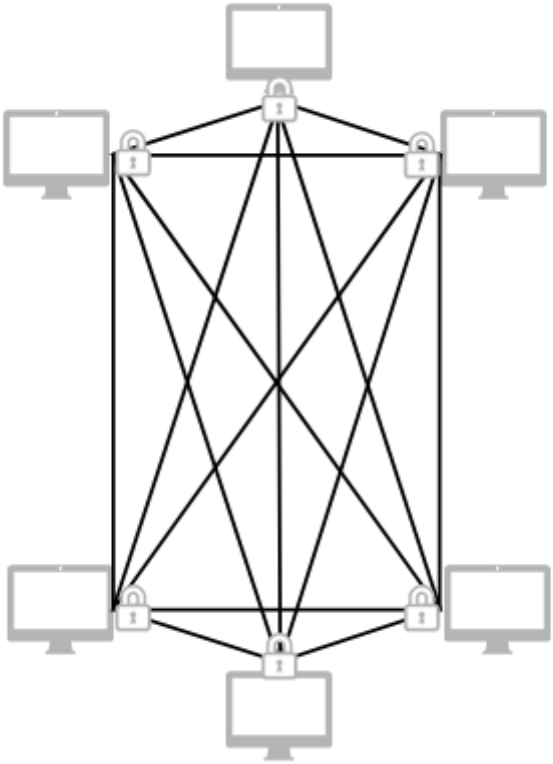
Yksityisen eli permissioned lohkoketjun hyötyjä ja haittoja:

- Nopeus, koska yksityiset eli permissioned lohkoketjut ovat yleensä jonkin tahon hallinnassa eivät ne tarvitse yksimielisyysmalleja turvallisuutensa ylläpitoon

- Ei laajentumisongelmia, yksimielisyysmallejen puuttumisen vuoksi myös lohkoketjun laajentaminen on helpompaa, sillä kaikkien lohkoketjun solmujen hyväksymistä ei vaadita

- Kaikki käyttäjät eivät ole saman arvoisia, koska yksityisissä lohkoketjuissa on jokin hallintataho eivät kaikilla sen käyttäjillä ole samoja oikeuksia, kuten siirtojen tekeminen tai varmentaminen (Solat ym., 2020, ss. 96–97)

Kuva 3. Permissioned lohkoketju (soveltaen BitYoga team, 2020).



Kuvassa nähdään että esimerkiksi yritys, joka hallitsee lohkoketjua voi päättää mitkä solmut saavat varmentaa ja tehdä siirtoja.

3.3 Consortium lohkoketju

Consortium lohkoketju on julkisen ja yksityisen lohkoketjun sekoitus, jossa hallinnoiva solmu voi valita onko data lohkoketjussa avointa vai rajoitettua. Consortium lohkoketjussa yleensä valitaan tietyt hallintosolmut, jotka suorittavat käyttäjien tekemät varmennukset. Consortium lohkoketjuja ovat R3CEV ja Hyperledger. (Niranjanamurthy ym., 2019, s. 10)

4 Lohkoketjun yksimielisyysmallit

Lohkoketjussa yksi tärkeimmistä asioista on kuka saa julkaista uuden lohkon, tätä toimenpidettä hallitaan yksimielisyysmallejen avulla. Yksimielisyysmalleja on monia erilaisia ja niiden avulla pyritään parantamaan lohkoketjun toimintaa. Näitä yksimielisyysmalleja

käytetään pääosin julkisissa lohkoketjuissa, joissa jokainen käyttäjä saa osallistua lohkon julkaisuun. (Yaga ym., 2018, s. 18)

Julkisissa lohkoketjuissa käyttäjät epäsuorasti kilpailevat toisiansa vastaan, kuka saa julkaista uuden lohkon, joten tarvitaan yksimielisyysmalleja. Yksimielisyysmallejen avulla pyritään saamaan täysin tuntemattomat käyttäjät toimimaan yhdessä, jotta voidaan välttyä ongelmilta, kuten kahden lohkon samanaikainen valmistuminen ja miksi käyttäjät jakaisivat muiden varmistamia lohkoja eteenpäin. Yksi suurimmista motivaattoreista miksi käyttäjät osallistuvat lohkon julkaisuun on mahdollinen voitettava kryptovaluutta tai siirtomaksu. (Yaga ym., 2018, s. 18)

Vaikka käyttäjät eivät välttämättä edes tiedä toisistaan muuta kun toistensa julkisen avaimen osoitteen. He ovat mahdollisen palkinnon ansiosta silti motivoituneita osallistumaan uusien lohkojen julkaisuun. Ensimmäiseksi kun käyttäjä liittyy lohkoketjuverkkoon hän saa vastaanottaa kopion lohkoketjusta ja hyväksyy siihen kuuluvat säännöt, jotka on merkattu genesis lohkoon. Genesis lohko on lohkoketjun ensimmäinen ja ainoa lohko, joka on valmiiksi varmennettu. Jokainen sen jälkeen varmistettu lohko kiinnittyy sen jatkoksi, kun se on varmennettu kyseisen lohkoketjun käyttämällä yksimeilisyysmallilla. (Yaga ym., 2018, s. 18)

4.1 Bysantin kenraalin ongelma

Bysantin kenraalin ongelmalla takoitetaan ongelmaa hajautetussa järjestelmässä. Kyseinen termi ”Bysantin kenraalin ongelma” saa nimensä kuvituksellisesta tilanteesta, missä useammat Bysanttilaiset armeijat piirittävät linnoitusta odottaen viimeistä varmistusta muilta kenraaleilta ennen hyökkäystä. Kuitenkin heidän ongelmanaan on epäilys siitä että yhden tai useamman armeijan kenraali voi olla petturi ja antaa tahalleen väärän käskyn. Täten vesittäen koko hyökkäyksen, sillä jos kaikki armeijat eivät hyökkää samanaikaisesti he tulevat epäonnistumaan ja suurin osa kuolemaan. (Mingxiao ym., 2017, s. 2567)

Kyseinen ongelma voidaan tavata myös lohkoketjussa. Esimerkiksi lohkoketjussa data, joka kulkee solmujen läpi saattaa olla väärää jos solmu, jonka läpi se tuli on esimerkiksi, joko hyökkäyksen kohteena tai sillä on ei niin ystävällisiä suunnitelmia. (Mingxiao ym., 2017, s. 2567)

4.2 Proof-of-work

Proof-of-Work yksimeilisyysmallissa käyttäjät voivat julkaista lohkon sen jälkeen, kun he ovat ensin ratkaisseet laskelmallisesti raskaan testin (Kuva 4). Testi on suunniteltu niin että se on raskas suorittaa, mutta helppo tarkistaa. (Yaga ym., 2018, s. 19)

Testistä saatu tulos toimii todisteena että kyseinen testin suorittanut käyttäjä on ratkaissut sen. Koska testi on tehty helposti tarkistettavaksi voivat täyssolmut helposti vastaanottaa monia lohkoehdokkaita ja hylätä ne joiden vastaukset eivät kelvanneet. (Yaga ym., 2018, s. 19)

Yksi yleinen testi on vaatia käyttäjiä selvittämään että lohkon tunnisteen hash jäänne on pienempi kuin kohdesumma. Tätä kyseistä tulosta voidaan säätää, joko pienemmäksi tai suuremmaksi täten muuttaen sen vaikeustasoa. Tehtävän ratkaisemiseksi, julkaisevat solmut yleensä tekevät pieniä muutoksia heidän lohkonsa tunnisteeseen esimerkiksi muuttamalla noncea. Tällä vaikeusasteen muuttamisella pyritään saamaan aikaan ettei yksi taho voi hallita yksin lohkojen julkaisemista. (Yaga ym., 2018, s. 19)

Bitcoinin proof-of-workissa esimerkiksi testin vaikeustasoa muutetaan siten että lohkon julkaisumäärä pysyisi noin yhdessä lohkossa kymmenessä minuutissa. Tähän päästäkseen lohkojen julkaisun vaikeustasoa muutetaan Bitcoinissa noin joka 2016 lohko. Jokaista yritystä varten on käyttäjän laskettava uusi tunniste heidän lohkolleen, kyseinen toimenpide on laskelmallisesti raskas. Prosessin raskauden takia joissakin proof-of-workia käyttävissä lohkoketjuverkoissa julkaisevia solmuja on asetettu paikkoihin, jossa sähkö on halpaa. Proof-of-workissa suoritetusta työstä solmuja palkitaan jollakin summalla esimerkiksi kyseistä kryptovaluuttaa. (Yaga ym., 2018, ss. 18–19)

Kuva 4. Proof-of-Work toiminta (soveltaen Benhaddou, 2019).

