Teemu Korhonen

Web 3.0 ja lohkoketjuteknologia

Tietotekniikan kandidaatintutkielma

29. tammikuuta 2024

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Teemu Korhonen

Yhteystiedot: teemu.t.korhonen@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Web 3.0 ja lohkoketjuteknologia

Title in English: Web 3.0 and blockchain technology

Työ: Kandidaatintutkielma

Opintosuunta: Kandidaatintutkielma

Sivumäärä: 18+0

Tiivistelmä: Tutkielmassa käydään läpi lohkoketjuteknologian tarjoamia mahdollisuuksia ja potentiaalia nykyisten järjestelmien rinnalla sekä osittain myös korvaajana keskittyen erityisesti luotettavan tiedonsiirron, hajautuksen ja tietoturvan näkökulmaan World Wide Webin kehityksessä kohti Web 3.0:n aikakautta. Vaikka lohkoketjuja hyödynnetään jo muun muassa toimitusketjujen hallinnassa ja kiinnostus lohkoketjuja kohtaan on lähivuosina kasvanut, vaatii uuden teknologian laajamittainen käyttöönotto parannuksia erityisesti skaalautuvuuteen liittyvissä ongelmissa.

Avainsanat: Web 3.0, lohkoketju, skaalautuvuus, Ethereum, älysopimukset, WWW:n tulevaisuus

Abstract: This study explores the possibilities and potential of blockchain technology alongside existing systems and, to some extent, as a replacement for them. The focus is on reliable data transfer, decentralization, and security in the development of the World Wide Web and Web 3.0. Even though blockchain technology is already being utilized for example in supply chain management and interest in blockchains has increased in recent years, the widespread adoption of this new technology requires improvements, especially addressing issues related to scalability.

Keywords: Web 3.0, blockchain, scalability, Ethereum, smart contracts, the future of WWW

Sisällys

1 Johdanto

Yhteiskunnan digitalisoituessa ja arjen palveluiden siirtyessä yhä enemmän sähköiseen muotoon, korostuvat samalla nykyisten järjestelmien puutteet ja haavoittuvuudet muun muassa keskitetystä luonteestaan johtuen. Alkuperäisen World Wide Webin kehittäjä Tim Berners-Lee kritisoi Decentralized Web Summit 2016 -tapahtumassa pitämässään puheessa webin nykytilaa ja toivoi tulevaisuuden kehityssuunnan olevan kohti hajautetumpaa internetiä, jossa käyttäjät voivat hallita paremmin omaa henkilökohtaista dataansa (Berners-Lee 2016). Hajautetumman webin kehittämiseksi vaaditaan kuitenkin muutoksia sen nykyisissä rakenteissa ja Web 3.0:n tarpeisiin vastaavan teknologian kehitystä. Tässä tutkielmassa tarkastellaan lohkoketjuteknologian potentiaalia osana Web 3.0 -ekosysteemiä.

Tutkielman ensimmäisessä luvussa käydään läpi World Wide Webin kehitysvaiheet ja nykyinen kehityssuunta sekä ongelmat WWW:n rakenteeseen ja nykyjärjestelmiin liittyen. Luvuissa 3-4 tutustutaan lohkoketjuun ja sen ominaisuuksiin, jonka lisäksi arvioidaan lohkoketjuteknologiaan liittyviä haasteita. Lopuksi pohditaan miltä tulevaisuus näyttää niin Web 3.0:n kuin lohkoketjuteknologiankin kannalta.

2 World Wide Webin kehitys

Tässä kappaleessa perehdytään tiivistetysti World Wide Webin (WWW) kehitysvaiheisiin. Teknologian kehitys on tuonut mukanaan useita uhkia, joita webin rakenne nykymuotoisena on osaltaan mahdollistanut. Kappaleessa listataan keskeisiä ongelmakohtia sekä käydään läpi lähihistorian varoittavia esimerkkejä tietoturvan pettämisestä.

