Tampereen yliopisto

Henry Andersson

# LOHKOKETJUTEKNOLOGIAN HYÖDYNTÄMINEN ELEKTRONISISSA ÄÄNESTYSJÄRJESTELMISSÄ

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Lokakuu 2022

# TIIVISTELMÄ

Henry Andersson: Lohkoketjuteknologian käyttäminen elektronisissa äänestysjärjestelmissä
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Lokakuu 2022

---

Tässä tutkielmassa tarkastellaan lohkoketjupohjaisen elektronisen äänestysjärjestelmän vaatimuksia. Tutkimusmuotona on kirjallisuuskatsaus, tutkimuksessa havainnollistetaan, miten lohkoketjuteknologioita voi käyttää elektronisissa äänestysjärjestelmissä. Kirjallisuuskatsauksessa nousi esiin jo käytössä olevia järjestelmiä, sekä tutkimuksissa ehdotettuja järjestelmiä, joista poimitaan yhtäläisyyksiä ja eroja, sekä pohditaan niitä. Yhdeksi keskeisimmistä asioista nousi esiin äänestäjän yksityisyyden ja vaalisalaisuuden turvaaminen sekä tulosten läpinäkyvyys, joka on mahdollista toteuttaa lohkoketjuteknologioita käyttämällä. Ehdotetuissa järjestelmissä äänestäjän tiedot salataan eri metodein, suosituin oli Paillier homomorfinen salaustapa, joka varmistaisi, ettei mahdollinen hyökkääjä näkisi äänestäjästä kuin salatun tiedon.

Nykyisten äänestysjärjestelmien tyyppejä ja niihin liittyviä ongelmia selvitettiin, ja erityisesti elektronisiin äänestyslaitteisiin osoittautui olevan huono luottamus. Niiden ongelmana on peukalointi, toimintahäiriöt ja väärinkäytökset. Ne käyttävät usein myös keskitettyä tietokantaa, joka mahdollistaa hakkerille tavan muuttaa suuria määriä ääniä samanaikaisesti. Nämä äänet eivät ole muuttumattomia ja äänten lasku ei ole läpinäkyvää. Paperiset äänestykset ovat turvassa näiltä uhilta, mutta niihin liittyy logistisia ongelmia, sekä korkea hinta ja äänten laskun hitaus. Etelä-Koreassa, Japanissa ja Moskovassa on kokeiltu lohkoketjun käyttämistä äänestyksessä ja Virossa on ääniä aloitettu tallentamaan lohkoketjuihin.

Lohkoketjun toiminta takaa muuttumattoman rakenteen, jolloin äänet ovat turvassa perinteiseltä hakkeroinnilta siten, ettei annettuja ääniä pystyy muuttamaan. Lohkoketjun ollessa myös hajautettu, ei voi hyökkääjä kohdistaa hyökkäystään yhteen tietokantaan, vaan hänen on saatava 51 % ketjun laskentatehosta haltuunsa muuttaakseen ketjua, joka on kallista ja suurissa ketjuissa käytännössä mahdotonta. Äänestysjärjestelmissä lohkoketjun on hyvä olla salattu, kunnes vaalit ovat päättyneet, jolloin ketju on tuotava julkiseksi, jolloin läpinäkyvyys saadaan toteutettua. On kuitenkin varmistettava, ettei äänestäjien dataa ole mahdollista selvittää tästä avoimesta ketjusta.

Avainsanat: Lohkoketju, äänestäminen, äänestysjärjestelmät, vaalit.

# SISÄLLYSLUETTELO

# 1 Johdanto

Tässä tutkielmassa havainnollistetaan voiko lohkoketjuteknologioita käyttää hyödyksi elektronisten äänestysjärjestelmien suunnittelussa, ja mitä vaatimuksia tällaiselle järjestelmälle on. Vaalit ja äänestäminen on demokraattisen yhteiskunnan kulmakivi, ja tutkimuksessa on tarkoitus selvittää voiko lohkoketjuteknologiaa hyödyntää elektronisten äänestysjärjestelmien kehittämisessä turvallisemmiksi ja läpinäkyvimmiksi. Aiheesta on tehty joitain tutkimuksia ja käytännön kokeiluja. Näissä järjestelmissä on havaittavissa yhtenäisiä teemoja ja tavoitteita, mutta monet ehdotetuista järjestelmistä poikkeavat toisistaan teknisellä toteutustasolla, usein riippuen tietyn maan vaalien vaatimuksista. Järjestelmää on muokattava sopivaksi jokaiselle vaalille, eikä ole kannattavaa pyrkiä tekemään yhtä järjestelmää, jota käytettäisiin kaikissa vaaleissa, vaan ohjeistuksia ja teknisiä vaatimuksia, joilla järjestelmää voidaan muokata erilaisten vaalien vaatimusten perusteella. Tämän tutkimuksen tavoitteena on havainnollistaa ja tuoda yhteen eri järjestelmien piirteitä ja sitä kautta järjestelmän vaatimuksia. Tämän tutkimuksen tutkimusmenetelmä on kirjallisuuskatsaus.

Toisessa luvussa käydään läpi erilaisia käytössä olevia äänestysjärjestelmiä ja havainnollistetaan niiden hyötyjä ja ongelmia. Kolmannessa luvussa käydään läpi lohkoketjun toiminnan ja sen piirteitä. Neljännessä luvussa käydään läpi jo olemassa olevia tai ehdotettuja lohkoketjuteknologiaan pohjautuvia äänestysjärjestelmiä. Viidennessä luvussa tuodaan yhteen eri järjestelmien ominaisuuksia, ja havainnollistetaan lohkoketjuteknologiaan perustuvan elektronisen äänestysjärjestelmän vaatimuksia ja siihen mahdollisesti liittyviä ongelmia. Kuudes kappale on yhteenveto.

# 2 Käytössä olevia äänestysjärjestelmiä

Käytössä olevat äänestysjärjestelmät voidaan jakaa karkeasti kahteen tyyppiin, kirjeäänestykseen ja elektroniseen äänestykseen. Molempiin tyyppeihin liittyy omat vahvuudet ja heikkoudet, jotka on otettava huomioon järjestelmää suunniteltaessa ja käytettäessä. On myös mahdollista käyttää järjestelmää, joka hyödyntää molempia tyyppejä mutta tällaisen järjestelmä ei ole kovin yleinen ja lisäksi se on kallis. Eri maissa on käytössä erilaisia järjestelmiä riippuen maan vaalien vaatimuksista. Suuremmissa maissa on käytössä usein elektronisia järjestelmiä sillä kirjeäänestys olisi liian hidasta ja logistisesti kallista, kun taas pienemmissä maissa suositaan edelleen kirjeäänestystä, sillä siihen on yleisesti korkeampi luotto kuin elektronisiin järjestelmiin.

## 2.1 Kirjeäänestys

Monissa maissa, kuten suomessa, on edelleen käytössä kirjeäänestys eli paperiset laput, jonka avulla äänestäjä antaa äänensä haluamalleen ehdokkaalle. Kirjeäänestykseen on yleisesti kovempi luottamus kuin elektroniseen äänestykseen (Evans ja Paul, 2004), mutta kirjeäänestys on logistisesti kallista ja haastavaa sekä vaatii paljon työntekijöitä joka tekee tästä äänestystavasta kallista (Khan ja Rasheed, 2021). Etenkin suurissa maissa kirjeäänestys on hankala toteuttaa (Mols, vasilomanolakis, 2020).