Kuvassa solmut suorittavat monimutkaisia laskutoimituksia. Nopein solmu, joka ratkaisee testin saa julkaista lohkon ja muiden solmujen testit hylätään.

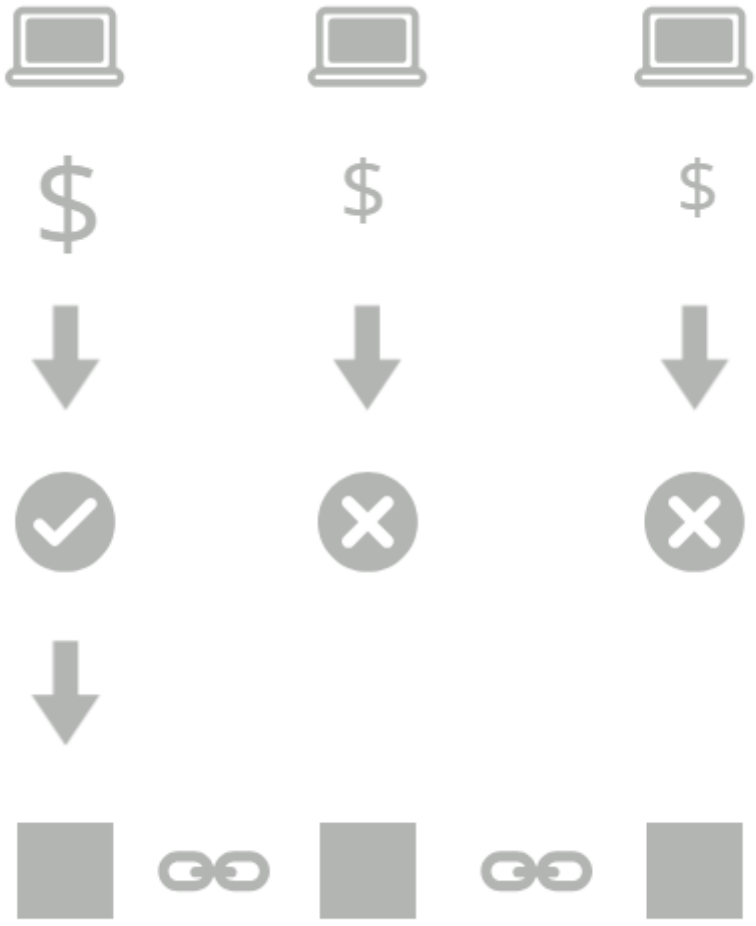
4.3 Proof-of-stake

Proof-of-stake yksimielisyysmallissa laskelmallisesti raskaiden testien ratkaisemisen sijaan käyttäjät asettavat panoksen eli investoivat kryptovaluuttaansa järjestelmään (Kuva 5). Tällä uskotaan että mitä enemmän käyttäjä on valmis investoimaan rahaansa, sitä suuremmalla syyllä hän haluaa lohkoketjun onnistuvan. Rahaa voidaan asettaa panokseksi monella tavalla, kuten lähettämällä se tiettyyn osoitteeseen, säilyttämällä sitä tietyllä lompakkosovelluksella tai lukitsemalla se tietynlaisella siirtotyypillä. (Yaga ym., 2018, ss. 21–22)

Proof-of-stake systeemi käyttää paljon vähemmän resursseja, kuten sähköä ja prosessointitehoa toimiakseen, kuin esimerkiksi proof-of-work systeemi. Tästä syystä johtuen, kuten myös siitä että proof-of-stakea käyttävissä lohkoketjuverkoissa oleva kryptovaluutta on yleensä valmiiksi jaettu käyttäjillensä, jotkin proof-of-stake lohkoketjuista ovat päättäneet vaihtaa käyttäjälle maksetun palkkion tuoreesti luodusta kryptovaluutasta käyttäjien maksamaan siirtomaksuun. (Yaga ym., 2018, ss. 21–22)

Proof-of-stake systeemissä on muutama eri tapa miten systeemi käyttää käyttäjien panoksia, kuten satunnaisvalinta, monikierros, rahan ikä ja delegaatti-systeemi. Yksi seikka kuitenkin on sama proof-of-stakessa riippumatta panoksen käyttötavasta. Se kellä on eniten rahaa investoituna tulee todennäköisemmin valituksi uuden lohkon julkaisijaksi. (Yaga ym., 2018, ss. 21–22)

Kuva 5. Proof-of-Stake toiminta (soveltaen Benhaddou, 2019).



Kuvassa solmut osallistuvat varmentamisprosessiin asettamalla tietyn panoksen. Lopputuloksena yleensä suurimman panoksen omaava solmu voittaa ja saa varmentaa lohkon.

5 Lohkoketjun toiminta

Lohkoketjussa käyttäjät tekevät tilisiirtoja toistensa kanssa, josta ne varmennetaan solmujen puolesta ja liitetään jatkoksi lohkoketjua. Näitä kyseisiä tilisiirtoja voidaan tehdä monenlaisilla eri sovelluksilla, verkkopalveluista digitaalisiin lompakkoihin tai älypuheliminsovelluksista tietokonesovelluksiin (Kuva 6). Kyseinen sovellus välittää siirron jollekkin solmulle lohkoketjussa. Kyseinen solmu voi olla kumpi tahansa, täyssolmu eli solmu, joka pitää lohkoketjun koko historiaa kirjalla tai ei julkaiseva täyssolmu. Kummassakin tapauksessa

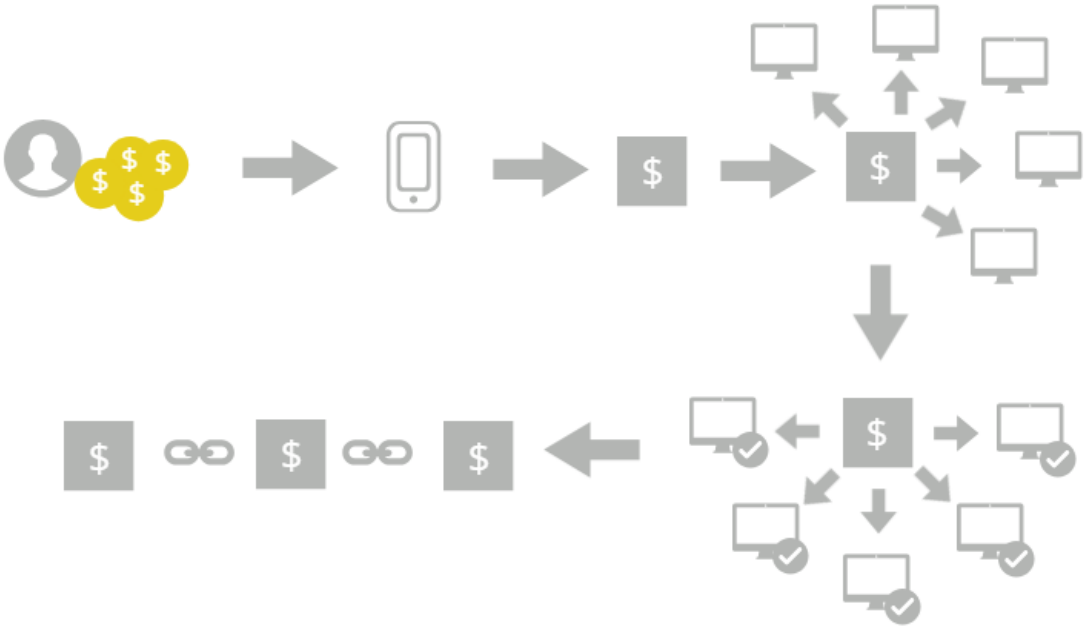
solmu välittää siirron kaikille verkossa oleville solmuille nähtäväksi. Tämän jälkeen siirto ei kuitenkaan siirry suoraan lohkoketjuun vaan siirto siirtyy odottamaan julkaisevaa solmua jonoon. (Yaga ym., 2018, s. 15)

Julkaisevan solmun poimittua siirto, on sen tärkeä varmistaa joitakin asioita, jotta siirto voidaan turvallisesti julkaista lohkoketjuun. Ensimmäinen on varmistaa että käyttäjällä on kryptovaluuttaa omistuksessaan, tämä voidaan tarkistaa siirron digitaalisesta kirjoituksesta. Toinen asia on tarkistus että käyttäjällä on oikeanlaista kryptovaluuttaa tilillään, tämä voidaan toteuttaa vertaamalla käyttäjän aiempia siirtoja hänen käyttäjätiliinsä tai hänen julkiseen avaimeensa. (Crosby, 2016, ss. 9–10)

Jokaisen käyttäjän tulee myös ennen siirtojen tekemistä todistaa että hän omistaa ”yksityisen avaimen”. Esimerkiksi Bitcoin lohkoketju käyttää kryptograafista varmennusta, jolla se suojaa siirrot käyttäjien välillä. (Crosby, 2016, ss. 9–10) Tähän kryptografiseen varmennukseen ja sen purkamiseen hyödynnetään ”Epäsymmetristä avain kryptografiaa” missä käytetään käyttäjien julkista ja yksityistä avainta (Yaga ym., 2018, s. 10). Kyseisten tapahtumien jälkeen lohkossa olevat siirrot on varmennettu ja voidaan aloittaa lohkon varmennus.