2.1 WWW:n vaiheet pähkinänkuoressa

Vuonna 1989 Sveitsin CERNissä työskennellyt englantilainen Tim Berners-Lee kehitti tehokkaampaa tapaa jakaa ja hallita tietoa CERNin tutkijayhteisössä. Hän esitteli tiedonhallintaan liittyvän ehdotuksensa seuraavin loppusanoin:

"We should work toward a universal linked information system, in which generality and portability are more important than fancy graphics techniques and complex extra facilities."(Berners-Lee 1989)

Berners-Leen ehdotus johti alkuperäisen World Wide Webin syntymiseen. WWW:n alkuvaiheelle tyypillisiä piirteitä ovat staattiset verkkosivut ja hyperlinkkien yhdistämät dokumentit, joiden sisällön julkaisemisesta vastaa verkkosivustoa ylläpitävä taho. Käyttäjillä oli sivustoilla käytännössä ainoastaan lukuoikeus. Webin ensimmäiseen vaiheeseen viitataan usein termillä Web 1.0. (Nath, Dhar ja Basishtha 2014)

WWW:n toiselle aikakaudelle, Web 2.0:lle, on ominaista interaktiivisemmat ja yhteisöllisemmät verkkosivustot, joissa käyttäjät osallistuvat myös sisällöntuottoon. Esimerkiksi sosiaalisen median alustat, keskustelufoorumit ja verkkoblogit kuvastavat Web 2.0:n aikakautta, jonka katsotaan ajoittuvan 2000-luvun alkupuolelta nykypäivään (O'reilly 2007).

Vuonna 2014 Ethereum-kryptovaluutan toinen perustajajäsen, Gavin Wood, visioi WWW:n seuraavan kehitysvaiheen perustuvan lohkoketjupohjaisiin ratkaisuihin, jonka keskiössä ovat mm. riippumattomuus keskinäisestä luottamuksesta, salattu tiedon julkaisujärjestelmä ja järjestelmän ylläpitoon insentivointi. Kannustinrakennetta voidaan verrata pienemmässä mittakaavassa jo käytössä olevaan BitTorrent-protokollaan, jossa tiedostoja lataavat käyttäjät osal-

listuvat samanaikaisesti myös tiedostojen jakamiseen, mikä mahdollistaa suuremmat tiedonsiirtonopeudet. Wood (2014). Hajautettuun ylläpitoon, sensuurinkestävyyteen ja datan omistusoikeuteen nojaavasta kehityssuunnasta puhutaan yleisesti termillä Web 3.0 (lyhyemmin Web3).

2.2 Webin nykyrakenteen ongelmat ja haavoittuvuudet

Internetin tarjoamat palvelut ja alustat ovat nykymuotoisena luonteeltaan keskitettyjä. Internetsivustojen toiminta ja ylläpito tapahtuu WWW-palvelimilla, datan säilytykseen käytetään erillistä tietokantaa ja myös verkkosivustojen haut tapahtuvat DNS-nimipalvelinten kontrolloimana. Vaikka DNS itsessään on hajautettu järjestelmä, on suuryrityksillä, kuten Googlella, Amazonilla ja Cloudflarella, merkittävä osuus julkisista DNS-nimipalvelimista (Moura ym. 2020). Kaikkea internetissä tapahtuvaa toimintaa voidaan ohjata tai rajoittaa näitä palveluita ylläpitävien tahojen toimesta. Verkkosivun, palvelun tai sovelluksen käytön edellytyksenä on kaikkien ylläpitävien osasten yhteistyö. Keskitetty rakenne tekee järjestelmistä kuitenkin alttiita tietoturvauhille, kuten palvelunestohyökkäyksille ja tietovuodoille. Esimerkkejä lähihistoriasta löytyy useita.

Vuonna 2019 haavoittuvuus Facebook-yhteisöpalvelussa johti yli 530 miljoonan käyttäjän tietojen vuotamiseen, näiden joukossa oli noin 1,2 miljoonaa suomalaista (Kyberturvallisuuskeskus 2021). Myös Playstation Networkin hakkerointi keväällä 2011 aiheutti lähes kuukauden käyttökatkoksen Playstationin verkkopalveluissa sekä tämän lisäksi 77 miljoonan käyttäjän henkilötietojen vuotamisen (The Guardian 2011). Suurin tietovuoto tapahtui 2013 Yahoolle, kun hakkerit saivat haltuunsa yli miljardin käyttäjätilin tiedot. Hakkeroinnista tiedotettiin vasta seuraavana vuonna (The Guardian 2016).