Kirjeäänestyksessä yksi ongelma on myös äänen pilaantuminen (engl. ballot spoiling), eli äänestyslappua ei voida laskea äänenä sillä siinä on joko vahingossa tai tahallisesti aiheutettuja puutteellisia tai ylimääräisiä merkintöjä, jotka mitätöivät äänen. (Wolf, Nackerdien, Tuccinardi, 2011) Ääniä voidaan pilata tahallisesti joko protestina esimerkiksi antamalla tyhjä ääni tai tahallisesti esimerkiksi äänten laskussa pilata tietyn ehdokkaan ääniä, jolloin näitä ääniä ei voida laskea, ja näin yrittää vaikuttaa vaalien lopputulokseen. Kirjeäänestystä pidetään kuitenkin turvallisena jollei turvallisimpana äänestysmenetelmänä, sillä äänten manipuloiminen on iso työ ja vaatii fyysisen pääsyn ääniin ja äänten muuttamisen tai pilaamisen yksi kerrallaan.

## 2.2 Elektroninen äänestys

Elektroniset äänestyslaitteet ovat monissa maissa käytössä oleva fyysinen laite tai laitteiden yhdistelmä, jota käytetään äänestämiseen. Laite rekisteröi, tallentaa ja laskee äänet automaattisesti äänestyksen aikana, jolloin niiden käyttäminen on kirjeäänestyksen paperilappuihin verrattuna huomattavasti nopeampaa, tehokkaampaa, halvempaa ja logistisesti helpompaa. (Rabeya Bosri, Abdur Razzak Uzzal, Abdullah Al Omar, A S M Touhidul Hasan, Md. Zakirul, Alam Bhuiyan, 2019, Md. Zakirul, Alam Bhuiyan, 2021)

Wolf, P., Nackerdien, R., Tuccinardi, D (2011) jakavat elektroniset äänestyslaitteet neljään ryhmään niiden perusperiaatteen perusteella:

Ensimmäinen tyyppi on erillinen äänestyslaite, joka nauhoittaa ja tallettaa äänet. Joskus näistä saa ”kuitin” mukaan, jolla äänestäjä voi varmistaa äänensä oikeellisuuden. Nämä mahdollistavat nopean datankeruun ja ääntenlaskun sekä ehkäisevät äänestyslappujen pilaantumisen. Näiden laitteiden ongelma on kuitenkin niiden käyttöönoton ja huollon hinta sekä niiden alttius manipulaatiolle sillä laitteita on yleensä käytössä satoja tai tuhansia, jolloin on mahdotonta tarkistaa jokaista laitetta.

Toinen tyyppi on optinen skannauslaite, joka skannaa koneluettavaa paperia. Näiden laitteiden käyttöönotto on helppoa, mutta kärsivät samoista ongelmista kuin edellinenkin laite ja lisäksi luottavat paperiin, jolloin logistiset kustannukset kasvavat.

Kolmas tyyppi koostuu kahdesta laitteesta, josta toinen tuottaa koneluettavan lipukkeen, jota käytetään toisessa laitteessa tallentamaan ääni. Tällöin jää fyysinen paperijälki, joka voidaan varmistaa ennen lopullista äänen antoa. Tämä tyyppi on kallis, sillä tarvitaan laitteita kaksin kappalein.

Neljäs tyyppi on äänestys internetin välityksellä. Äänet annetaan laitteella, joka on yhteydessä internettiin ja äänet menevät keskitetylle laskentaserverille. Tämä tyyppi mahdollistaa tarkat ja nopeat tulokset sekä etänä ja ilman valvontaa tapahtuvan äänestämisen. Uhkina kuitenkin on hakkerointihyökkäykset, potentiaalinen anonymiteetin ja yksityisyyden puute ja kolmannen osapuolen influenssi ääniin.

Elektronisiin äänestyslaitteisiin, ja erityisesti internet äänestämiseen, on helpompi toteuttaa laajemman skaalan hyökkäyksiä, jotka ovat vaikeampi havaita, kun taas paperiset äänestykset vaativat fyysisen pääsyn lappuihin ja niiden käsin muokkaamisen yksi kerrallaan. Elektronisissa laitteissa jo yhden koodirivin muuttaminen voi muuttaa miljoonia ääniä. (Park, Specter, M., Narula, N., & Rivest, R. L., 2021)

Elektronisia äänestyslaitteita on käytössä mm. Argentiinassa, Brasiliassa, Filippiineillä, Australiassa, Italiassa, Yhdysvalloissa ja Briteissä, ja niitä valmistavat lähinnä yksityiset yritykset, jolloin kaikkien laitteiden verifioiminen on mahdotonta. Laitteista on pyritty tekemään turvallisia, mutta niiden turvallisuutta on kritisoitu paljon, ja laitteisiin on yleisesti huono luottamus. (Borsi ja muut, 2019; Pawlak, 2018).

Solanki ja Divykant (2021) kertovat, että elektronisten äänestyslaitteiden käyttöönoton myötä valeäänet ja äänestyspaikkojen kaappaus on laskussa, kun taas peukalointi, toimintahäiriöt ja väärinkäytökset ovat nousussa. Syyksi tälle he antavat tekniset edistykset digitaalisen tekniikan alalla. Äänestyspaikkojen kaappauksella tarkoitetaan tilannetta, jossa halutaan saada ääniä tietylle ehdokkaalle joko uhkaamalla äänestäjiä tai estämällä heiltä pääsy oikeaan äänestyspaikkaan.

Brosin ja muiden (2019) mukaan tutkimukset ovat osoittaneet näiden laitteiden olevan alttiita monenlaisille hyökkäyksille. Laitteet ovat itsessään turvallisia perinteiseltä hakkeroinnilta sillä ne eivät ole yhteydessä verkkoon tai verkkoyhteys on todella hyvin suojattu, mutta ovat alttiita muunlaisille hyökkäyksille. Pawlak ja muiden (2018) mukaan

yksi hyökkäyskeino on soluttautunut hyökkääjä, joka on onnistunut muuttamaan lähdekoodia, jolloin äänestystulosta voidaan muuttaa. Myös laitteisiin on mahdollista asentaa erillinen siru, joka voi muuttaa äänestystulosta. Laitteiden säilöntäpaikkaan voidaan hyökätä ja laitteiden tietokannatkaan eivät ole turvassa erilaisilta hyökkäyksiltä, sillä näiden laitteiden ongelma on usein niiden keskitetyt järjestelmät ja tietokannat, jolloin riittää, että hyökätään vain yhteen kohteeseen.

Myös sosiaalista hakkerointia eli käyttäjään itseensä kohdistuvaa ”hakkerointia” voidaan harjoittaa. Sosiaalisessa hakkeroinnissa uhrille vakuutetaan hyökkääjän olevan jotain muuta kuin hän oikeasti on ja täten saada uhri tekemään jotain hyökkääjälle suotuisaa mitä uhri muuten ei tekisi. Sosiaalinen hakkerointi on yleistä esim. huijauspuheluissa tai hyökkääjien pyrkiessä päästä fyysisesti kiellettyyn paikkaan. Elektroniset äänestyslaitteet ovat fyysisesti äänestyspaikalla, jolloin äänestäjä on alttiina myös uhkailulle tai pakottamiselle, jos hyökkäys tapahtuu äänestyspaikalla. (Solanki & Divykant. 2021) Perinteiset paperivaalitkin ovat alttiita samalle hyökkäykselle, mutta näitä tapauksia tiedetään onneksi hyvin vähän. Elektronisiin äänestysjärjestelmiin pystyy myös lisäämään ääniä.