Lohko sisältää aina tunnisteen ja rungon. Lohkon tunnisteessa on määritelty tietoja lohkosta ja lohkon rungossa taas on kyseiseen lohkoon lisätyt varmennetut siirrot. Uusi lohko linkitetään aina edelliseen käyttämällä edellisen lohkon hashattyä tunnistetta. Tällä saadaan aikaan se että jos jotakin lohkoa muutetaan niin se huomataan nopeasti koska se vaikuttaa sitä seuraavien lohkojen tunnisteen ja hashin yhdistelmään. (Yaga ym., 2018, ss. 15–17)

Kuva 6. Lohkoketjun toiminta (soveltaen Wild, 2015).



Kuvassa ensimmäiseksi käyttäjä lähettää rahat esimerkiksi älypuhelinsovelluksen kautta maksupyynnön lohkoketjuun. Tämän jälkeen maksupyyntö jaetaan lohkoketjuverkon solmuille, jonka jälkeen ne varmentavat maksupyynnön ja lopuksi lohko varmennetusta maksupyynnöstä lisätään lohkoketjuun.

6 Epäsymmetrinen avain kryptografia

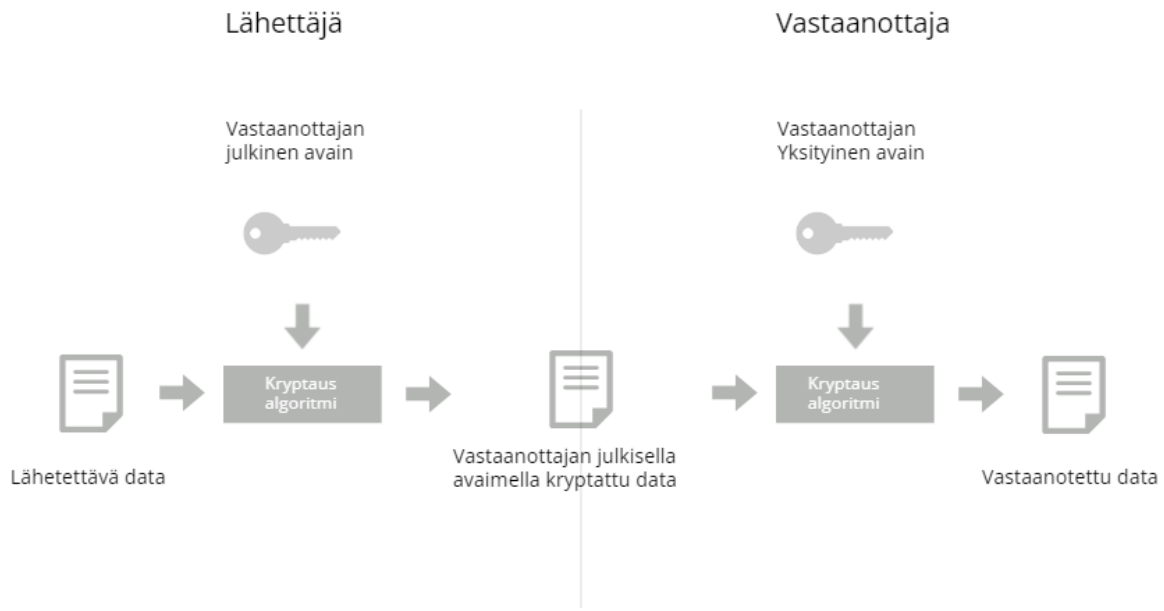
Lohkoketju käyttää toimintaketjussaan tekniikkaa, jota kutsutaan nimellä epäsymmetrinen avain kryptografia. Kyseisessä tekniikassa käyttäjät omistavat niin sanotun yksityisen ja julkisen avaimen. (Puthal ym., 2018, s. 2) Avaimet ovat matemaattisesti yhteydessä toisiinsa. Kuitenkaan julkisen avaimen perusteella ei voida jäljittää käyttäjän yksityistä avainta (Yaga ym., 2018, s. 11).

Yksityinen avain tulee säilyttää salassa muilta käyttäjiltä ja se toimii kyseisen käyttäjän lompakon avaimena. Lompakko on verrattavissa pankkitiliin, siellä säilytetään käyttäjän kryptovaluuttaa. Yksityistä avainta käytetään myös muiden käyttäjien vastaanotettujen siirtojen avaamista varten luotavaan kirjoitukseen, joka on kryptattu lähettäjän yksityisellä avaimella ja vastaanottajan julkisella avaimella (Kuva 7). (Puthal ym., 2018, s. 2)

Toinen avain eli julkinen avain toimii käyttäjän lompakon osoitteena, johon esimerkiksi siirrot voidaan lähettää ja jolla lähettäjä kryptaa lähetettävän viestin. On suositeltavaa että käyttäjät vaihtavat julkista avaintaan tietyin väliajoin säilyttääkseen anonymiteettinsä lohkoketjussa. (Puthal ym., 2018, s. 2)

Epäsymmetrinen avain kryptografia auttaa luottamuksen luomisessa tilanteessa missä käyttäjät eivät tunne toisiaan, kuten julkisessa lohkoketjussa. Se antaa mahdollisuuden myös pitää siirrot julkisina ja samalla lisää mekanismin jonka avulla voidaan varmistaa siirtojen todenmukaisuus. (Yaga ym., 2018, s. 11)

Kuva 7. Epäsymmetrinen avain kryptografia (soveltaen Robinson, 2018).



Kuvassa lähettäjä ensin kryptaa lähetettävän datan vastaanottajan julkista avainta käyttäen, jonka jälkeen kryptattu data kulkee lohkoketjun kautta vastaanottajalle. Vastaanottaja lopuksi dekryptaa saamansa datan käyttäen hänen omaa yksityistä avaintaan ja täten näkee alkuperäisen sisällön.

6.1 Yksityinen avain

Lohkoketjussa yksityinen avain on yksi toisesta osasta, jonka avulla epäsymmetrinen avain kryptografia toimii. Yksityistä avainta voidaan verrata käyttäjän salasanaan, avaimen avulla voidaan käyttää käyttäjän tilillä olevia digitaalisia varoja. Sen takia yksityisen avaimen

suojaus on käyttäjälle hyvin tärkeää. Jos yksityinen avain sattuu katoamaan tai käyttäjä unohtaa sen, on sitä käytännössä mahdoton luoda uudelleen. Jos taas joku saa tietoonsa tämän avaimen hän voi hallita tilillä olevia varoja. (Yaga ym., 2018, s. 13)

Erityisesti julkisissa lohkoketjuissa käyttäjien tulee itse muistaa ja säilyttää heidän avaimiansa. Tätä varten kuitenkin on olemassa ohjelmistoja, joita kutsutaan lompakoksi, mitkä tekevät siitä helpompaa. Lompakot voivat tehdä monia asioita, kuten käyttäjän digitaalisten varojen kirjanpito, mutta tärkein ominaisuus sille on yksityisen avaimen, julkisen avaimen ja osoitteiden ylläpito. (Yaga ym., 2018, s. 13)

6.2 Julkinen avain

Lohkoketjussa julkinen avain on nimensä mukaan jaettu puoli avaimista. Julkinen avain toimii käyttäjän tilin osoitteena tai numerona, johon käyttäjälle tehtävät maksut ja siirrot voidaan suunnata. Tämän avulla voidaan suojata käyttäjän anonymiteettiä, sillä varsinkin julkisissa lohkoketjuissa anonymiteetin ylläpito on erityisen tärkeää. (Aydar ym., 2020, ss. 4–6) Kuitenkaan edes julkinen avain ei suojaa käyttäjän anonymiteettiä täysin, sen vuoksi on suotavaa vaihtaa julkista avainta sopivin väliajoin (Puthal ym., 2018, s. 2).