Vaikka mainittuihin tapahtumiin johtaneita syitä on useita, on käyttäjätunnusten ja datan säilöminen keskitetyillä palvelimilla ja tietokannoissa yksi tietovuodot mahdollistanut tekijä. Ihmisten arkaluontoisten tietojen ollessa nykyisin lähes kokonaan sähköisessä muodossa, korostuu tietoturvan merkitys näiden tietojen säilömisessä. Yhdysvaltalaisen luottotietoyritys Equifaxin vuoden 2017 tietomurron yhteydessä Equifaxin tietokannoista vietiin 143 miljoonan amerikkalaisen tietoja, joiden joukossa oli muun muassa henkilötunnuksia, osoitteita

sekä ajo- ja luottokorttien numeroita. Kyseisestä tapahtumasta laaditun raportin mukaan hakkerit pääsivät yrityksen verkkoon murtauduttuaan käsiksi useisiin tietokantoihin. Asiakastietojen keskitetyn saatavuuden lisäksi tietovuodon laajuuteen vaikuttivat muun muassa yrityksen laiminlyömät tietoturvapäivitykset sekä yrityksen verkon segmentoinnin puute. (“The Equifax Data Breach” 2018)

2.3 Riippuvuus kolmannesta osapuolesta

Webin rakenteen lisäksi lukuisat arkipäivän palvelut riippuvat kolmannesta osapuolesta. Verkkokaupat, sähköiset maksujärjestelmät, sosiaalisen median alustat, äänestysjärjestelmät sekä matka- ja majoitusvarauspalvelut ovat vain muutama esimerkki riippuvuudesta luotetun kolmannen osapuolen toimintaan. Käyttäjän kannalta helpomman käytettävyyden vastapainona on usein vähentynyt yksityisyys ja varsinaisen palvelun ulkopuoliset ansaintamallit. Mielenkiinnon kohteisiin ja selailukäyttäytymiseen perustuva kohdennettu mainonta on mainostajan näkökulmasta hyödyllistä, mutta käyttäjä ei usein ole tietoinen kaikesta kerätystä datasta (Toubiana ym. 2010). Luottokorttivarkauden tapahtuessa on rikoksen uhrin edun mukaista, että pankki voi tarvittaessa kuolettaa varastetun kortin ja estää maksuliikenteen. Mahdollisuus asiakkaiden tilien hallinnointiin voi kuitenkin johtaa myös tarpeettomaan tilin sulkemiseen sekä mahdollisiin taloudellisiin tappioihin (MTV Uutiset 2017).

3 Lohkoketju

Hajautus on toistuva teema webin seuraavaa kehitysvaihetta tarkasteltaessa. Käyttäjälähtöisen, hajautetusti ylläpidetyn, luotettavan ja turvallisen webin kehitys vaatii uudistuksia myös olemassa oleviin tietorakenteisiin. Lohkoketjuteknologia tarjoaa perusominaisuuksiensa puolesta potentiaalisen vaihtoehdon ja onkin usein keskeisessä roolissa Web 3.0:n ympärillä olevassa keskustelussa.

3.1 Määritelmä

Lohkoketju on eräänlainen hajautettu tietorakenne, jossa transaktiot ja data tallennetaan lohkoihin, eivätkä ne ole muutettavissa. Lohkoketjun ylläpito ja toimintaperiaatteet määrittyvät konsensusalgoritmin perusteella, mistä tunnetuimpana esimerkkinä on Bitcoinin lohkoketjussakin käytettävä Proof of Work (Nakamoto 2008), joka tunnetaan yleisemmin louhintana. Kun lohkoketjussa tapahtuu transaktio, se todennetaan verkkoon osallistuvien toimesta ketjun viimeiseksi lisättävään lohkoon. Konsensusalgoritmeja on nykyisin useita, mutta yhdistävänä tekijänä on transaktioiden sekä datan validoinnista yleensä kryptovaluutan muodossa saatava palkkio, joka toimii kannustimena verkon ylläpitoon liittymiseen. Ylläpitoon osallistuminen vaatii yleensä joko tietokoneen laskentatehoa tai tiettyä osuutta ylläpidettävän lohkoketjun kryptovaluutasta.

3.2 Historiaa

Terminä lohkoketju sai alkunsa 2008 luodusta virtuaalivaluutta Bitcoinista. Bitcoin: A Peer-to-Peer Electronic Cash System -dokumentin kirjoittanut, pseudonyymiä "Satoshi Nakamoto" käyttävä henkilö, kuvasi tekniikkaa lohkoista muodostuvana ketjuna, joka vakiintui myöhemmin lohkoketjuksi. Bitcoin ja lohkoketjuteknologia luotiin vastaamaan digitaalisen rahan ongelmiin (Nakamoto 2008). Riippuvuus kolmannesta osapuolesta, kuten pankeista ja maksupalveluntarjoajista, maksuvälineiden väärinkäytön ja petosten kasvu sekä digitaalisen rahan rajattoman luomisen aikaansaama inflaatio ovat esimerkkejä epäkohdista, joihin uusi virtuaalivaluutta pyrki vastaamaan.