Äänestyslaitteet kuitenkin tuovat positiivisia asioita, kuten edellä mainitut logistiset ja rahalliset helpotukset sekä äänten laskun helpottuminen, kun se tapahtuu elektronisesti ja automaattisesti (Pawlak ja muut (2018). Paperiset äänestykset ovat kalliita, sillä papereiden tulostus ja levitys sekä ääntenlasku vie aikaa ja vaivaa, sekä vaatii paljon väkeä. Tällaisten äänestysten järjestäminen maissa, jossa asuu paljon ihmisiä, on lähes mahdotonta.

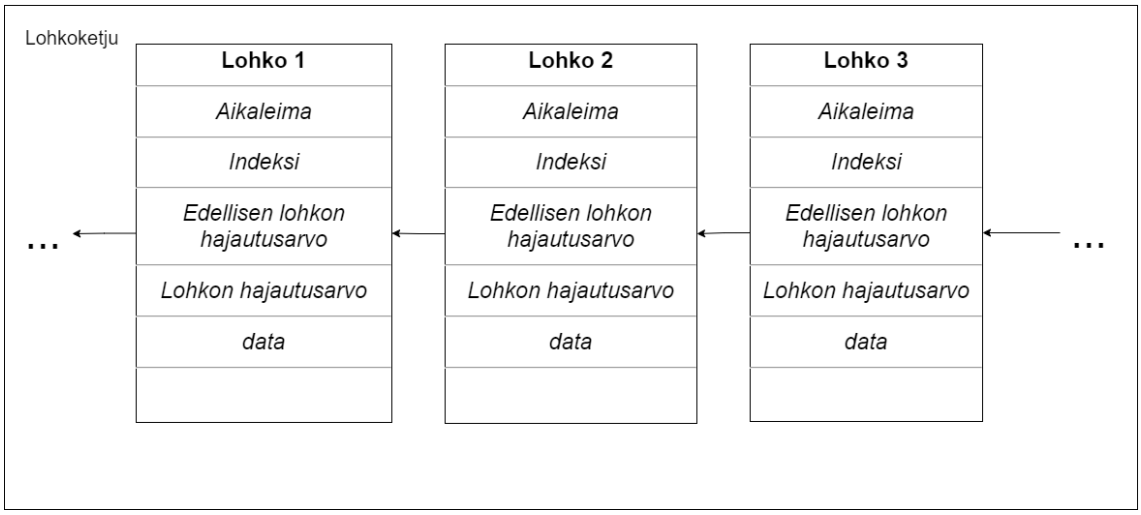
# 3 Lohkoketjut

Lohkoketju on eräänlainen tietorakenne, joka koostuu järjestetystä listasta datayksiköitä, lohkoista, jotka on linkitetty toisiinsa, jolloin ne muodostavat lohkoketjun. Lohkoketju hyödyntää hajautusarvoja ketjun luomiseen; jokainen lohko sisältää edellisen lohkon hajautusarvon, jolloin lohkojen datan muuttaminen on mahdotonta sillä silloin hajautusarvo muuttuisi, jolloin lohko ei enää sopisi ketjuun ja se hylättäisiin.

Lohkoketjuista tunnetuimmat esimerkit ovat Bitcoin ja Etherium kryptovaluutat. Erilaisset lohkoketjualustat käyttävät erilaisia konsensus algoritmeja ja mekanismeja. Näistä yleisimpiä ovat proof-of-work, jota mm. Bitcoin käyttää, ja proof-of-stake, jota mm. Etherium käyttää.

Lohkoketjut ovat siis ketju lohkoja, jotka sisältävät informaatiota. Lohkoketjujen sisältämä informaatio voi vaihdella hyvin yksinkertaisesta, jokin arvo, hyvin monimutkaisiin toiminnallisiin funktioihin. Lohkoketjut on toteutettu vertaisverkossa eli ketju ei ole kiinteällä palvelimella vaan jaettu solmuihin, jotka levitetään ympäriinsä, jotka muodostavat verkon. Solmut keskustelevat keskenään ja näin muodostavat järjestelmän.

Vertaisverkon solmut sisältävät kaikki kopion lohkoketjusta ja kun uusi lohko lisätään ketjuun, se välitetään jokaiselle solmulle, jotka tarkistavat uuden lohkon sopivuuden ketjuun konsensus algoritmien avulla, eli solmujen on oltava yhtä mieltä uuden lohkon sopivuudesta lohkon jatkeeksi tai se hylätään. Uusia lohkoja lisätään ketjuun usein laskemalla monimutkaisia matemaattisia kaavoja, tätä kutsutaan louhinnaksi. Uuden lohkon laskemisen palkkioksi saa yleensä pienen summan kryptovaluuttaa, jotka rakentuvat lohkoketjuteknologian ympärille ja toivat lohkoketjuteknologian maailmankartalle.




*Kuva 1. Kaavakuva lohkoketjun rakenteesta*

Lohkoketjun rakenne on turvallinen, sillä mitään ketjun yksittäistä lohkon dataa ei voi muuttaa ilman että muutetaan muitakin lohkoja. Jotta konsensusalgoritmit hyväksyisivät muutetut tai virheelliset lohkot on muutettava vähintään 51 % ketjun lohkoista, sillä lohkojen hajautusarvo muuttuisi ja koska jokainen lohko sisältää edellisen lohkon hajautusarvon viitteen ei muutettu lohko sopisikaan enää ketjuun ja se hylättäisiin. Tätä kutsutaan 51 % hyökkäykseksi. Kun solmuja ja lohkoja on paljon ja lohkon louhiminen vaatii paljon prosessointitehoja, voidaan olettaa ettei 51 % hyökkäys ole kannattavaa, kun laskennalliset kulut ylittävät mahdolliset hyödyt. Tällainen oletus voidaan tehdä, kun puhutaan kryptovaluutoista, mutta kun kyse on poliittisesta äänestyksestä voi hyökkääjällä olla muut kuin rahalliset tavoitteet, jolloin 51 % hyökkäykseen on suhtauduttava vakavasti.

### 3.1 Proof-of-work

Proof-of-work on vuonna 1993 kehitetty menetelmä, jolla oli tarkoitus estää palvelunestohyökkäykset (DDoS) laittamalla palvelun käyttäjä tekemään jotain työtä, yleensä prosessointiaikaa vaativaa. Vuonna 2009 Bitcoinin kehittäjä Satoshi Nakamoto kehitti tätä ideaa pidemmälle käyttämällä sitä konsensusalgoritmissa, jolla validoidaan transaktiot ja lisätään uusia lohkoja ketjuun. Proof-of-work toimii siten, että louhijat kilpailevat toistensa kanssa ratkaistakseen hankalia laskennallisia pulmia. Näiden pulmien ratkaiseminen vaatii laskentatehoa, mutta vastauksen oikeellisuuden tarkistaminen on kevyttä ja helppoa. Kun joku louhijoista on ratkaissut pulman, hän voi lähettää uuden lohkon verkkoon, jossa muut louhijat verifioivat ratkaisun oikeaksi ja lohko voidaan lisätä ketjuun, ja uusi päivitetty ketju välitetään kaikille solmuille. Bitcoinissa louhijan on arvattava pseudosatunnainen arvo, jonka on täytettävä tietyt kriteerit kun se syötetään hajautusfunktion läpi ja yhdistetään lohkon dataan. Kun ratkaisu löydetään, se välitetään muille solmuille, jotka varmistavat ratkaisun oikeellisuuden. Uusi lohko lisätään ketjuun jossa ratkaisu on louhijan todiste hänen tekemästään työstään, jolloin hänet palkitaan tietyllä määrällä kryptovaluuttaa.