7 Web3.0

Web3.0 on seuraava askel web1.0 ja web2.0 jälkeen. Web3.0 perustuu suurin osin lohkoketjuteknologian ympärille. Tämän vuoksi sen neljä suurinta keskeisintä pilaria ovat kryptovaluutat, ei vaihdeattavat poletit, hajautetut autonomiset organisaatiot ja metaversumit. (Murray ym., 2022, ss. 2–9)

Yksi keskeisimmistä lupauksista web3.0 on antaa käyttäjille takaisin hallintaa miten he haluavat jakaa omia yksityisiä tietojansa. Web3.0 pyrkii tuomaan parannusta edeltäjäänsä web2.0, jossa ongelmana on että monet yritykset käytännössä omistavat käyttäjiensä datan ja myyvät sitä tienaten rahaa käyttäjiensä yksityisyyden hinnalla. (Murray ym., 2022, ss. 2–9)

Web3.0 myös mahdollistaa lohkoketjujen älysopimusten käytön. Näiden älysopimusten avulla kaksi käyttäjää voivat autonomisesti ilman kolmansia osapuolia suorittaa älysopimuksiin kirjattuja toimintoja eli esimerkiksi vaihtaa kryptovaluuttaa toistensa välillä. (Murray ym., 2022, ss. 2–9)

Web3.0 myötä uskotaan myös että valta jakautuisi enemmän pienemmille tahoille vähentäen täten web2.0 tapahtuvaa keskittyneisyyttä ja yritysten käyttäjilleen kohdistettua yksityisen datan keräämistä (Murray ym., 2022, ss. 2–9).

7.1 Ei uniikit ja uniikit poletit

Lohkoketjussa arvoa kuvaavia esineitä kutsutaan poleteiksi. Näitä poletteja voidaan vaihtaa käyttäjien välillä ja ne voidaan jakaa kahteen eri muotoon. Ei uniikit poletit (FT) ja uniikit poletit (NFT). (Egliston & Carter, 2023, ss. 3–4)

Poleteista ei uniikit sopeutuvat erinomaisesti pelaajien väliseen vaihtamiseen esimerkiksi kryptovaluuttaan ja ne voivat olla saman arvoisia toisten samanlaisten polettien kanssa. Toinen poletti eli uniikki poletti puolestaan on enemmänkin täysin uniikki esine, jolla on uniikki tunniste ja jota ei voida vaihtaa samanlaiseen kappaleeseen, sillä nimensä mukaan sitä ei ole olemassa. Lisäksi uniikissa poletissa on sen metadatassa yhteys sen omistavan tahon virtuaalilompakon osoitteeseen tämä yhteys toimii todisteena poletin omistajuudesta. (Egliston & Carter, 2023, ss. 3–4)

Uniikkien polettien (NFT) kauppa on saanut huomiota niin teollisuus kuin tiedeyhteisöissä. Wang kertoo että 24 tunnin kryptovaluutan vaihtovolyymi on 341,017,001,809 USD:ta ja uniikkien polettien vaihtovolyymi puolestaan on 4,592,146,914 USD:ta. Vain viidessä kuukaudessa uniikkiin polettiin liittyvät vaihdot ovat saavuttaneet 1.3% koko kryptovaluutta marketin vaihdoista. (Wang ym., 2021, s. 2)

7.2 Hajautetut autonomiset organisaatiot

Hajautetut autonomiset organisaatiot lyhenteeltään DAO. Ovat lohkoketjussa olevia organisaatioita, jotka mahdollistavat nimensä mukaan organisaation toiminnan suurimmin osin älysopimuksien kautta. (Murray ym., 2022, s. 16)

Hajautetuissa autonomisissa organisaatioissa älysopimuksiin voidaan kirjata organisaation rakenne, hallinto ja toimintaperiaatteet, jonka jälkeen ne suorittavat itse loput tarvittavat asiat, kuten siirtojen varmennukset. Täten korvaten tarpeen ihmishallinnolle. (Murray ym., 2022, s. 16)

Hajautetuissa autonomisissa organisaatioissa voidaan myös myöntää niiden osallisille niin sanottuja hallintopoletteja, joilla organisaatioon kuuluvat voivat vaikuttaa miten organisaatio kehittyy tai mihin se käyttää esimerkiksi varojaan (Murray ym., 2022, s. 16).

8 Lohkoketju videopeleissä

Lohkoketjupelit ovat lohkoketjun sisällä toimivia videopelejä. Pelit eivät niinkään eroa tavanomaisista peleistä huomattavasti pelattavuutensa vuoksi, mutta enemmänkin toimintatapansa takia. Kuitenkin lohkoketjupelit useimmiten pyrkivät olemaan klikkauspelien tapaisia pelejä, jotka toimivat jonkin aikaa ilman pelaajan välitöntä paikallaoloa. Tämän kaltaisissa peleissä kuitenkin päätarkoituksena on että pelaaja klikkaa jotakin nappia mikä kasvattaa esimerkiksi jotakin lukua ja tiettyyn lukuun päästessä jotakin tapahtuu. Useimmiten palkinnot eri haasteiden läpäisemisestä perustuvat lohkoketjupeleissä kryptovaluuttaan tai johonkin omistettavaan osaan pelin sisällä. Lisäksi lohkoketjupelit näyttävät ei lohkoketjupelien tapaan samankaltaisesti mainoksia, jotka toimivat lisätulona pelikehittäjille. (Almohsen ym., 2022, s. 3)

Lohkoketjupeleissä käytetään pääosin jotakin kryptovaluuttaa maksuvälineenä esimerkiksi Bitcoinia tai Ethereumia. Lisäksi lohkoketjujen muuttumattomuus ja älysopimukset tuovat turvaa peleissä olevien esineiden omistajuuden varmentamiseen. Älysopimusten avulla pelaajat voivat tehdä esineiden omistajuuden vaihtoja välittömästi ilman tarvetta kolmansille osapuolille. Lisäksi älysopimusten avulla voidaan helposti seurata esineiden tämänhetkistä omistajuutta. (Gao & Li, 2021, s. 598)

Lohkoketjuteknologia on nähty mullistavana teknologiana eri toimialojen tuotannossa, jakamisessa ja kulutuksessa. Tarjoamalla hyötyjä molemmille kulutuksen ja tuotannon osakkaille. Sama voidaan nähdä myös lohkoketjuvideopeleissä ja niiden pyrkimyksessä tarjota hyötyjä niin pelaajilleen kuin kehittäjilleen. (Egliston & Carter, 2023, s. 2) Tämän vuoksi lohkoketjuteknologia on yhtiä mielenkiintoisimpia teknologioita 2000-luvulla, jopa yhdeksän vuotta ensimmäisestä ilmestymisestään Bitcoinista. Lohkoketju on jatkanut kehittymistään julkisesta jaetusta tilikirjasta monenlaisiin teknologioihin, kuten Ethereum alustalla toimivat dApp:it. (Min ym., 2019, s. 1)

Kuitenkin Min kirjoittaa että dApp:it kärsivät suurien läpimurto applikaatioiden puutteesta. Initial coin offering (ICO) applikaatio on toiminut suurimpana dApp:na Ethereum alustalla toimivien polettien ilmestymisestä alkaen, mutta lukuisat huijaukset ja turhat poletit ovat

syöneet sen suosiota vuosien aikana. Tämän vuoksi Min kuvailee että digitaaliset pelit voisivatkin tuoda mahdollisen pelastuksen tälle teknologialle. (Min ym., 2019, s. 1)

Lohkoketjupelien suurin lupaus onkin tarjota vaihtoehtoa suurimmin osin suurien AAA-kokoisten peliyhtiöiden suorittamalle rahastukselle, jossa kaikki pelaajien luoma hyöty oli se sitten pelin kulttuurin kehittämistä tai pelin ohjelmiston avulla luotu lisäsisältö päätyy suoraan ja ainoastaan peliyhtiölle itselleen. Lohkoketjupelit näkevät pelaajat enemmänkin taloudellisina kohteina ja tarjoavat heille mahdollisuuden investoida peliin saaden täten reilumman kohtelun, mutta hyväksymällä myös sijoitukseen liittyvät riskit. (Egliston & Carter, 2023, s. 3)

8.1 Play-to-Earn

Videopeleillä on ollut vuosien varrella monenlaisia erilaisia binsesmalleja (Taulukko 1). Nämä bisnesmallit ovat kehittyneet teknologian evoluution mukana koittaen pysyä houkuttelevana niin kuluttajalle kun tuottajalle. (Karapapas ym., 2022, s. 1)

Ensimmäisenä ja ehkä tunnetuimpana oli tavanomainen Pay-to-Play (P2P), missä pelaajat maksavat peliyhtiöille pelistä jonkin suuremman kertasumman etukäteen ja saavat täten suoraan täyden pääsyn pelaamaan koko peliä. P2P mallin jälkeen pelien bisnesmallit kehittyivät ilmaiseen Free-to-Play (F2P) malliin. F2P mallissa pelaajat pääsevät pelaamaan peliä täysin ilmaiseksi, mutta usein täyttä peliä ei voida kuitenkaan pelata ilmaiseksi. Täyden pelikokemuksen avaamiseksi usein pelaajat joutuvat maksamaan niin sanotusta lisäsisällöstä. Lisäsisältö voi olla esimerkiksi pelin sisäisiä tavaroita tai uusia karttoja. F2P malli on myös luonut tietä pelaajien uralle ammattipelaajina ja eSports toimialalle. F2P mallin jälkeen lohkoketjupelien myötä suosituimmaksi on noussut Play-to-Earn (P2E) malli. (Karapapas ym., 2022, s. 1)