2014 Vitalik Buterinin toimesta syntynyt Ethereum on Bitcoinin tapaan julkinen lohkoketju, joka lisäsi koodin suorittamisen mahdollisuuden lohkoketjussa. Buterinin mukaan Ethereum on alusta älysopimuksille ja hajautetuille sovelluksille. Älysopimuksilla viitataan lohkoketjussa olevalle ohjelmakoodille, joka suorittaa ennalta määrättyjä tehtäviä tiettyjen ehtojen täyttyessä. Älysopimuksia voidaan käyttää esimerkiksi datan tai kryptovaluutan siirtoon, automatisoituun maksunkäsittelyyn, digitaalisten äänestysten toteuttamiseen tai ohjelmoidun tokenin luontiin. Muita käyttötarkoituksia Ethereumille ovat mm. hajautetut autonomiset organisaatiot (DAO) ja hajautettu tiedostontallennus. (Buterin 2014). Buterin itse luonnehti Ethereumin olevan "kuin hajautettu käyttöjärjestelmä lohkoketjulle"(Digital Finance 2017, käännös minun). Ethereumin menestyksen seurauksena älysopimuksia hyödyntävien lohkoketjujen määrä kasvoi merkittävästi, mutta Ethereum on tämän tutkielman kirjoitushetkellä edelleen ekosysteemiin kiinnitetyn arvon (total value locked) mukaan mitattuna selkeästi suurin lohkoketju (Coinmarketcap 2023).

3.3 Mikä tekee lohkoketjuteknologiasta tietoturvallisen ja luotettavan?

Lohkoketju muodostuu aikajärjestyksessä olevista lohkoista, jotka sisältävät transaktiodatan (esim. kryptovaluutan siirto, älysopimus yms.) lisäksi muun muassa aikaleiman, yksilöllisen kryptografisen tiivisteen ja tiedon edellisen lohkon kryptografisesta tiivisteestä. Lohkot lisätään ketjuun lohkoketjulle ominaisen konsensusmekanismin määrittämin säännöin. Konsensusmekanismi lohkoketjuissa viittaa menetelmään, jonka avulla lohkoketjun ylläpitoon osallistuvien kesken päätetään, mitkä tapahtumat tai lohkot hyväksytään ja lisätään lohkoketjuun. Esimerkiksi Bitcoin-lohkoketjussa käytetään paljon laskentatehoa vaativaa Proof of Work -algoritmia (Nakamoto 2008). Lohkoketjuun lisätyn lohkon tiedot ovat pysyviä ja varmennettavissa. Tämän lisäksi lohkoketjun toiminta ei hajautetun rakenteensa johdosta ole riippuvainen yksittäisistä solmuista, vaan kopio lohkoketjun tilasta on jokaisella lohkoketjun ylläpitoon osallistuvalla. Zhang, Xue ja Liu tiivistävät julkaisussaan lohkoketjun toimivan turvallisena ja hajautettuna tilikirjana, joka arkistoi kaikki kahden osapuolen väliset transaktiot tehokkaasti, pysyvästi ja todennettavalla tavalla (Zhang, Xue ja Liu 2019, s. 3).

4 Uuden teknologian puutteet ja haasteet nykymuodossaan

Lohkoketjuteknologialla on suuresta potentiaalistaan huolimatta useita puutteita nykyisessä tilassaan. Näistä puutteista johtuen uuden teknologian käyttöönotto on ollut eri aloilla hidasta. Tässä kappaleessa käsitellään lohkoketjujen keskeisiä haasteita.

4.1 Skaalautuvuus

Jo Ethereumin syntyvaiheessa Vitalik Buterin listasi yhdeksi huolenaiheeksi lohkoketjun skaalautumisen (Buterin 2014, s. 33). Jokainen lohkoketjussa tapahtuva transaktio prosessoidaan lohkoketjun ylläpitoon osallistuvien solmupisteiden (eng. node) toimesta ja lohkoketjun koko kasvaa vastaavasti jokaisen transaktion myötä. Lohkoketjun koon kasvaessa on todennäköistä, että koko lohkoketjun historian säilyttävien ja ylläpitoon osallistuvien täyssolmujen (eng. full node) määrä vähenisi ja keskittyisi yksittäisten tahojen vastuulle, mikä puolestaan tekisi lohkoketjun ylläpidosta keskitetympää ja altistaisi sen muun muassa 51% hyökkäyksille, jossa yli puolet lohkoketjua ylläpitävistä solmuista voivat yhteisestä päätöksestä estää normaalien transaktioiden tapahtumisen, peruuttaa jo tapahtuneita transaktioita tai vaihtoehtoisesti aiheuttaa aikaisemman transaktion uudelleenlähetyksen.