Tämä menetelmä takaa turvallisen, luotettavan, muuttumattoman, reilun ja läpinäkyvän mekanismin. Tämän menetelmän ongelmia on erittäin suuri energiankulutus ja laskentateholliset vaatimukset, sekä skaalautumattomuus. Tämä mekanismi ei myöskään sisällä minkäänlaista tapaa rangaista väärinkäytöksiä tai sellaisen yrittämistä. Eräs ongelma on myös se, että jotkut käyttäjät yhdistävät laskentatehojaan (engl. mining pool), jolloin lohkoketjusta tulee enemmän keskitetty, kun tavoitteena on hajautettu järjestelmä. Nämä keskitetyt louhintapoolit ovat niin isoja, että jos kolme suurinta poolia yhdistyisivät olisi heillä hallussaan yli 50 % louhintatehosta, jolloin väärennettyjä ja virheellisiä transaktioita voitaisiin hyväksyä (Pool Distributin, btc.com, avattu 8.11.2022). (Etherium.org, avattu 1.11.2022)

### 3.2 Proof-of-stake

Proof-of-stake konsensusalgoritmi kehitettiin vuonna 2011 korjaamaan proof-of-work algoritmin ongelmia, mm. korkea energiankulutus sekä laskentatehojen yhdistäminen. Tässä algoritmissa sen sijaan, että käyttäjät kilpailisivat toisiaan vastaan louhinnassa, valitaan pseudosatunnaisesti yksi solmu validoimaan uusi lohko. Jotta solmu voidaan valita mahdolliseksi validoijaksi, on tämän talletettava tietty määrä rahaa verkkoon panoksena. Mitä suurempi panos, sen suurempi mahdollisuus on tulla valituksi validoimaan seuraavan lohko. Tämä skaalautuu lineaarisesti. Lohkon transaktioiden validoimisen jälkeen solmu palkitaan tietyllä määrällä kryptovaluuttaa.

Jos validoija hyväksyy väärennettyjä transaktioita menettää hän osan panoksestaan. Niin kauan kuin menetetty panos on suurempi, kuin mitä saisi väärän transaktion hyväksymisestä, voidaan olettaa solmujen toimivan oikein ja sääntöjen mukaisesti. Jos solmu lopettaa validoijana olemisen ei panostaan ja palkintoja saa heti takasin, sillä järjestelmän on kyettävä rankaisemaan, jos käykin ilmi, että solmu on hyväksynyt väärennettyjä transaktioita. Tämä algoritmi käyttää 99.9 % vähemmän energiaa, verrattuna proof-of-work algoritmiin (Yle uutiset, 14.9.2022 *https://yle.fi/uutiset/3-12623106)*, ja esimerkkisi Etherium, yksi suurimmista kryptovaluutoista, on siirtynyt käyttämään tätä algoritmia. Proof-of-stake myös vähentää keskityksen riskiä mikä johtaa suurempaan hajautukseen, joka on toivottua.

Tässäkin algoritmissa on vaarana 51 % hyökkäys, jossa tietyllä osapuolella on hallussaan 51 % verkosta, mutta tämä on epäkäytännöllistä etenkin suurimpien kryptovaluuttojen kohdalla, sillä se maksaisi kymmeniä miljardeja, huomattavasti enemmän, kuin mitä hyökkäyksestä hyötyisi. (wackerow, 2022)

### 3.3 Älysopimukset

Älysopimukset ovat sopimuksia, jotka voivat sisältää suoritettavia funktioita tai koodia, joka ajetaan automaattisesti. Näitä sopimuksia käytetään määrittelemään ja sääntöjä ja älysopimukset valvovat niitä automaattisesti. Näitä ei voi poistaa ja transaktiot ovat peruuttamattomia. Älysopimukset Ehterium verkossa eivät vaadi käyttölupaa eli kuka tahansa voi tehdä ja/tai käyttää sellaista. Älysopimukset eivät vaadi valvomiseen kolmatta osapuolta, valvojaa, hallitsijaa tms., vaan hoitavat itse sopimuksen sääntöjen noudattamisesta. Älysopimukset eivät voi saada dataa ”oikeasta maailmasta” esimerkiksi HTTP pyyntöjen avulla vaan ne luottavat oraakkeleihin (engl. oracle), jotka toimivat siltana lohkoketjussa olevan älysopimuksen ja lohkoketjun ulkopuolella olevan datan välillä. (wackerow, 2022)

# 4 Ehdotettuja lohkoketjuteknologioihin perustuvia äänestysjärjestelmiä

Lohkoketjupohjaisia äänestysjärjestelmiä on viimevuosien aikana tutkittu, ja erilaisia järjestelmiä on ehdotettu. Tuon tässä esille muutamia järjestelmiä jotka sisältävät mielestäni oleellisia piirteitä ja toiminnallisuuksia sekä huomioita lohkoketjupohjaiseen äänestysjärjestelmään. Näissä ehdotuksissa löytyy samoja piirteitä sekä eroavaisuuksia, joita pyrin kappaleessa viisi käymään läpi ja löytämään niistä parhaimmat ratkaisut.

## 4.1 ethVote

Mols & Vasilomanolakis (2020) lovitat ethVote konseptin lohkoketjupohjaisesta äänestysjärjestelmästä, joka hyödyntää Etherium lohkoketjua, älysopimuksia, Paillier-homomorfista salausjärjestelmää äänten salaamiseen ja laskemiseen sekä ei-vuorovaikutteisia nollatietotodistusta (engl. non-interactive zero-knowledge proof) äänten, tulosten salausten ja salausten purkujen oikeellisuuden laskemiseen. Tämä ehdotettu järjestelmä koostuu selainpuolen sovelluksesta ja Etherium lohkoketjussa olevasta kolmesta erillisestä älysopimuksesta, jotka kontrolloivat logiikan koko järjestelmälle. Ne tallentavat listan äänioikeutettuja äänestäjiä, vaalien järjestelytietoja ja jokaisen käyttäjän salatut äänet.

Nämä kolme älysopimusta ovat:

1) Rekisteröintiviranomainen (Registration authority): Älysopimus, joka tallentaa jokaisen äänioikeutetun äänestäjän Etherium osoitteen. Jokainen osoite voi sisältää identifioitavaa informaatiota, joka tallennetaan osoitteen kanssa, jonka on oltava salattu. Äänestäjien on autentikoitava itsensä Rekisteröintiviranomaiselle menemällä fyysisesti paikalle näyttämään henkilöllisyystodistus, sillä verkossa tapahtuva autentikointi saattaisi tuoda haavoittuvaisuuksia järjestelmään.
2) Vaalitehdas (Election factory): Tämä älysopimus on vastuussa uusien vaalisopimusten (election contracts) luomisesta, ja niiden Etherium osoitteen ylläpitämisestä. Kun uusi vaali luodaan, annetaan sille nimi ja kuvaus, alku ja loppuaika sekä julkinen salausavain homomorfiseen salaukseen.
3) Vaali (Election): Tämä älysopimus sisältää ydinlogiikan järjestelmälle. Kolme vaihetta määrittelevät saatavat funktionaalisuudet:
    a) *Ennen vaaleja.* Vaaliviranomainen (election authority) voi lisätä ehdokkaita vaaleihin. Ennen vaaleja äänestäjät voivat nähdä ketkä ehdokkaat ovat saatavilla.
    b) *Vaalien aikana.* Ehdokkaiden lista on kiinteä ja äänestäjät voivat antaa salatun äänensä käyttämällä julkista avainta, joka on tallennettu älysopimukseen. Jokainen ääni koostuu listasta salattuja nollia ja ykkösiä, jotka indikoivat saiko ehdokkaat äänen äänestäjältä vai ei. Vain yksi ykkönen per ääni on sallittu. Ennen äänen hyväksymistä älysopimukseen lähetetään Rekisteröintivi-

ranomaiselle kysely äänestäjän osoitteesta verifioimaan, onko hänellä äänioikeus. Jos äänestäjä vaihtaa äänensä ylikirjoitetaan olemassa oleva ääni. Laskentavaiheessa salatut luvut lasketaan yhteen ja tämän luvun salauksen purusta saatu numero on kyseisen ehdokkaan äänien kokonaismäärä.