Videopelaajat ovat jo pitkään tienneet ettei pelaaminen ole rahallisesti tuottava harrastus vaikka useilla pelaajilla voi olla jopa tuhansia tunteja upotettuna peliin on siitä todellisuudessa ollut pelaajalle yleensä vain haittaa rahallisesti. Lisäksi useiden pelien hinnat ovat kasvamaan päin ja itse pelien kehittäjät ovat siirtyneet vuosi vuodelta pahempien rahoitustoimenpiteiden käyttöön. Tämän ilmiön vuoksi Play-to-Earn pelit ovat keränneet suosiota. (Delfabbro ym., 2022, ss. 2–3)

Play-to-Earn pelit ovat pelejä, joista myös pelaaja voi saada hyötyä pelkällä pelaamisellaan esimerkiksi ansaitsemalla poletteja, joita voidaan vaihtaa jopa oikeaan rahaan. Itse

konseptina Play-to-Earn ei ole uusi, eikä se aina vaadi lohkoketjua taustalle toimiakseen, kuten Delfabbro antaa kirjoituksessaan ilmi. Esimerkiksi Diablo-sarjan peleissä, jotka eivät ole lohkoketjupelejä on voitu vaihtaa pelaajien kesken pelin sisäisiä kosmeettisia esineitä oikeaan rahaan. Kuitenkin lohkoketju voi mahdollistaa joitakin hyötyjä Play-to-Earn peleihin, kuten kryptovaluutan ansaitseminen pelaamisesta ja pelien välisen tavaroiden vaihtamisen. (Delfabbro ym., 2022, ss. 2–3)

Taulukko 1. Eri pelien bisnesmallien vertailu.

	Mahdollisuus ansaita rahaa pelaamisesta	**Pelin hinta**	**Mahdollisuus pelata koko peliä ilman tarvittavia lisäosia**
Pay-to-Play	**Usein ei mahdollisuutta ansaita varoja pelaamisesta. Tavaran vaihtaminen rahaan usein jopa pelin sääntöjen vastaista.**	**Peliä ostettaessa, jokin maksettava kertasumma.**	**Pelistä riippuvainen vanhemmat pelit usein olivat yksittäisiä kokonaisuuksia, mutta uudemmat pelit voivat sisältää lisäosia.**
Free-to-Play	**Sama kuin Pay-to-Play mallissa. Tavaroiden vaihtaminen rahaksi rikkoo pelin sääntöjä.**	**Täysin ilmainen**	**Usein kaiken sisällön saavuttamiseksi pelaajan pitää ostaa se.**
Play-to-Earn	**Pelistä ansaittuja varoja voidaan sääntöjen puitteissa vaihtaa kryptovaluuttaan.**	**Usein pelin alussa asetettava alkupääoma.**	**Pelistä ansaittavaa rahaa käytetään pelin sisällön ostamiseen.**

8.2 Play-to-Earn haitat

Vaikka Play-to-Earn saattaa vaikuttaa hyvin lupaavalta vaihtoehdolta hyvien puoliensa vuoksi, kuten rahan ansaitseminen pelaamisella. Sisältyy siihen myös joitakin haittapuolia.

Esimerkiksi Englistonin mukaan yleinen kuvituskuva Play-to-Earn lohkoketjupeleissä on ollut että polettien ansiosta pelaamiselle syntyisi jokin ylläpidettävä arvo ja että pelaajat voisivat poletteja vaihtamalla tehdä paljonkin ylimääräistä tuloa itselleen.

SkyMavisin Axie Infinite pelin kautta on huomattu kuitenkin että vain taitavimmilla pelaajilla, jotka osallistuvat pelin ”scholarship” ohjelmaan on mahdollisuus tienata siltikin juuri ja juuri Filippiinien minimipalkan verran tuloa. Lisäksi on myös osittain syntynyt narratiivi missä pelaajat kuvitellaan lohkoketjupeleissä enemmänkin sijoittajina, jotka koittavat vain tienata ja saada pelaamisellaan haltuunsa arvoikkaita poletteja, joita he voivat vaihtaa isoilla alustoilla, kuten Binance, FTX ja OpenSea. (Egliston & Carter, 2023, ss. 11–13)

Kuitenkin esimerkiksi lohkoketjupeli Nyan Heroes on nimenomaan ilmoittanut kehittävänsä pelejä juuri siihen tarkoitukseen että pelaajat voisivat hyötyä niistä rahallisesti vaihtamalla poletteja toisten pelaajien kanssa. Mutta myös jotkin lohkoketjualustat, kuten Ubisoft:in Quartz alusta puskevat tätä ilmilötä vastaan ilmoittamalla että heidän alustallaan tullaan vaatimaan pelaajilta tiettyä peliaikaa ennen kuin pelaajan on mahdollista ansaita poletteja. Tällä Ubisoft pyrkii pitämään alustan enemmänkin oikeille pelaajille kun pelkille investoijille. (Egliston & Carter, 2023, ss. 11–13)

Yleisin haittaskenaario kuitenkin mitä Play-to-Earn peleissä tapahtuu on sama mitä on nähty aiemmin tavanomaisissakin videopeleissä, kuten esimerkiksi World of Warcraftin kullan myynnissä. Itse materiaalin hankkiminen ulkoistetaan maihin, jossa asuu paljon matalapalkkaisia ihmisiä ja kullan myyjät muualla maailmassa vetävät itselleen isoimman osan tuotoista. Axie Infinite pelissä on nähty sama tapahtuvan kun rikkaat niin sanotut ”valaat” omistavat suurimman osan pelin poleteista. (Egliston & Carter, 2023, ss. 11–13)

9 Lohkoketjun avulla saavutettavat hyödyt videopeleissä

Lohkoketjuteknologia mahdollistaa lohkoketjupeleissä saman kuin se mahdollistaa rahan säilyttämisessä eli jaetun tilikirjan, datapankin ja älysopimusten käytön. Tähän datapankkiin voidaan helposti kirjata kaikki mahdolliset pelaajien keskenään käymänsä vaihdot pelin sisällä. Lisäksi lohkoketjulla voidaan mahdollistaa esimerkiksi eri pelien välinen esineiden ja polettien vaihtaminen. (Min ym., 2019, s. 1)

Pelien sisäisten hyötyjen lisäksi lohkoketju tuo parannuksia pelien suojaukseen, ykistyisyyteen ja omistajuuden varmentamiseen, varsinkin älysopimuksien avulla. Pelaajat myös saavat lohkoketjun myötä omistajuuden esineilleen peleissä, joita he pelaavat. Tarkoittaen että tavarat jotka he omistavat pelissä voivat olla uniikkeja, vaihdettavia, ja täysin pelinkehittäjästä riippumattomia. (Min ym., 2019, s. 1)