Olennainen osa lohkoketjun skaalautuvuutta on sen transaktioiden käsittelynopeus, jota mitataan arvolla TPS (Transactions Per Second). Imran Bashir mainitsee (Bashir 2020, s. 1206) julkisten lohkoketjujen, kuten Bitcoinin ja Ethereumin, olevan hitaita, eivätkä ne suorituskykynsä puolesta sovellu käytettäväksi esimerkiksi maksujärjestelmissä, jotka vaativat tuhansien transaktioiden käsittelynopeuden sekunnissa. Bashir kertoo Bitcoinin käsittelynopeuden olevan 3-4 TPS ja Ethereumin noin 14 TPS luokkaa, josta ne eivät nykyhetkeen mennessä ole parantuneet huomattavasti, vaikka arviot kyseisten lohkoketjuen maksiminopeudesta hieman vaihtelevatkin. Suorituskyvyn ja skaalautuvuuden rajoitteisiin liittyy myös lohkoketjun kohonneet transaktiokulut. Kulut vaihtelevat kiireisinä aikoina merkittävästi myös vuorokauden eri aikoina (Cointelegraph 2021).

Skaalautuvuuden parantaminen on lohkoketjujen keskeinen kehityskohde, johon lohkoketjujen parissa työskentelevät tahot ovat suunnitelleet ja toteuttaneet useita ratkaisuja. Yksi Ethereumin lähestymistavoista skaalautuvuuden parantamiseksi on esimerkiksi toisen kerroksen skaalaus (eng. Layer 2 scaling), jossa osa toiminnallisuudesta ja transaktioista suoritetaan sivuketjussa vähentäen pääketjun rasitusta (ethereum.org 2023b).

4.2 Lohkoketjun turvallisuus

Vaikka lohkoketjuteknologia tuo mukanaan monia turvallisuusetuja, liittyy siihen samalla myös tiettyjä turvallisuusuhkia. Näistä suurimmaksi Mosakheil mainitsee tutkielmassaan 51% hyökkäyksen. 51% hyökkäyksellä viitataan tilanteeseen, jossa hyökkääjä saa haltuunsa vähintään 51 prosenttia lohkoketjun ylläpidosta vastaavien solmujen laskentatehosta, mikä mahdollistaa mm. transaktioiden uudelleenlähetyksen, peruutuksen tai uusien transaktioiden todentamisen estämisen (Mosakheil 2018, s.62-64). Käytännön tasolla kyseinen hyökkäys on kuitenkin suurimpien lohkoketjujen kohdalla äärimmäisen hankalaa ja vaatisi taloudellisesti valtavan panostuksen. Esimerkiksi Proof of Work -konsensusmekanismia käyttävien lohkoketjujen, kuten Bitcoinin, laskentatehovaatimukset kasvavat verkon laajenemisen myötä ja ajan kuluessa 51% hyökkäyksen toteutus hankaloituu entisestään (www.ledger.com 2022). Bitcoinin historiassa ei olekaan yhtään onnistuneesti siihen kohdistunutta 51% hyökkäystä.

Älysopimusten ohjelmoinnin mahdollisuus laajensi lohkoketjujen käyttömahdollisuuksia, mutta lisäsi samanaikaisesti lohkoketjuteknologiaan liittyvien turvallisuusuhkien määrää. Huang, Bian, Li, Zhao ja Shi (2019) luettelevat älysopimusten tietoturvaa käsittelevässä julkaisuussaan haavoittuvuuksien voivan johtaa esimerkiksi seuraavanlaisiin tilanteisiin:

- saldon toistuva lähetys
- sopimuksen tarkoitukseton tuhoutuminen ja varojen siirtyminen ei-valtuutetulle tilille
- lähetetyn rahan jääminen lukittuun tilaan
- palvelunestohyökkäys käynnissä olevaan sopimukseen

Älysopimuksia on hankala paikata jälkikäteen ja Huang ym. painottavatkin älysopimuskehityksessä testauksen ja tietoturva-auditoinnin merkitystä ennen käyttöönottoa. (Huang ym. 2019)

4.3 Lohkoketjujen trilemma

Lohkoketjujen trilemma viittaa haasteeseen, jossa on vaikea saavuttaa samanaikaisesti kolme keskeistä ominaisuutta: hajautus, turvallisuus ja skaalautuvuus. Hajautettu ja turvallinen lohkoketju ei ole helposti skaalattavissa, turvallinen sekä skaalautuva lohkoketju on toteutettavissa helpoiten ilman hajautusta, hajautettu ja skaalautuva lohkoketju on helpommin altis turvallisuusriskeille. (ethereum.org 2023a) Ratkaisu lohkoketjujen trilemmaan tekisi lohkoketjuteknologiasta käyttökelpoisemman useille sovellusalueille ja houkuttelevamman vaihtoehdon otettavaksi käyttöön myös perinteisissä liiketoimintaympäristöissä.