c) *Vaalien jälkeen.* Kuka vain voi hakea listan osoitteita, jotka antoivat äänen ja heidän salatun äänensä. Tämä antaa kenelle tahansa mahdollisuuden laskea jokaisen ehdokkaan tuloksen. Käyttämällä nollatietotodistusta vaaliviranomainen voi todistaa, että lasku on tarkka ilman että paljastetaan yksityistä avainta.

ethVoten ollessa avoimen lähdekoodin projekti olisi hyökkääjälle triviaalia selvittää käytetyt salausmenetelmät ja tätä hyödyntäen kirjoittaa ohjelma, joka salaa virheellisiä ääniä, jotka näyttävät samalta kuin oikea ääni. Esimerkiksi sen sijaan että hyökkääjä salaisi arvon ”1” hän voisi salata arvon ”1000” tai hän voisi äänestää useaa ehdokasta ja koska nämä haitalliset äänet näyttävät salauksen jälkeen samalta kuin oikeat äänet, on tällainen hyökkäys mahdollinen. Tällainen hyökkäys ei kuitenkaan jäisi huomaamatta, sillä laskentavaiheessa äänten määrää verrataan äänestäneiden määrään ja ylimääräiset äänet huomattaisiin. Tosin tällöin vaalituloksesta tulisi pätemätön, joka heikentäisi luottoa järjestelmään.

Ratkaisu tähän ongelmaan on hyödyntää nollatietotodistusta, jonka avulla voidaan todistaa fakta toiselle osapuolelle ilman että paljastetaan itse faktaa. Tarkistava osapuoli ei tiedä itse faktasta mitään, mutta voi silti vakuuttua, että faktaa todistava osapuoli tietää faktan. Täten äänestäjä voi vakuuttaa älysopimukselle, että hänen salattu ääni noudattaa kaikkia sääntöjä ja on validi ilman että hän paljastaa itse salattua ääntä.

Etherium lohkoketjun käyttäminen on kuitenkin kallista, ja jokainen ehdokas nostaa hintaa, ja suurella määrällä ehdokkaita järjestelmästä tulee nopeasti hyvin kallis. Saksassa käytettiin vuoden 2017 liittovaaleihin 92 miljoonaa euroa (Blaze et al 2019, Mols et al, 2020). Äänestyksessä annettiin noin 47 miljoonaa ääntä, jonka hinta olisi Maaliskuussa Etherium lohkoketjussa vuonna 2020 152,3 miljoonaa euroa. Hintaa voidaan kuitenkin laskea eri menetelmin: i) käyttämällä yksityistä lohkoketjua, ii) käyttämällä Etherium 2.0:aa, joka on siirtynyt käyttämään proof-of-stake menetelmää, joka on 99,9 % energiankulutukseltaan pienempi, iii) yksityisten avainten kokojen pienentämien. Vaihtoehdoissa i) ja iii) on kuitenkin ongelmia.

### 4.2 Auditable Blockchain Voting System (AVBS)

Pawlak, Guziur ja Poniszewska-Marańda (2018) ehdottivat artikkelissaan valvottua ja ei etänä olevaa äänestysjärjestelmää, joka käyttää lohkoketjuja äänen tallentamiseen ja verifioimiseen. Järjestelmän on tarkoitus parantaa äänestysprosessia Puolassa. Järjestelmä koostuu kuudesta komponentista:

- asiakassovelluksista (äänestyspaikat), ovat kevyitä ohjelmia, jotka sijaitsevat äänestyspaikoilla, ja niitä käytetään äänten antamiseen lohkoketjutransaktioiden muodossa.
- Tunnettujen solmujen järjestelmä, on joukko lohkoketjun solmuja, jotka tallentavat lohkoja ja louhivat uusia.
- Äänestystunnus, aakkosnumeraalisia koodeja, joita käytetään äänestäjien todentamiseen ja valtuutukseen.
- Äänestäjän vahvistama paperinen esitys äänestä, joka sisältää saman informaation, kuin ABVS. Tätä voidaan käyttää esim. perinteisen paperiäänen tapaan, tuomaan lisää turvallisuutta tarkistukseen ja verifioimiseen.
- Moduuli äänten virheellisyyden ilmoituksille, joka raportoi epäjohdonmukaisuudet äänissä.
- Laskentaohjelma, joka iteroi lohkoketjun läpi ja tuottaa äänestyksen tuloksen

Äänestäminen AVBS:lla jakautuu kolmeen vaiheeseen:

1. Vaalien valmisteleminen. Käytetyt ohjelmistot ja laitteet allekirjoitetaan ja sertifioidaan. Vaalivirkailijat valitsevat instituutiot, joita käytetään solmuina lohkoketjujärjestelmässä ja lopuksi äänestystunnukset generoidaan ja jaetaan.
2. Äänestysvaihe. Äänestäjät identifioivat itsensä äänestyspaikalla heille satunnaisesti annetulla äänestystunnuksella. He antavat äänensä käyttämällä tätä äänestystunnusta, ja lopuksi laittavat paperisen esityksen äänestä uurnaan. Tunnetut solmut louhivat lohkoja, jotka sisältävät äänen ja saavuttavat konsensuksen. Tässä vaiheessa on tärkeää, että lohkoketju pysyy yksityisenä.
3. Äänten lasku ja verifikaatio. Tässä viimeisessä vaiheessa järjestelmä on deaktivoitu ja laskentaohjelma(t) tuottavat äänestyksen tuloksen. Käyttämättömät äänestystunnukset tuodaan julki, jotta voidaan verifioida oikea äänten määrä ketjussa. Lopuksi lohkoketju tuodaan julkiseksi, jotta kuka tahansa voi tarkistaa ja ilmoittaa epäjohdonmukaisuuksista.

Tätä järjestelmää testattiin, jotta saataisiin viite tarvittavan laitteiston tehokkuuteen. He käyttivät eri pituisia lohkoketjuja, joista pisimmät (> 1 280 000 lohkoa) aiheuttivat muistiongelmia testilaitteistossa. He toteavat myös, että äänestystuloksen saaminen yhdeltä solmulta on nopea prosessi. Lisäksi he tuovat ilmi, että on laitteiston ja käyttöjärjestelmään liittyviä ongelmia, jotka on korjattava ennen seuraavaa testivaihetta. (Pawlak et al, 2018)

### 4.3 Secure Internet Voting using Blockchain Technology

Khan & Rasheed (2021) ehdottavat järjestelmää, joka toimii suljetussa Etherium lohkoketjussa ja käyttää älysopimuksia. Järjestelmä käyttää Paillier homomorfista salausta ja salaisen avaimen vaihtoa (engl. private key shifting) äänestäjän yksityisyyden ja identiteetin turvaamiseen. Äänestysprosessi järjestelmässä sisältää neljä vaihetta:

i) Äänestäjien ja ehdokkaiden rekisteröinti. Äänestäjä rekisteröi itsensä virallisella paikalla missä hänen sormenjälkensä ja verkkokalvo skannataan ja lähetetään järjestelmälle, joka tekee transaktion suljettuun lohkoketjuun sisältäen äänestäjän tiedot. Sama tapahtuu ehdokkaille.

ii) Äänestysprosessin käynnistäminen. Rekisteröintivaiheen jälkeen vaaleista vastuussa oleva taho käynnistää äänestysprosessin vaalipäivänä.

iii) Äänestäminen. Järjestelmä tarkistaa äänestäjän rekisteröinnin ennen kuin ääni voidaan antaa. Järjestelmä salaa äänestäjän tiedot, ennen lohkoketjuun tallentamista. Järjestelmä tuo anonymiteetin ja piilottaa annetut äänet, eikä edes järjestelmän hallitsijataho voi nähdä tuloksia kesken äänestysvaiheen.

iv) Tulosten julkaisu. Järjestelmä purkaa äänten salauksen ja laskee sekä ilmoittaa tuloksen.

Lohkoketjun ollessa hajautettu järjestelmä on hyökkääjän vaikea tuhota koko lohkoketjua, joka sisältää äänestäjien datan. Myös lohkoketjujen muuntamattomuus pätee tähän järjestelmään eli vaikka hyökkääjä pääsisikin käsiksi palvelimelle, jossa säilytetään dataa ja suojattuja salausavaimia, hän näkisi vain salatun datan eikä voisi muuttaa bittiäkään tästä datasta. Järjestelmä huomioi myös tuplaäänet tarkistamalla äänestäjän äänestysstatuksen, ja jos äänestäjä on jo antanut äänensä ei uutta ääntä hyväksytä. (Khan Rasheed, 2021)

### 4.4 Blockchain-Based Electronic Voting System for Election in Turkey

Bulut, Kantarci, Keskin ja Bahtiyar (2019) esittävät lohkoketjupohjaista äänestysjärjestelmää Turkkiin paikkaamaan nykyisen äänestysjärjestelmän ongelmia. Vaikka järjestelmä on suunniteltu turkkiin, voi yleistä toimintamallia ja ideaa räätälöidä tietyn maan järjestelmälle sopivaksi. Tämä ehdotettu järjestelmä koostuu useammasta tasosta, jonka avulla eliminoidaan pullonkauloja ja viivettä ja niistä johtuvia ongelmia. Jos Turkin kokoista maata edustaisi yksi lohkoketju olisi latenssi ja synkronoinnin hitaus ongelma. Tasojen välillä on turvattu linkki ja tasoja voi olla niin monta kuin tarvitaan, jolloin järjestelmä olisi skaalautuva. Turkin kokoiselle maalle kerrotaan kahden tason olevan riittävä. Alimmalla tasolla on lohkoketju joka koostuu solmuista jotka edustavat äänestyslaitteita joiden avulla kansalaiset äänestävät.

Lohkoja on kahden tyyppisiä. Ensimmäinen on alimman tason lohkoketjun rakentamista varten ja siihen tallennetaan ehdokkaan tiedot, äänestyspaikan tiedot ja erilaisia

lohkoketjuun tarvittavia hajautusarvoja. Toinen tyyppi koostuu edellisen lohkon hajautusarvosta ja avainsanasta, joka indikoi lohkojen listaa. Alimmalla tasolla jokainen lohko koostuu yhdestä transaktiosta ja kaikki transaktion informaatio tallennetaan. Lohkojen informaatio (äänet) lähetetään eri ajanjaksoissa alemmalta tasolta ylöspäin klustereissa. Datan vaihtaessa tasoa sen johdonmukaisuus tarkistetaan ja lähetetään lippu, joka indikoi joko hyväksymistä tai hylkäämistä. Prosessia toistetaan, kunnes lohkoketju saavuttaa konsensuksen. Näin yhden lohkoketjun koko ei kasva liian suureksi vaan kaikkea dataa voidaan käsitellä nopeasti ja tehokkaasti.

Tämä järjestelmä on turvallinen 51 % hyökkäykseltä, sillä hyökkääjän on fyysisesti päästävä käsiksi äänestyslaitteeseen ja koska laitteita on paljon ja niitä vartioidaan ei tämä ole käytännöllisesti katsoen mahdollista. Bulut ja muut nostavat esille myös järjestelmän kestävyyden erilaisia katastrofeja vastaan. Lohkoketjun ollessa hajautettu, yhden tai useamman äänestyslaitteen vahingoittuessa ketju on turvassa, jolloin vaalit ja vaalipäivä on turvattu. He toteavat myös, että Turkin vaalien ääntenlaskun virallisen tulokseen saaminen voi kestää nykyjärjestelmällä jopa kymmenen päivää ja heidän ehdottamansa järjestelmä antaa tuloksen lähes heti, sillä riittää että tarkastelee ketjun jokaista solmua, joka pitää sisällään kaiken tarvittavan informaation vaalituloksen saamiseen.

# 5 Lohkoketjuteknologiaan perustuvien äänestysjärjestelmien vaatimuksia ja huomioon otettavaa

Sierra Leone on ensimmäinen maa, joka on ottanut lohkoketjuteknologian käyttöön vaaleissaan, ja se on laskenut äänten peukaloinnin mahdollisuutta (Solanki ja Meva, 2021), mikä on hyvä esimerkki lohkoketjuteknologian potentiaalista.

Vuonna 2007 Viro otti käyttöön internetin kautta tapahtuvan äänestämisen. Viron äänestysmalli on ainutlaatuinen, eikä mikään muu maa käytä samanlaista mallia. Virossa äänestyksessä on mahdollisuus äänestää sekä ”perinteisesti” paperilla, että internetin välityksellä. Paperinen ääni on siinä mielessä arvokkaampi, että paperinen ääni kumoaa internetin kautta annetun äänen. Tämä suojaa uhkailulta, pakottamiselta ja äänen ostamiselta, kun hyökkääjä ei voi varmistua, ettei äänestäjä mene jälkeenpäin muuttamaan ääntä. (Ehin, Solvak, Willemson, Vinkel, 2022) Virossa on myös alettu tallentamaan ja prosessoimaan ääniä hyödyntäen lohkoketjuverkkoa (Cabuk ja Karaarslan (2018).

Cabuk ja Karaarslan (2018) nostavat myös esille huonon luottamuksen e-äänestämiseen ja järjestelmien turvallisuuteen. Tämä on myös yksi syy, miksi Virossa on käytössä sekä paperiset äänestyslipukkeet, että internetin kautta tapahtuva äänestäminen. Ihmiset pitävät paperisia äänestyslappuja paljon turvallisimpina, vaikka niihinkin kohdistuu monia uhkia ja hyökkäyksiä. Lohkoketjuteknologialla voidaan yrittää parantaa ihmisten luottamusta e-äänestämiseen, mutta se saattaa olla hankala tehtävä sillä lohkoketjun toiminta, ja ominaisuudet ovat monelle tuntematon asia, ja tämän tutkimuksen yksi tavoitteista on tuoda lohkoketjun toiminnot ja hyödylliset ominaisuudet äänestysjärjestelmissä paremmin ymmärrettäväksi.

Länsi-Virginiassa aloitettiin vuonna 2018 käyttämää lohkoketjupohjaista äänestysjärjestelmää nimeltä Voatz, jonka avulla mm. ulkomailla asuvat pystyvät äänestämään. Voatz järjestelmästä on tehty monia analyyseja, ja sen turvallisuutta on kritisoitu (Specter, Koppel, Weitzner, 2020). Japanissa Tsukuba kaupungissa kokeiltiin lohkoketjupohjaisen äänestysjärjestelmän pilottia, jossa äänestäjän verifioimiseen käytettiin 12 numeroa pitkää koodia. Moskova testasi lohkoketjun käyttämistä kolmella vaalialueella vuonna 2019 ja tässä järjestelmässä äänestäjällä oli täysi anonymiteetti. (Solanki ja Meva, 2021) Maissa, jossa demokratia on uhattuna tai siinä on paljon epäkohtia tuo lohkoketjupohjainen järjestelmä turvaa jos äänestäjän identiteetti pystytään salaamaan ja/tai tekemään anonyymiksi kuitenkin varmistaen, että äänen voi antaa vain sallitun määrän kertoja ja ettei peukalointia tapahdu.

Yksi keskeisimmistä esiin nousseista seikoista lähes kaikissa ehdotetuissa järjestelmissä on äänestäjän yksityisyyden ja vaalisalaisuuden turvaaminen, sekä vaalien, annettujen äänten ja laskemisen prosessien oikeellisuus ja tulosten läpinäkyvyys. Tämä vaikut-

taa olevan mahdollista toteuttaa käyttämällä lohkoketjuteknologioita, jonka avulla voidaan luotettavasti salata tietoa esim. äänestäjän yksityisyyttä varten, mutta myös näyttää salattua tietoa esim. annettu ääni, ilman että paljastetaan äänestäjän henkilöllisyyttä tai ääni voidaan jäljittää tiettyyn henkilöön. Lohkoketju on kuitenkin tuotava julkiseksi jossain kohtaa prosessia, jotta läpinäkyvyys säilyy ja jotta kuka tahansa voi halutessaan tarkistaa vaalituloksen oikeellisuuden. On myös luotava väylä, jonka kautta tuloksen voi tarkistaa ja raportoida mahdolliset löydetyt virheet tai äänet, jotka eivät täsmää tulokseen.

Erilaisissa ehdotetuissa järjestelmissä vaihteli, että käytetäänkö suljettua- vai julkista lohkoketjua. Suljettu lohkoketju äänestysvaiheessa oli suosituin, ja suljetussa lohkoketjussa on se hyöty, että voidaan olettaa kaikkien solmujen olevan rehellisiä ja voidaan käyttää pienempää määrää solmuja, jolloin laitteiston tehokkuusvaatimukset pienenevät ja transaktioiden validointiaika lyhenee, sekä louhinnan hinta laskee (Pawlak ja muut, 2021). On kuitenkin tärkeää suojata tämä suljettu järjestelmä ulkopuolisilta hyökkäyksiltä sillä pienempi määrä solmuja helpottaa 51 % hyökkäyksen. Tähän on kuitenkin erilaisia keinoja estää suljettuun lohkoketjuun kohdistuvat hyökkäykset.

Khan ja Rasheed (2021) käyttivät Paillier homomorfista suojausta ja salaisen avaimen vaihtotekniikkaa äänten salaamiseen, jolloin vaikka hyökkääjä pääsisikin verkkoon sisälle hän näkee vain salatut äänet eikä voi niiden salausta purkaa ilman salaista avainta tai muuttaa ääntä lohkoketjun muuttumattoman rakenteen takia. On siis tärkeää käyttää muitakin salaus- ja suojauskeinoja eikä luottaa puhtaasti lohkoketjuun. Lohkoketjun tarkoitus on toimia tiedon säilyttävänä hajautettuna tietorakenteena ja äänet, äänestäjien identiteetti ja muut tiedot on salattava ennen lohkoketjuun tallentamista. Lohkoketjun rakenteen ollessa muuttumaton ja hajautettu on lohkoketjuun pohjautuva äänestysjärjestelmä turvassa perinteiseltä hakkeroinnilta, joka voisi muuttaa perinteisessä tietokannassa olevaa dataa. On siis tärkeää hyödyntää lohkoketjun tuomaa muuttumatonta ja hajautettua teknologiaa eikä tallentaa dataa tietokantaan vaan tallettaa data lohkoketjuun.

Äänestäjän identiteetin tarkistamiseen ehdotettiin erilaisia tapoja. Kaikissa oli kuitenkin havaittavissa samankaltaisuuksia, eli henkilön on mentävä fyysisesti esittämään henkilöllisyystodistus, jolloin hänet rekisteröidään äänestäjäksi. Ehdotuksia oli sormenjäljen- ja verkkokalvoskannauksesta rekisteröintivaiheessa, jolla äänestäjä tunnistautuu äänestysvaiheessa, kertakäyttöiseen koodiin, jolla äänestäjä tunnistautuu äänestäessä. Eri tunnistautumismenetelmästä huolimatta, kaikki tallentavat äänestäjän tietoja ja statuksen lohkoketjuun, jonka avulla tarkistetaan äänestäjän äänestysstatus. Jos ääni on jo annettu, voidaan joko hylätä uusi lohko tai vaihtaa äänestäneen antamaa ääntä riippuen salliiko vaalien säännöt äänen vaihtamisen. Kuten aikaisemmin mainittu, äänen vaihtamisen mahdollisuus suojaa äänestäjiä pakottamiselta, uhkailulta tai äänen ostamiselta, mutta tekee järjestelmästä monimutkaisemman.

Borsi ja muut (2019) toteavat, että heidän ehdottamansa järjestelmä suojaa myös fyysisiltä uhilta esimerkiksi äänestyspaikan kaappaamiselta sillä heidän ehdottamassa järjestelmässä voi äänestää sekä fyysisestä paikasta että mobiililaitteen avulla. Tämä tuo turvaa äänestäjälle uhkailulta tai pakottamiselta, sillä hänen ei tarvitse fyysisesti mennä mihinkään äänestääkseen. Tämä ratkaisu huomioi myös köyhempien maiden kansalaisia, joilla kaikilla ei ole varaa tai pääsyä mobiililaitteeseen, sekä muut rajoittuneet henkilöt ketkä eivät voi mobiililaitetta käyttää. Eli on huomioitava ja mahdollistettava jokaiselle äänestäminen.

Lohkoketjuteknologian suurimpia heikkouksia ovat louhinnan vaatima suuri energiamäärä ja prosessointiteho käytettäessä proof-of-work algoritmeja, ja skaalautuvuuden hankaluudet sillä suuri määrä solmuja hidastaa järjestelmää. Proof-of-stake on huomattavasti energiatehokkaampi ja laskennallisesti kevyempi kun kaikki louhijat eivät kilpaile keskenään, mutta samalla turvallisuus ja hajautuvuus kärsivät. Kuitenkin, jos lohkoketju on suljettu, kunnes äänet on laskettu ja tulokset julkaistu, proof-of-stake algoritmin voidaan olettaa olevan tarpeeksi turvallinen. Samalla laskentatehovaatimukset ja energiankulutus laskevat. Avoimen verkon ongelmia on avoimuus, jolloin kaikki transaktiot ovat kaikkien nähtävillä eikä välttämättä haluta äänestystuloksia nähtäväksi äänestyksen aikana, vaan vasta äänestysajan päätyttyä. Käytetty suljettu lohkoketju on kuitenkin tuotava julkisesti heti äänestyksen loputtua, jotta vaalien läpinäkyvyys täyttyy. Mahdolliset paperiset tai muulla keinolla annetut äänet on lisättävä lohkoketjuun äänestystuloksen läpinäkyvyyden maksimoimiseksi.

Suljettuun lohkoketjuun tarjotaan monia työkaluja ja palveluita ja niistä yksi kehittyneimmistä on Linux Foundationin alaisuudessa perustettu hyperledger fabric. Hyperledger fabric on yritystason luvallinen hajautettu kirjanpitotekniikka. Se keskittyy valtuutettujen lohkoketjuverkkojen käyttöön hajautetuissa kaupallisissa sovelluksissa ja sillä on useita elementtejä turvallisuuteen, toiminnallisuuteen ja tiedon näkyvyyteen liittyen. Hyperledger fabric on tehokas tekniikka ja sen avulla voi tehdä omia personalisoituja lohkoketjupalveluita ja se on erinomainen työkalu äänestysjärjestelmään. González, Mena, Muñoz, Rojas, Sosa-Gómez (2022) ehdottavatkin hyperledger fabric alustaa käytettävän heidän äänestysjärjestelmäehdotuksessaan. He toteavat yhdeksi julkisten lohkoketjujen, kuten Bitcoinin ja Ehterium 1.0:n ongelmaksi transaktionopeudet, jota on rajoitettuja, mutta käyttämällä luvallista lohkoketjua ja hyperledger farbricia he ovat saaneet transaktionopeudeksi 20 000 transaktiota per sekunti. Suljettu lohkoketju pitää ketjun koon pienempänä, jolloin tehovaatimukset laskevat ja vältytään pullonkaulasta, jota suuri avoin ketju voi tuoda, kun ketju on synkronoitava useiden solmujen kesken.

# 6 Yhteenveto

Nykyisin käytössä olevissa äänestysjärjestelmissä on suuria turvallisuusaukkoja kuten alttius manipulaatiolle, väärinkäytölle, hakkeroinnille ja virheille. Käyttämällä lohkoketjuteknologioita voidaan paikata näitä aukkoja. Äänestäjän yksityisyyden turvaaminen ja vaalisalaisuuden pitäminen on kriittistä, jotta jokainen voi antaa äänensä turvallisesti ilman ulkopuolista uhkailua pelkoa seurauksista. Tämä on erityisen tärkeää maissa, jossa demokratian toteutumisessa on vielä kehitettävää. Lohkoketjuteknologiat tarjoavat muuttumattoman rakenteensa avulla turvallisen säilöntäpaikan äänille siinä mielessä, ettei annettua ääntä voi kukaan muuttaa muuta kuin 51 % hyökkäyksellä, jonka toteuttaminen on erityisen kallista. On kuitenkin muistettava, että lohkoketjut eivät takaa kuin muuttumattoman tietorakenteen ja säilöntäpaikan äänille ja data on suojattava ja salattava muilla keinoilla ennen lohkoketjuun asettamista.

Lohkoketjuteknologioilla voidaan myös taata vaalien läpinäkyvyys, sillä ketju voidaan tuoda julkiseksi kaikille tarkasteltavaksi vaalien jälkeen, jolloin epäjohdonmukaisuudet tai väärinkäytökset huomattaisiin. Tässä vaiheessa on tärkeää varmistaa, ettei äänestäjää voida kohdentaa tai jäljittää tiettyyn ääneen (tai toisinpäin) tai vaalisalaisuuden pitämisen periaate katoaa ja demokratia ei toteudu vaaditulla tasolla. Lohkoketjun tarkasteluun ja mahdollisten epäjohdonmukaisuuksien raportoimiseen on luotava työkalu, jolle kaikilla on pääsy ja jonka käyttäminen on intuitiivista lohkoketjuihin perehtymättömälläkin henkilöllä. Lohkoketjut eivät korjaa kaikkia vaalijärjestelmien ongelmia, mutta ne ovat oivallinen teknologia paikkaamaan osaa ongelmista, jolloin ollaan askeleen lähempänä turvallisia ja reiluja vaaleja.

## Lähdeluettelo


- Bosri, Uzzal, A. R., Omar, A. A., Hasan, A. S. M. T., & Bhuiyan, M. Z. A. 2019. Towards a Privacy-Preserving Voting System Through Blockchain Technologies. 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 602–608. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00116
- Bulut, R., Kantarci, A., Keskin, S., & Bahtiyar, S. (2019). Blockchain-Based Electronic Voting System for Elections in Turkey. 2019 4th International Conference on Computer Science and Engineering (UBMK), 183–188. https://doi.org/10.1109/UBMK.2019.8907102
- Çabuk, U.C., Karaarslan, E.: A survey on feasibility and suitability of blockchain techniques for the E-voting systems. Int. J. Adv. Res. Comput. Commun. Eng. ISO 3297:2007 Certified 7(3) (2018)
- corwintines, 3.11.2022, PROOF-OF-STAKE, etherium.org, avattu 8.11.2022, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. Government Information Quarterly, 39(4), 101718. https://doi.org/10.1016/j.giq.2022.101718
- Evans, & Paul, N. 2004. Election security: Perception and reality. IEEE Security & Privacy, 2(1), 24–31. https://doi.org/10.1109/MSECP.2004.1264850
- González, C. D., Mena, D. F., Muñoz, A. M., Rojas, O., & Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. Applied Sciences, 12(2), 531–. https://doi.org/10.3390/app12020531
- Khan, & Rasheed, H. S. 2021. Secure Internet Voting using Blockchain Technology. 2021 International Conference on Cyber Warfare and Security (ICCWS), 82–86. https://doi.org/10.1109/ICCWS53234.2021.9703027

- Mols, & Vasilomanolakis, E. (2020). ethVote: Towards secure voting with distributed ledgers. 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1–8. https://doi.org/10.1109/CyberSecurity49315.2020.9138866
- Park, Specter, M., Narula, N., & Rivest, R. L. 2021. Going from bad to worse: from Internet voting to blockchain voting. Journal of Cybersecurity (Oxford), 7(1). https://doi.org/10.1093/cybsec/tyaa025
- Pawlak, Guziur, J., & Poniszewska-Marańda, A. 2018. Towards the Blockchain Technology for System Voting Process. In Cyberspace Safety and Security (Vol. 11161, pp. 209–223). Springer International Publishing. https://doi.org/10.1007/978-3-030-01689-0_17
- Pool Distribution, avattu 8.11. 2022, https://btc.com/stats/pool, avattu 8.11.2022
- Solanki, & Meva, D. 2021. Proposed Secure and Robust Voting System Using Blockchain Conceptual Framework. In Emerging Technologies in Data Mining and Information Security (pp. 661–671). Springer Singapore. https://doi.org/10.1007/978-981-15-9927-9_64
- Specter, M. A., Koppel, J., & Weitzner, D. (2020). The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections. PROCEEDINGS OF THE 29TH USENIX SECURITY SYMPOSIUM, 1535–1552.
- wackerow, 2.9.2022, INTRODUCTION TO SMART CONTRACTS, avattu 8.11.2022, *https://ethereum.org/en/developers/docs/smart-contracts/*
- wackerow, 27.9.2022, Proof-of-work, Etherium.org, avattu 1.11.2022, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/
- Wolf. P., Nackerdien. R., Tuccinardi. D., 2011, Introducing Electronic Voting: Essential Considerations