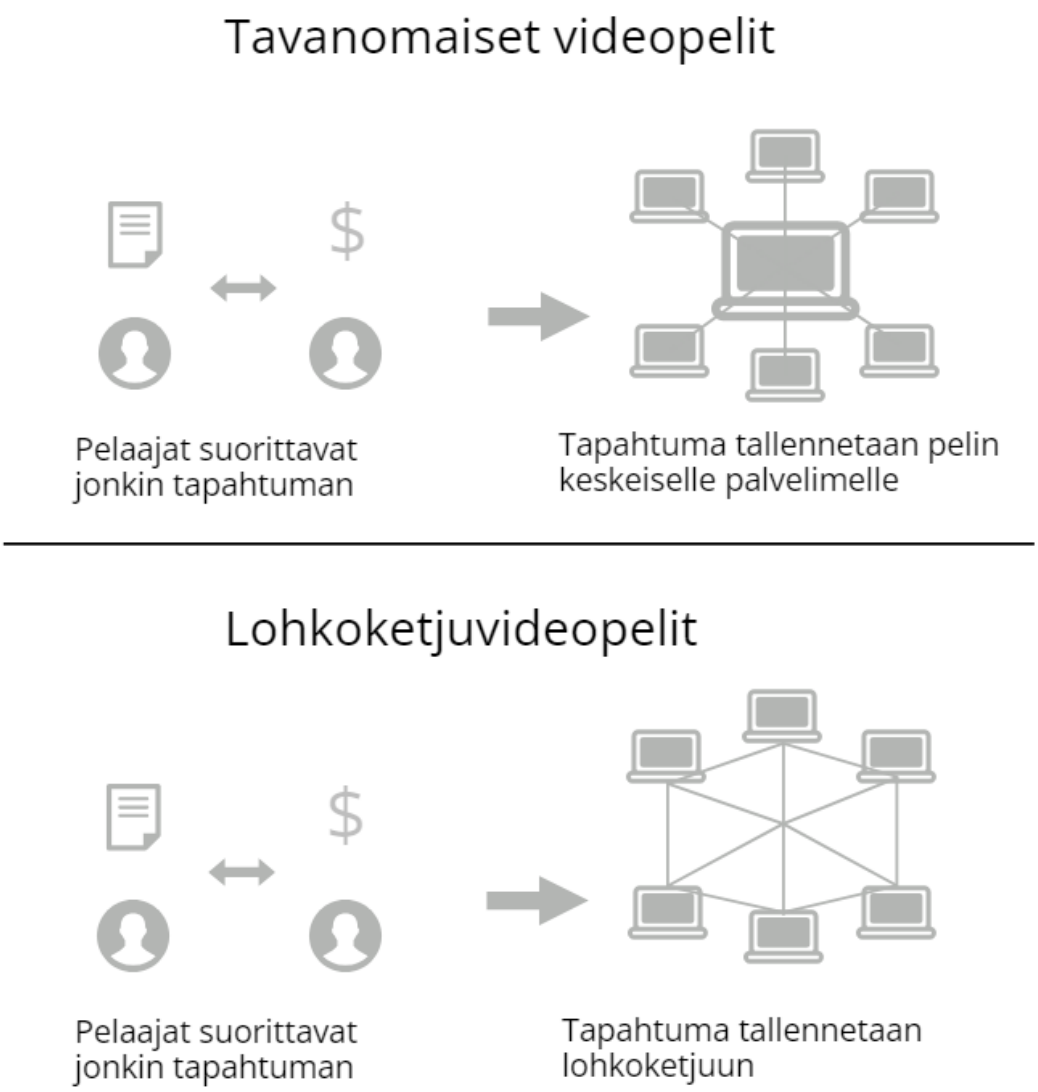
9.1 Tavaroiden säilytys hajautetussa datapankissa

Lohkoketjun avulla voidaan suojata pelin sisältämää dataa paljon paremmin kuin esimerkiksi tavanomaisissa videopeleissä. Tavanomaisissa videopeleissä kaikki data, kuten esineiden omistajuus ja vaihtohistoria säilytetään pelin keskeisessä tietokannassa (Kuva 8). Tämä luo suuren riskin, sillä kaikki käyttäjät luottavat yhteen lähteeseen datan todenmukaisuuden suhteen. Keskeisessä tietokannassa olevaa dataa voidaan manipuloida, joko esimerkiksi hyökkääjän tai jopa epärehellisen pelintuottajan toimesta ja kellään käyttäjällä ei ole edes tietoakaan että näin on päässyt käymään. Tämä kyseinen ongelma voidaan kuitenkin korjata täysin lohkoketjun avulla. (Scholten ym., 2019, s. 380)

Scholten tuo tekstissään esiin hyvän esimerkin lohkoketjun tuomasta hyödystä videopelejen datan säilyttämisessä hajautetussa datapankissa. Esimerkissä pelaajat tekevät keskenään tavallisen vaihtokaupan pelin sisällä. Videopelissä pelaaja A myy miekan pelaajalle B. Tavanomaisesti tämä tieto on tallennettu pelin palvelimelle C ja vaihdon tapahtuessa pelaaja A lähettää palvelimelle C pyynnön päivittää miekan omistajuus pelin datapankkiin. Kyseisessä skenaariossa pelin datapankki vastaa lohkoketjun tilikirjaa, poikkeuksena ettei se ole hajautettu. Tämä luo suuren riskin, sillä vaikka keskeiset datapankit ovat nopeita ja toimivia, niissä on yksi keskeinen piste mihin esimerkiksi hyökkäys voidaan kohdistaa. Lisäksi ne vaativat käyttäjiään luottamaan yhteen tahoon niiden hallitsemisessa. (Scholten ym., 2019, s. 380)

Scholten tuo esimerkeiksi kolme asiaa, mitä jos pelissä tapahtuu virhe ja vaihto korruptoituu kun se koitetaan lisätä palvelimen datapankkiin, hakkeri päättää manipuloida pelin datapankkia tai jopa pelin yksi hallintotaho päättää jonain päivänä pyyhkiä koko datapankin tyhjäksi. Tähän ongelmaan lohkoketjuteknologia voi tarjota ratkaisun. Sen avulla pelaajat A ja B, sekä palvelin C kaikki pitävät omat kopionsa pelin datapankista ja kun esimerkiksi pelin sisäinen vaihto tapahtuu, yksi tai useampi solmu ratkaisevat kyseisen vaihdon yksimielisyysmalleja hyödyntäen ja tieto päivitetään jokaisen tahon datapankin kopioon. (Scholten ym., 2019, s. 380)

Kuva 8. Lohkoketjuvideopelien tietojen tallentaminen vertaus (soveltaen Chainlink, 2023).



Kuvassa verrataan lohkoketjuvideopelien tietojen tallennusta hajautettuun järjestelmään verrattuna tavanomaisten videopelien tietojen tallentaminen ei hajautettuun järjestelmään. Hajautettu järjestelmä on turvallisempi ja luotettavampi hyökkäyksiä kohtaan verrattuna tavanomaiseen tietokantaan.

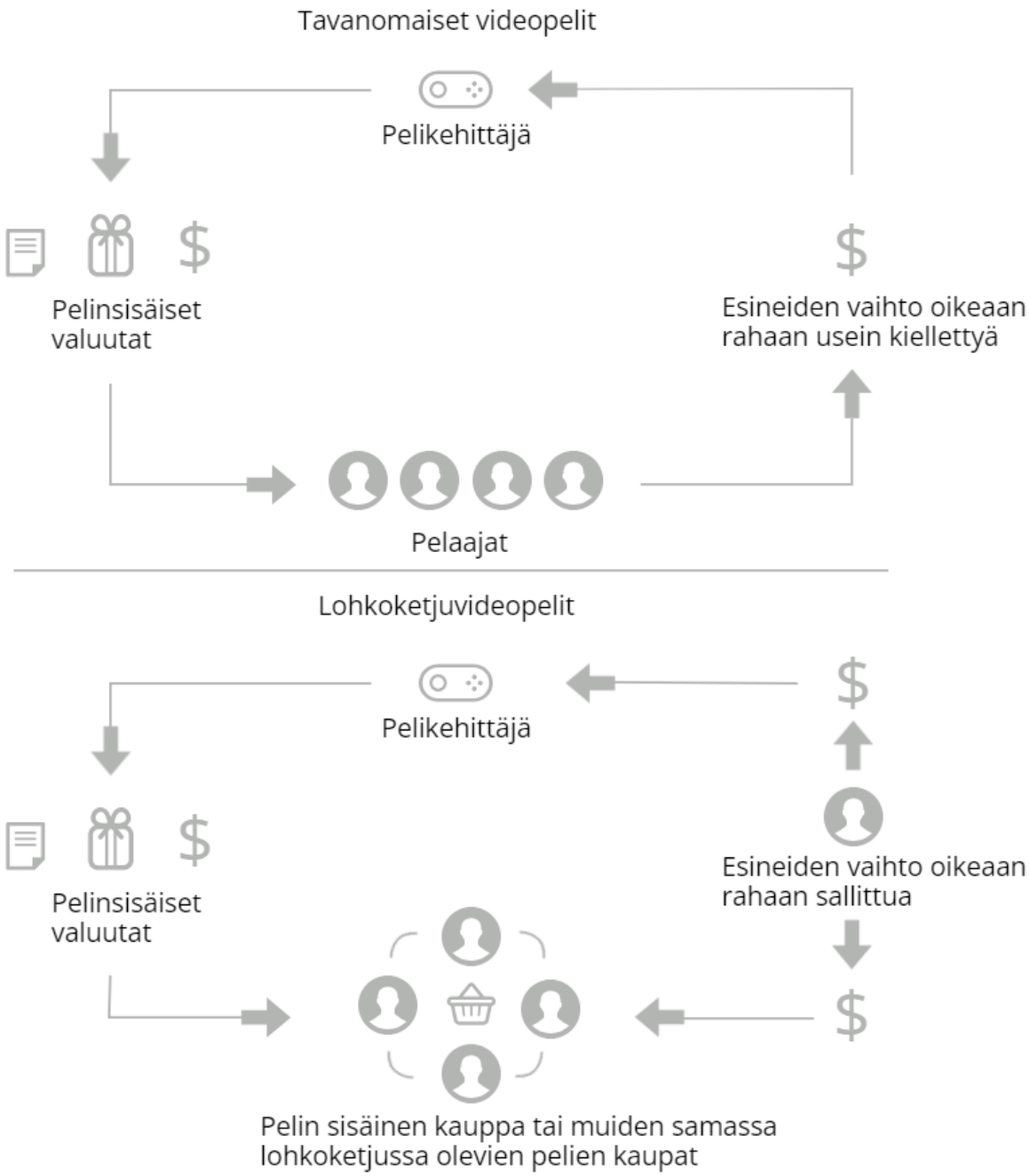
9.2 Tavaroiden vaihtaminen pelien välillä