5 Lohkoketjujen rooli Web 3.0:n kehityksessä

5.1 Toimialat, joissa uusi teknologia on jo käytössä

Lohkojetjupohjaisia ratkaisuja on käytössä jo useilla eri toimialoilla ja kiinnostus lohkoketjuteknologiaa kohtaan kasvaa jatkuvasti. Toimitusketjut ovat olleet suosittu kohde uuden teknologian hyödyntämiselle ja lohkoketjuja onkin otettu käyttöön mm. helpottamaan ruuantuotannon monitorointia ja ruuan alkuperän todentamista (IBM 2023) sekä koronapandemian rokotetoimitusten seurannassa (Reuters 2021). Ethereumin alkuperäisessä visiossa mainittu hajautettu tietovarasto oli usean vuoden ajan teorian tasolla, mutta viime vuosina lohkoketjuyritykset ovat onnistuneet vision toteutuksessa, mikä tarkoittaa mahdollisuutta tiedostojen hajautettuun taltiointiin järjestelmässä, jonka ylläpitoon osallistuvat käyttäjät hyötyvät myös kryptovaluutan muodossa ylläpidosta (Storj 2023). Pilvi- ja verkkoisännöintipalvelut ovat looginen käyttökohde lohkoketjualustojen piirissä siirryttäessä kohti hajautetumpaa Web 3.0 -kehitysvaihetta. Useat lohkoketjuyritykset pyrkivät luomaan edullisemman, nopeamman ja turvallisemman ratkaisun suosittujen palveluiden, kuten AWS:n tai Google Cloudin, rinnalle ja nettisivuja sekä sovelluksia onkin jo mahdollista julkaista hajautetun vaihtoehdon piirissä (Flux Cloud 2023).

5.2 Potentiaaliset käyttökohteet

Sähköisen äänestyksen yleistyessä luotettavan äänestysjärjestelmän sekä äänestäjän henkilöllisyyden varmentamisen tarve korostuu. Benabdallah ym. (2022) tutkivat lohkoketjuteknologiaa kiinnostavana vaihtoehtona sähköisen äänestysjärjestelmän toteutukselle, joka olisi ominaisuuksiltaan mm. julkinen, yksilöllisesti todennettava, luotettava, toimintavarma, tunnistautumisen ja anonymiteetin mahdollistava sekä samalla vaalivilpin mahdollisuutta vähentävä ratkaisu. Lohkoketjujen käyttöä äänestyksen järjestämisessä ei kuitenkaan toistaiseksi ole testattu laajassa mittakaavassa. (Benabdallah ym. 2022)

Singh, Singh ja Kim (2018) tutkivat lohkoketjujen hyödyntämistä esineiden internetissä (IoT) ja kokevat sen varteenotettavana vaihtoehtona IoT-laitteiden välisessä kommunikoinnissa

yhä useampien kotitalouksien laitteiden ollessa yhdistettynä internetiin. IoT:n alakategoriaksi luonnehdittava ajoneuvojen internet (eng. Internet of Vehicles, IoV) mahdollistaa esimerkiksi itseohjautuvien autojen käytön, mutta itseohjautuvien ajoneuvojen käyttö laajemmassa mittakaavassa vaatii IoV-infrastruktuurilta ehdotonta turvallisuutta ajoneuvojen ja sensoreiden välisessä kommunikoinnissa. Narbayeva ym. (2020) näkevät lohkoketjuteknologialla tutkimuksessaan potentiaalia parantaa useita osa-alueita ajoneuvojen internetissä esimerkiksi liikenneturvallisuuteen, luotettavaan datansiirtoon ja kyberhyökkäyksien estämiseen liittyen.

Lohkoketjuissa toimivat kryptovaluutat voivat tarjota vaihtoehtoisen tavan perinteisille valuutoille ja maksujärjestelmille Nakamoton alkuperäisen vision mukaisesti (Nakamoto 2008). Esimerkiksi kryptovaluuttoja maksutapana hyväksyvien verkkokauppojen määrä on kasvanut lähivuosina, mutta vastoin Bitcoinin luonnissa keskeisenä nähtyä riippumattomuutta kolmannesta osapuolesta, tapahtuvat kryptovaluuttamaksujen käsittelyt useimmissa tapauksissa vielä erillisen maksupalveluntarjoajan kautta. Lohkoketjujen käyttö on nostettu esiin myös mm. digitaalisen euron kohdalla, vaikka kyseessä onkin suunnitelma digitaalisesta keskuspankkirahasta (Euroopan keskuspankki 2023).

5.3 Tulevaisuusnäkymät

Siirtyminen kohti Web 3.0:n aikakautta tapahtuu vaiheittain, eikä vaadi nykyisten järjestelmien täysmittaista korvaamista lohkoketjupohjaisilla, hajautetuilla järjestelmillä. Nämä voivat myös täydentää toisiaan. Esimerkiksi Benabdallah ym. (2022) äänestysjärjestelmiä tarkastelevassa julkaisussa mainitaan esimerkkinä lohkoketjujen käyttö paperiäänien laskemisessa kunnan tai äänestysalueen tasolla, vaikka maanlaajuisten vaalien järjestämisessä ja äänioikeutettujen luettelon laatimisessa edellytettäisiinkin keskitettyä viranomaistahoa (Benabdallah ym. 2022). Bitcoinin alkuajoista lähtien toistuneet uutiset kryptovaluutan käytöstä rahanpesun ja huumausainekaupan välineenä sekä kryptopörsseihin kohdistuneet hakkeroinnit (CNN Business 2018) ovat osaltaan hidastaneet laajempaa hyväksyntää kryptovaluutan takana toimivaa uutta teknologiaa kohtaan. Useat suuret yritykset, kuten Microsoft (2023), Google (2023) ja MongoDB Inc. (2023) ovat kuitenkin mukana Web 3.0:n kehittämisessä ja ovat myös ottaneet käyttöön lohkoketjuja hyödyntäviä ratkaisuja, mikä osoittaa aitoa kiinnostusta lohkoketjuihin ja niiden tuomiin mahdollisuuksiin teknologisen kehityksen saralla.

Lähteet

Bashir, Imran. 2020. *Imran Bashir (2020). Mastering Blockchain : A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition.* Packt Publishing.

Benabdallah, Ali, Antoine Audras, Louis Coudert, Nour El Madhoun ja Mohamad Badra. 2022. “Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review”. *IEEE Access* 10:70746–70759. https://doi.org/10.1109/ACCESS.2022.3187688.

Berners-Lee, Tim. 1989. “Information Management: A Proposal”. Viitattu 24. tammikuuta 2024. https://www.w3.org/History/1989/proposal.html.

———. 2016. “Keynote Address: Tim Berners-Lee – "Re-decentralizing the web - some strategic questions"”. Viitattu 17. joulukuuta 2023. https://2016.decentralizedweb.net/.

Buterin, Vitalik. 2014. *Ethereum White Paper, A Next-Generation Smart Contract and Decentralized Application Platform.* https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.

CNN Business. 2018. “$530 million cryptocurrency heist may be biggest ever”. Viitattu 17. joulukuuta 2023. https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html.

Coinmarketcap. 2023. “Largest Blockchains in Crypto Ranked by TVL”. Viitattu 24. tammikuuta 2024. https://coinmarketcap.com/chain-ranking/.

Cointelegraph. 2021. “Here are the best and worst times of the day to use Ethereum”. Viitattu 3. tammikuuta 2024. https://cointelegraph.com/news/here-are-the-best-and-worst-times-of-the-day-to-use-ethereum.

Digital Finance. 2017. “What is Ethereum? Vitalik Buterin explained it as...” Viitattu 5. joulukuuta 2023. https://www.digfingroup.com/what-is-ethereum/.

ethereum.org. 2023a. “A digital future on a global scale: The challenge of decentralized scaling”. Viitattu 20. tammikuuta 2024. https://ethereum.org/en/roadmap/vision/.

ethereum.org. 2023b. “LAYER 2”. Viitattu 20. tammikuuta 2024. https://ethereum.org/en/layer-2/.

Euroopan keskuspankki. 2023. “Kysyttyä digitaalisesta eurosta”. Viitattu 17. joulukuuta 2023. https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb.faq_digital_euro.fi.html.

Flux Cloud. 2023. Viitattu 15. joulukuuta 2023. https://runonflux.io/.

Google. 2023. “Blockchain Node Engine”. Viitattu 17. joulukuuta 2023. https://cloud.google.com/blockchain-node-engine.

Huang, Yongfeng, Yiyang Bian, Renpu Li, J. Leon Zhao ja Peizhong Shi. 2019. “Smart Contract Security: A Software Lifecycle Perspective”. *IEEE Access* 7:150184–150202. https://doi.org/10.1109/ACCESS.2019.2946988.

IBM. 2023. “IBM Food Trust”. Viitattu 14. joulukuuta 2023. https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust.

Kyberturvallisuuskeskus. 2021. “Facebookin vuonna 2019 varastettuja tietoja julkaistu - mukana 1,2 miljoonan suomalaisen tiedot”. Viitattu 3. joulukuuta 2023. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/facebookin-vuonna-2019-varastettuja-tietoja-julkaistu-mukana-12-miljoonan-suomalaisen.

Microsoft. 2023. “Supply Chain Blockchain Initiative”. Viitattu 17. joulukuuta 2023. https://www.microsoft.com/en-us/garage/wall-of-fame/supply-chain-blockchain-initiative/.

MongoDB Inc. 2023. “Blockchain Database: A Comprehensive Guide”. Viitattu 17. joulukuuta 2023. https://www.mongodb.com/databases/blockchain-database.

Mosakheil, Jamal Hayat. 2018. “Security threats classification in blockchains”, https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1093&context=msia_etds.

Moura, Giovane CM, Sebastian Castro, Wes Hardaker, Maarten Wullink ja Cristian Hesselman. 2020. “Clouding up the internet: How centralized is dns traffic becoming?” Teoksessa *Proceedings of the ACM Internet Measurement Conference,* 42–49.

MTV Uutiset. 2017. “Helsinkiläismiehen tilit suljettiin varoittamatta epäilyttävän rahaliikenteen vuoksi: "Voi johtaa pienyrittäjällä isoihin tappioihin"”. Viitattu 21. joulukuuta 2023. https://www.mtvuutiset.fi/artikkeli/helsinkilaismiehen-tilit-suljettiin-varoittamatta-epailyttavan-rahaliikenteen-vuoksi-voi-johtaa-pienyrittajalla-isoihin-tappioihin/6523282.

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf.

Narbayeva, Saltanat, Timur Bakibayev, Kuanysh Abeshev, Irina Makarova, Ksenia Shubenkova ja Anton Pashkevich. 2020. “Blockchain technology on the way of autonomous vehicles development”. *Transportation Research Procedia* 44:168–175.

Nath, Keshab, Sourish Dhar ja Subhash Basishtha. 2014. “Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges”. Teoksessa *2014 International Conference on Reliability Optimization and Information Technology (ICROIT),* 86–89. https://doi.org/10.1109/ICROIT.2014.6798297.

O’reilly, Tim. 2007. “What is Web 2.0: Design patterns and business models for the next generation of software”. *Communications & strategies,* numero 1, 17.

Reuters. 2021. “British hospitals use blockchain to track COVID-19 vaccines”. Viitattu 20. tammikuuta 2024. https://www.reuters.com/technology/british-hospitals-use-blockchain-track-covid-19-vaccines-2021-01-19/.

Singh, Madhusudan, Abhiraj Singh ja Shiho Kim. 2018. “Blockchain: A game changer for securing IoT data”. Teoksessa *2018 IEEE 4th World Forum on Internet of Things (WF-IoT),* 51–55. https://doi.org/10.1109/WF-IoT.2018.8355182.

Storj. 2023. Viitattu 20. tammikuuta 2024. https://www.storj.io/how-it-works.

“The Equifax Data Breach”. 2018. Viitattu 1. joulukuuta 2023. https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

The Guardian. 2011. “PlayStation Network hackers access data of 77 million users”. Viitattu 1. joulukuuta 2023. https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data.

The Guardian. 2016. “Yahoo hack: 1bn accounts compromised by biggest data breach in history.” Viitattu 1. joulukuuta 2023. https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

Toubiana, Vincent, Arvind Narayanan, Dan Boneh, Helen Nissenbaum ja Solon Barocas. 2010. “Adnostic: Privacy preserving targeted advertising”. Teoksessa *Proceedings Network and Distributed System Symposium.*

Wood, Gavin. 2014. “Insights into a Modern World: ĐApps: What Web 3.0 Looks Like”. Viitattu 4. joulukuuta 2023. https://gavwood.com/dappsweb3.html.

www.ledger.com. 2022. Viitattu 16. joulukuuta 2023. https://www.ledger.com/academy/glossary/51-attack.

Zhang, Rui, Rui Xue ja Ling Liu. 2019. “Security and privacy on blockchain”. *ACM Computing Surveys (CSUR)* 52 (3): 1–34.