Myös muita hyötyjä voidaan saavuttaa videopeleissä lohkoketjun avulla, kuten esimerkiksi samojen esineiden käyttö pelien välillä. Pfeiffer antaa kirjoituksessaan esimerkiksi World of

Warcraftin ja Diablon. Kummatkin pelit ovat saman peliyhtiön Blizzard Enterntainmentin omistuksessa olevia pelejä, joskin eivät aivan samaa peligenreä. Kumpikin peli kuitenkin käyttää samaa mekanismia esineiden arvon määrittämiseksi. (Pfeiffer ym., 2020, s. 3)

Esimerkkinä melko arvottomat esineet ovat peleissä merkitty harmaalla värillä, näistä hieman arvokkaammat valkoisella. Näitä esineitä Pfeiffer kuvaa esimerkissään että ne voisivat olla lohkoketjussa normaaleina merkintöinä. Vihreät esineet ovat esineitä, joilla on hieman arvoa nämä esineet voisivat esimerkin mukaan toimia poletteina, joita voidaan lisätä tarvittaessa. Violetit esineet ovat esineitä, joilla on jo aika paljon arvoa peleissä. Näitä Pfeiffer esittää uniikeiksi poleteiksi, joita on vain rajoitetun verran pelissä. Lopuksi vielä oranssit esineet. Nämä esineet ovat arvoltaan legendaarisia esineitä, jotka voisivat olla täysin uniikkeja poletteja, joilla on oma uniikki tunnuksensa ja jota ei voi olla monta samanlaista. Kyseisiä poletteja voisi vaihtaa pelaajien välillä lohkoketjussa toimivissa peleissä (Kuva 9). Myös tapauksissa, joissa poletit eivät ole käytettävissä eri peleissä voitaisiin hyödyntää älysopimuksia, joilla poletit voitaisiin vaihtaa mahdollisesti oikeaksi rahaksi. (Pfeiffer ym., 2020, s. 3)

Kuva 9. Lohkoketjuvideopelien esineiden vaihto verrattuna tavanomaisiin videopeleihin (soveltaen Chainlink, 2023).



Kuvassa verrataan tavaroiden vaihtamista ja myymistä tavanomaisissa videopeleissä lohkoketjuvideopeleihin. Tavanomaisissa videopeleissä vaihto on mahdollista ainoastaan pelin sisällä ja esineiden myynti oikeaa rahaa vastaan on usein pelin sääntöjä vastaan. Lohkoketjuvideopeleissä esineitä voi vaihtaa muiden samassa lohkossa olevien pelien välillä ja vaihto kryptovaluuttaan on myös mahdollista.

9.3 Luottamus, suojaus ja yksityisyys

Yksityisyys on yksi suurimmista asioista lohkoketjussa. Usein perinteisissä verkon kautta tapahtuvissa maksutapahtumissa ihmiset usein pelkäävät yksityisyytensä puolesta. Nykyään monet jokapäiväisessä käytössä olevat mobiiliohjelmat käyttävät yhä enemmän yksityisiä tietoja toimintaansa muodostaen riskejä yksityisyyteen liittyen. (Gao & Li, 2021, ss. 601–602)

Lohkoketjujen älysopimusten avulla näitä riskejä voidaan kuitenkin välttää, käyttämällä älysopimusten autonomisia toimintoja, joissa käyttäjä voi itse valita miten se jakaa yksityisiä tietojaan. Varsinkin lohkoketjuvideopeleissä missä vaihtoja tehdään usein nämä älysopimukset tuovat turvaa pelaajille ja heidän yksityisyydelleen. (Gao & Li, 2021, ss. 601–602)

Toinen lohkoketjun tuomista eduista on suojaus. Lohkoketju tarjoaa hajautetun järjestelmän mikä tuo turvaa erilaisilta kyberhyökkäyksiltä, sillä hyökkäys yhteen kohtaan järjestelmää ei riitä sen kaatamiseen. (Gao & Li, 2021, ss. 601–602)

Lohkoketju myös tarjoaa käyttäjilleen avoimuutta ja läpinäkyvyyttä vaihtojen tekemisessä, sillä kuka vaan voi lohkoketjussa tarkistaa jonkin esineen tapahtumahistorian. Kolmantena tärkeänä hyötynä lohkoketju tuo luottamusta ylläolevien asioiden avulla. Lisäksi koska lohkoketjussa ei käytetä kolmatta osapuolta tai ketään keskeistä varmentajaa on luottamus toimintaan erityisen tärkeää. (Gao & Li, 2021, ss. 601–602)

9.4 Pelaajien mahdollisuus vaikuttaa peliin

Yksi tärkeä ominaisuus, jonka lohkoketjuteknologia voi tuoda videopeleihin on mahdollisuus vaikuttaa mihin suuntaan ne kehittyvät. Lohkoketjuvideopeleissä pelaajilla on mahdollisuus sijoittaa varojaan hallintopoletteihin. Hallintopolettien avulla pelaajat voivat äänestää mitä muutoksia peleihin halutaan tehdä. (Delfabbro ym., 2022, s. 4)

10 Yhteenveto ja loppupohdinnat

Lohkoketjuteknologia voi avata monia ovia videopelien tulevaisuudessa ja niiden kehityksessä niin pelaajille kuin itse videopelien kehittäjille (Taulukko 2). Pelaajien mahdollisuus tehdä vaihtoja toistensa kanssa eri pelien esineiden välityksellä on suuri etu mikä ei ole ollut usein mahdollista ennen lohkoketjupelien ilmestymistä, myös pelin sisäisten

esineiden oikea omistajuus ja oikean rahan mahdollinen ansaitseminen on suuri etu pelaajille ja antaa heille motivaatiota pelata enemmän.

Myös lohkoketjupelien suoma mahdollisuus pelaajille vaikuttaa pelien kehityksen ja tulevaisuuden suuntaan sijoittamalla valuuttaa siihen on ennen ollut käytännössä mahdottomuus. Tämän lisäksi monet muutkin tavanomaisten videopelien ongelmat, kuten pelien sisäinen huijaaminen, peleihin kohdistetut hyökkäykset ja pelien laiton lataaminen on ratkaistavissa lohkoketjuteknologian avulla.

Lohkoketjuteknologia tarjoaa hajautetun rankenteensa vuoksi pelaajille varmuutta ettei peliä voida kaataa kohdistamalla esimerkiksi kyberhyökkäys pelin ylläpitäjää kohtaan. Koska lohkoketjuteknologiassa jokaisella pelaajalla on oma kopionsa pelin datapankista ei pelien sisäinen huijaaminen ole juurikaan mahdollista, ellei huijari omista suurinta osaa pelin poleteista tai ellei sillä ole tietokoneessaan laskentatehoja suorittaakseen 51% hyökkäys mikä on hyvin harvinaista ja lähes mahdotonta toteuttaa onnistuneesti.

Play-to-Earn mallin ollessa suosituin lohkoketjupelien keskuudessa ja lohkoketjupelien toimiessa lohkoketjuverkon päällä mahdollistaa se ettei pelejä voida ladata yksinpelien lailla laittomasti verkosta täten antamalla suojaa ja motivaatiota lohkoketjupelikehittäijä kohtaan.

On kuitenkin myös todettava ettei lohkoketjuteknologia ole aivan täydellinen ja silläkin on omat rajoituksensa videopeleissä. Esimerkiksi julkisissa lohkoketjuissa vaadittavien yksimeilisyysmallien vuoksi siirtoja ei voida tehdä niin nopeasti kuin tavanomaisissa keskitetyissä videopeleissä. Tämä tuo myös jonkin verran rajoituksia lohkoketjupelien pelattavuuteen ja sen vuoksi lohkoketjupelit ovat usein hyvin simppelin näköisiä klikkauspelejä.

Kuitenkin lohkoketjuteknologia on vielä todella alkuvaiheessa varsinkin videopelien osalta ja ajanmittaan on selvää että nykyiset ongelmat voidaan ratkaista teknologian kehittyessä eteenpäin.

Taulukko 2. Tavanomaisten videopelien vertaaminen lohkoketjuvideopeleihin.

	Hajautetun järjestelmän hyödyt	**Pelistä ansaittavien tavaroiden vaihtaminen muiden pelien välillä**	**Parempi luottamus suojaus ja yksityisyys**	**Mahdollisuus vaikuttaa pelin kehityksen suuntaan**
Tavanomaiset videopelit	**Tavanomaiset videopelit käyttävät keskitettyjä tietokantoja toiminnassaan, jotka ovat tiedettyjä olevan haavoittuvaisia hyökkäyksille.**	**Tavanomaisissa videopeleissä tavaroiden vaihtaminen pelien välillä on usein mahdotonta, sekä usein pelien esineiden vaihtaminen oikeaan rahaan on jopa sääntöjen vastaista.**	**Tavanomaisissa videopeleissä pelejen kirjautumiseen käytetään käyttäjänimeä ja salasanaa, jotka ovat tallennettu keskeiseen tietokantaan.**	**Tavanomaisissa videopeleissä pelaajat ovat täysin pelikehittäjien armoilla mihin suuntaan pelit kehittyvät.**
Lohkoketjuvideopelit	**Lohkoketjuvideopelit käyttävät toiminnassaan hajautettuja tietokantoja, jotka tuovat suojaa hyökkäyksiä kohtaan, sillä yhden solmun kaatuminen ei haittaa.**	**Lohkoketjuvideopeleissä tavaroiden vaihtaminen pelien välillä on täysin mahdollista ja pelien esineiden myyminen on täysin sallittua.**	**Lohkoketjupeleissä käyttäjänimen ja salasanan sijaan henkilöt ovat kirjautuneina heidän digitaalista lompakkoa käyttäen.**	**Lohkoketjupeleissä hallintopolettien avulla pelaajat voivat vaikuttaa äänestämällä mihin suuntaan peli kehittyy.**

Opinnäytetyön tekeminen oli pitkä, mutta mielenkiintoinen prosessi. Koin kehittyväni suuresti prosessin aikana niin itse raportin kirjoittamisessa kuin lähteiden etsimisessä ja itse lohkoketjuteknologian tuntemuksessa.

Aiheen koin olevan tärkeä ja relevantti, sillä videopelien keskuudessa eletään murrosta, missä pelikehittäjät alkavat kääntää katseitaan kohti uusia teknologioita, kuten metaversumit ja lohkoketju.

Lohkoketjuteknologiat ovat suurelle osalle täysin tuntematon aihe ja useat ihmiset kokevat epäluottamusta sitä kohtaan, vaikka se voi tuoda monenlaisia parannuksia ja hyötyjä muillekkin kun pelkille videopeleille.

Koska lohkoketju teknologiana on uusi eikä ehkä niin esillä. Tieto sen etsimiseen on osin hyvinkin rajallista varsinkin lohkoketjuvideopelien kohdalla. Myös koska kyseessä on moderni teknologia, joka kehittyy käytännössä joka vuosi on siihen relevantin kirjallisuuden etsiminen haasteellista ja useimmat artikkelit ovatkin suurimmin osin hypelehtien julkaisemia.

Kuitenkin oma tuntemukseni aiheesta oli kohtalainen jo valmiiksi, joten se auttoi hieman lähdeaineiston hakemisessa. Loppujen lopuksi opinnäytetyöni tulos oli odotettu kirjallisuuskatsaus lohkoketjuteknologian hyödyistä videopeleissä ja koin saaneeni maaliin kutakuinkin kaiken haluamani opinnäytetyöni suhteen.

Oma tarkoitukseni on antaa opinnäytetyöni lukijalle käsitys ja ymmärrystä lohkoketjuteknologiasta ja ehkä hieman rikkoa jäätä useiden epäluottamusten suhteen. Tämä oli ensimmäinen pidempi raportti minkä olen koskaan kirjoittanut, joten alku oli osin hankala. Opinnäytetyöni ei suinkaan ole täydellinen ja sitä varmasti pystyisi kehittämään enemmän, mutta tähän tilanteeseen koen että se on juuri sopiva ja onnistunut.

Lähteet

Alharby, M., & Moorsel, A. V. (2017). Blockchain Based Smart Contracts: A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*, 125–140. https://doi.org/10.5121/csit.2017.71011

Almohsen, H., Banaweer, G., & Alharthi, S. (2022). *Players Trust and Awareness of Blockchain Gaming and NFTs*. https://doi.org/10.13140/RG.2.2.22224.99844

Benhaddou, S. (2019). Learning Blockchain: Proof of Stake. Linkedin. https://www.linkedin.com/pulse/learn-blockchain-proof-stake-sofyan-benhaddou

BitYoga team. (2020). Blockchain for social media – A cloud-agnostic Blockchain as a Service (BaaS) offering permissioned blockchain services for agile social media. Articonf. https://articonf.eu/blockchain-for-social-media/

Chainlink. (2023). What Are Blockchain Games? Chainlink Blog. https://blog.chain.link/blockchain-gaming/

Crosby, M. (2016). *BlockChain Technology: Beyond Bitcoin*. *2*. https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Di Pierro, M. (2017). What Is the Blockchain? *Computing in Science & Engineering*, *19*, 92–95. https://doi.org/10.1109/MCSE.2017.3421554

Egliston, B., & Carter, M. (2023). Cryptogames: The promises of blockchain for the future of the videogame industry. *New Media & Society*, 14614448231158614. https://doi.org/10.1177/14614448231158614

Gao, S., & Li, Y. (2021). An empirical study on the adoption of blockchain-based games from users' perspectives. *The Electronic Library*, *39*(4), 596–614. https://doi.org/10.1108/EL-01-2021-0009

Iredale, G. (2019). *Introduction To Permissioned Blockchains*. [Public vs Private Blockchain Network]. 101Blockchains. https://101blockchains.com/permissioned-blockchain/

Karapapas, C., Syros, G., Pittaras, I., & Polyzos, G. C. (2022). Decentralized NFT-based Evolvable Games. *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 67–74. https://doi.org/10.1109/BRAINS55737.2022.9909178

Liang, Y.-C. (2020). Blockchain for Dynamic Spectrum Management. Teoksessa Y.-C. Liang (Toim.), *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence* (ss. 121–146). Springer. https://doi.org/10.1007/978-981-15-0776-2_5

Min, T., Wang, H., Guo, Y., & Cai, W. (2019). *Blockchain Games: A Survey* (arXiv:1906.05558). arXiv. http://arxiv.org/abs/1906.05558

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2567–2572. https://doi.org/10.1109/SMC.2017.8123011

Mohanta, B., Panda, S., & Jena, D. (2018). *An Overview of Smart Contract and Use Cases in Blockchain Technology*. https://doi.org/10.1109/ICCCNT.2018.8494045

Murray, A., Kim, D., & Combs, J. (2022). The Promise of a Decentralized Internet: What is Web 3.0 and How Can Firms Prepare? *Business Horizons*. https://doi.org/10.1016/j.bushor.2022.06.002

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Computing*, *22*(S6), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5

Pfeiffer, A., Kriglstein, S., & Wernbacher, T. (2020). Blockchain Technologies and Games: A Proper Match? *International Conference on the Foundations of Digital Games*, 1–4. https://doi.org/10.1145/3402942.3402996

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). *Everything you Wanted to Know about the Blockchain*. https://www.smohanty.org/Publications_Journals/2018/Mohanty_IEEE-CEM_2018-Jul_Blockchain.pdf

Robinson, K. (2018). What is Public Key Cryptography?. Twilio. https://www.twilio.com/blog/what-is-public-key-cryptography

Scholten, O. J., Hughes, N. G. J., Deterding, S., Drachen, A., Walker, J. A., & Zendle, D. (2019). Ethereum Crypto-Games: Mechanics, Prevalence, and Gambling Similarities. *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, 379–389. https://doi.org/10.1145/3311350.3347178

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the Origins and Variations of Blockchain Technologies. *IEEE Security & Privacy*, *17*(1), 72–77. https://doi.org/10.1109/MSEC.2019.2893730

Solat, S., Calvez, P., & Naït-Abdesselam, F. (2020). Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *Journal of Software*, *16*, 95–106. https://doi.org/10.17706/jsw.16.3.95-106

Wild, J., Arnold, M., & Stafford, P. (2015). Technology: Banks seek the key to blockchain. Financial Times. https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NIST IR 8202; s. NIST IR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Zhang, Y., & Liu, D. (2022). Toward Vulnerability Detection for Ethereum Smart Contracts Using Graph-Matching Network. *Future Internet*, *14*(11), Article 11. https://doi.org/10.3390/fi14110326

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko