Tampereen yliopisto

Ville-Vesa Sarin

LOHKOKETJUTEKNOLOGIA ÄÄNES-TYSJÄRJESTELMÄN POHJANA

Informaatioteknologian ja viestinnän tiedekunta

Kandidaatintutkielma

Marraskuu 2022

TIIVISTELMÄ

Ville-Vesa Sarin: Lohkoketjuteknologia äänestysjärjestelmän pohjana

Kandidaatintutkielma

Tampereen yliopisto

Tietojenkäsittelytieteiden tutkinto-ohjelma

Marraskuu 2022

Demokraattisessa poliittisessa järjestelmässä äänestäminen on yksi tärkeimpiä tapoja saada kansalaisten mielipiteet selville. Paperiseen äänestykseen liittyy kuitenkin paljon riskejä liittyen vaalituloksen peukalointiin. Elektronista äänestämistä ja vaaliuurnien korvaamista tietokoneilla on kokeiltu ympäri maailmaa, mutta koska tiedot tallentuvat yhdelle keskitetylle palvelimelle, on järjestelmä erittäin helppo kohde kyberhyökkäyksille. Nousevana teknologiana lohkoketju voisi tarjota turvallisemman alustan äänestysjärjestelmälle, sillä se tarjoaa hajautetun rakenteensa ansiosta todella vahvan tietoturvan.

Tutkielma on kirjallisuuskatsaus ja sen tarkoituksena on tarkastella lohkoketjuteknologian tarjoamia ominaisuuksia, nykyisiä käytössä olevia lohkoketjupohjaisia äänestysjärjestelmiä sekä tutkijoiden esittämiä malleja äänestysjärjestelmistä. Tutkimuskysymykseni on: ”Mitä hyviä ja huonoja puolia liittyy hajautetun lohkoketjuteknologian käyttöönottoon äänestysprosessissa?” Tutkielmaan käytetty kirjallisuus on suurimmaksi osaksi haettu Tampereen yliopiston Andor-tietokannasta, mutta lisäksi käytin myös Institute of Electrical and Electronics Engineers -järjestön (IEEE) sähköistä tietokantaa ja Google Scholaria.

Lohkoketjun ansiosta vaaleissa annetut äänet pysyvät muuttumattomina, äänestäjän anonymiteetti on turvattu ja äänestysprosessi voi olla alusta loppuun läpinäkyvä. Äänestys on avoin kaikille halukkaille tarkastelijoille, joka lisää luottamusta äänestysprosessiin ja jokainen voi varmistua siitä, että annettu ääni on tallennettu oikein. Lisäksi on mahdollista siirtää äänestäminen jokaisen kansalaisen tietokoneeseen tai mobiililaitteeseen, jolloin vaalipaikoilta vapautuu työvoimaa. Koko äänestysprosessi voisi olla täysin automatisoitu.

Kirjallisuudesta selviää, että tutkimustieto aiheesta tukee lohkoketjuteknologian soveltamista äänestystarkoituksiin teoriassa. Suoritetut kokeilut ovat kuitenkin toistaiseksi olleet mittakaavaltaan hyvin pieniä ja niissäkin on havaittu joitain tietoturvariskejä. Koska lohkoketjun suojaus on tietokoneen laskemien energiaintensiivisten algoritmien varassa, kasvaa myös laskuaika lohkoketjuverkoston laajetessa. Tähänastiset kokeilut ovat olleet vain paikallisia tai alueellisia kokeiluja, eikä näyttöjä koko maan kattavasta testauksesta vielä ole.

Avainsanat: demokratia, äänestäminen, hajautettu järjestelmä, lohkoketju

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

SISÄLLYSLUETTELO

1 Johdanto ... 1

2 Tutkimusmenetelmä ... 3

3 Äänestysjärjestelmien ongelmia ... 3

4 Lohkoketjuteknologia ... 4

4.1 Lohkoketjujen luokittelu 5

4.2 Konsensusmekanismit 5

4.3 Älysopimus 6

5 Nykyiset toteutukset lohkoketjuäänestämisestä ... 6

5.1 Lohkoketjukokeilut Moskovassa 6

5.2 Agora 7

5.3 Voatz 7

6 Esitetyt järjestelmät ... 8

6.1 Hajautettu verkkoäänestysjärjestelmä 8

6.2 Auditable Blockchain Voting System 8

6.3 Ethereum-äänestysjärjestelmä 9

6.4 Chaintegrity 10

6.5 Voting Management System 10

6.6 Blockchain-enabled E-voting 11

7 Käytännön toteutuksen haasteita ... 12

8 Keskustelu ... 13

9 Yhteenveto ... 14

Lähdeluettelo ... 15

1 Johdanto

Äänestäminen on yksi tärkeimpiä demokraattisen järjestelmän peruspilareita (Mehta ja muut, 2021). Demokraattisessa äänestysprosessissa kerätään maan kansalaisilta heidän mielipiteensä asiaan äänen muodossa, jonka jälkeen äänet lasketaan ja äänestyksen voittaja ratkeaa sen mukaan, mitä enemmistö äänesti. Perinteisesti äänet on kerätty määrätyillä äänestyspaikoilla paperilapuille kirjoittamalla, jonka jälkeen laput tiputetaan uurnaan. Paperinen äänestysprosessi on kuitenkin melko hidas ja vaatii suuren määrän työntekijöitä vahtimaan, että jokainen saapuva äänestäjä toimii etiketin mukaan, mutta sen lisäksi äänten laskuun vaadittava työmäärä on valtava. Lisäksi juuri ääniä laskiessa on myös mahdollista vahingossa tai tahallaan muokata äänestystuloksia, riippuen toki paikalla olevasta valvonnan tasosta (McCorry ja muut, 2021).

Edistysaskeleeksi perinteiseen paperiäänestämiseen on esitetty internetin välityksellä tapahtuvaa elektronista äänestämistä, joka vapauttaa työvoimaa itse äänestyspaikalta ja äänien laskusta automatisoimalla prosesseja ja suorittamalla äänten laskun automaattisesti (Mehta ja muut, 2021). Äänten automaattinen lasku myös vaikeuttaa äänten määrän manipulointia. Mutta elektronisessa äänestyksessä on myös huonot puolensa: koska tietojärjestelmät ovat keskitettyjä, on se helppo kohde kyberhyökkäyksille (Khanpara ja muut, 2022). Elektroniseen äänestysjärjestelmään on myös todella helppo kohdistaa palvelunestohyökkäyksiä, joiden tarkoitus on kuormittaa palvelimet jolloin ne kaatuvat tai niiden saatavuus rajoittuu äänestäjille (Wei & Wen, 2018).

Ratkaisuna elektronisen äänestyksen haavoittuvaisuuteen on viime vuosina noussut uusi teknologia nimeltä lohkoketju, joka käyttää hajautettua kirjanpitoteknologiaa. Tietokanta muodostuu useista keskenään kommunikoivista solmuista (node) jotka operoivat konsensusmekanismilla, eli vaikka hakkeri pääsisikin käsiksi solmuun, ei yhden solmun hallussapito riittäisi, sillä solmut tarkistavat kaikki solmut koko järjestelmästä ja lopulta vallitseva tila on se, joka löytyy suurimmasta osasta solmuja. Käytännössä siis hakkerin olisi pidettävä hallussaan yli puolet solmuista, joka on lähes mahdotonta, jos järjestelmässä vain on käytössä riittävä määrä solmuja. (Huang ja muut, 2022)

Lohkoketjuteknologian käyttöönotto äänestystarkoituksiin takaa äänestäjän anonyymiteetin, tietoturvan sekä äänestystulosten läpinäkyvyyden ja muuttumattomuuden (Koštál

ja muut, 2019). Teknologian käyttöönotto kansallisen äänestyksen kontekstissa on kuitenkin kaikkea muuta kuin ongelmaton. Lohkoketjun tarjoama tietoturva perustuu sen ratkaisemiin monimutkaisiin yhtälöihin ja laskelmiin, jotka ovat todella energiaintensiivisiä ja niiden ajaminen tietokoneella on loppujen lopuksi melko kallista (Jafar ja muut, 2021). Nimenomaan lohkoketjujen konsensusmekanismi, joka varmistaisi äänestysten muuttumattomuuden vaatii paljon laskentatehoa ja on epäselvää, onko teknologiaa mahdollista ottaa käyttöön kansallisessa äänestyksessä (Park ja muut, 2021).

Park ja muut (2021) esittävät myös, että lohkoketjuteknologia tuo mukanaan myös uusia ongelmia, jotka puuttuvat muista edellä mainituista äänestysjärjestelmistä: hajautettu järjestelmä tarkoittaa käytännössä, ettei ole olemassa tiettyä auktoriteettia, joka on vastuussa toiminnasta. Ongelmatilanteen sattuessa vaaditaan uudenlaista koordinaatiota, joka vuorostaan hidastaa prosesseja. Näin ollen lohkoketjujärjestelmässä havaittujen epäkohtien korjaaminen vie enemmän aikaa ja vaivaa ja samalla lisää koko järjestelmän haavoittuvaisuutta. Lisäksi heidän mukaansa uuden äänestysjärjestelmän käyttöönotto saattaa vieraannuttaa käyttäjiä ja että siirtyminen elektroniseen äänestämiseen suosii korkeatuloisia ja korkeammin koulutettuja. (Park ja muut, 2021)

Tutkimuskysymykseni on: ”Mitä hyviä ja huonoja puolia liittyy hajautetun lohkoketjuteknologian käyttöönottoon äänestysprosessissa?” Tutkielmassa tarkoituksena on tarjota yleinen käsitys lohkoketjun mahdollisuuksista liittyen äänestämiseen ja tietoturvaan, mutta samalla kartoittaa hieman teknologian käytännöllisyyttä ja kannattavuutta äänestämisen käyttötapauksessa. Minkälaisia epävarmuuksia käytännön toteuttamiseen liittyy ja onko näillä tiedoilla mahdollista ottaa täysimittaista järjestelmää käyttöön?

Luvussa kaksi käyn läpi tutkimusmenetelmääni, muun muassa sitä, mistä ja miten löysin lähteeni. Paperi- ja elektronisen äänestämisen kompastuskiviä käsittelen luvussa kolme. Sen jälkeen esittelen lohkoketjuteknologian tarkemmin luvussa neljä ja avaan siihen liittyvää käsitteistöä. Lisäksi käsittelen sen sisäisiä mekanismeja ja tarkastelen, minkälaisia eri lohkoketjuja on mahdollista toteuttaa ja mitä aiheen tutkijat ovat mieltä siitä, mikä olisi paras ratkaisu äänestyksen kontekstissa. Kun käsitteistö ja perusideat lohkoketjuihin liittyen ovat tulleet tutuksi, luvussa viisi tarkastelen aikaisempia lohkoketjujärjestelmien kokeiluja ympäri maailmaa. Luvussa kuusi tarkastelen tutkijoiden kehittämiä järjestelmien luonnoksia. Luvussa seitsemän käyn läpi tutkimuksen tuloksia ja tutkijoiden havaitsemia ongelmia käytännön toteutuksessa. Lopuksi luvuissa kahdeksan ja yhdeksän tuon esille omaa pohdintaa aiheesta ja vedän tutkielman yhteen.

2 Tutkimusmenetelmä

Tutkielma on kirjallisuuskatsaus, joten se pohjautuu kokonaan aikaisempaan tutkimukseen ja sen tarkoituksena on saada kuva siitä, mitä valitsemastani aiheesta tällä hetkellä tiedetään. Etsin kirjallisuutta pääosin Tampereen Yliopiston Andor-tietokannasta, mutta käytin myös Institute of Electrical and Electronics Engineers -järjestön (IEEE) sähköistä tietokantaa sekä Googlen Scholar-palvelua. Tein haut pelkästään englannin kielellä, sillä tajusin nopeasti, ettei suomen kielellä ole oikeastaan ollenkaan julkaistua sisältöä aiheeseeni liittyen. Käyttämiäni hakusanoja oli muun muassa ”blockchain”, ”voting”, ”e-voting”, ”decentralized”, ”e-democracy”, ”digital governance”. Yhdistelin hakusanoja ”AND” ja ”OR” -operaattoreiden kanssa ja hankin lisää kokeiltavia hakusanoja kirjoittamalla osuvista tutkimuksista löytyvät avainsanat talteen. Huomasin kuitenkin, että relevantit tutkimukset löytyivät melko helposti, enkä tarvinnut kovin laajaa hakusanastoa löytääkseni tarpeelliset tiedot.

Hakutuloksia löytyi melko paljon, useita kymmeniä ja joskus jopa satoja joka hakusanalla, joten tein artikkeleiden karsimisen silmämääräisesti: luin artikkelin tiivistelmän, jonka jälkeen otin kaikki hyvältä vaikuttavat lähteet Excel-taulukkoon. Sen jälkeen aloin lukea artikkeleita läpi ja kirjoitin jokaisesta artikkelista ylös muistiinpanot myöhempiä työvaiheita varten ja samalla otin ylös artikkelin käytettävyyden merkkaamalla rivin värillä: vihreä tarkoittaa että lähde on hyvä ja käytettävissä, punainen että lähde menee ohi aiheeni ja keltainen että artikkelissa voi olla jotain, josta on hyötyä. Kun olin lukenut kaikki keräämäni artikkelit kertaalleen läpi, hain uusilla hakusanoilla ja toistin koko prosessin pariin kertaan.

Löytämäni artikkelit ovat todella uusia, vanhin on vuodelta 2018 ja uusin vuodelta 2022 joten koen niiden olevan edelleen hyvinkin relevantteja. Mukana on paljon konferenssijulkaisuja, joista sain paljon tutkijoiden suunnittelemia äänestysjärjestelmiä. Konferenssijulkaisuissa puhuttiin myös paljon tähänastisista lohkoketjuäänestämisen kokeiluista. Aineiston analyysin tein artikkelista kirjoittamieni muistiinpanojen pohjalta. Niiden avulla oli helppo ryhmittää artikkeleita ja luonnostella tutkielman rakennetta.

3 Äänestysjärjestelmien ongelmia

Perinteinen paperiäänestämisprosessi Suomessa kulkee niin, että äänestäjä saapuu äänestyspaikalle, jossa hänet osoitetaan äänestyskoppiin, jonne hän menee kirjoittamaan ää-

nensä. Sen jälkeen hän ojentaa äänensä äänestyspaikalla toimivalle virkailijalle, joka laittaa äänen uurnaan. Äänten keräämisen jälkeen henkilökunta laskee saadut äänet, merkkaa tuloksen ylös ja ilmoittaa tuloksen eteenpäin. Koko prosessi vaatii paljon ulkopuolisen ihmisen läsnäoloa ja työpanosta, joka mahdollistaa äänestystuloksien tahattoman tai tahallisen vääristämisen (Farooq ja muut, 2022; Huang ja muut, 2022). Saatuja ääniä voidaan peukaloida, mutta myös äänien mielivaltainen lisääminen on mahdollista (McCorry ja muut, 2021). Kaikki tapahtuu piilossa äänestäjiltä, eikä ole varmuutta siitä, rekisteröitiinkö annettu ääni kuten oli tarkoitettu.

Elektroninen äänestäminen (jatkossa lyhennettynä ”e-äänestäminen”) on 2000-luvulla herättänyt mielenkiintoa ja sitä on pidetty ratkaisuna paperiäänestämisen puutteisiin (Mehta ja muut, 2021). Sen sijaan että ihminen käsittelisi ja laskisi äänet, tapahtuu äänestys internetin välityksellä, jolloin tietokone suorittaa toimenpiteet. E-äänestyksessä on oltava todella varma tietoturva, jotta ääniä ei päästä muuttamaan tai poistamaan. Lisäksi äänestäjän anonyymiys on suojattava. Wein & Wenin (2018) mukaan e-äänestykseen kohdistuu suuri tietoturvariski, sillä ne perustuvat keskitettyyn tietojärjestelmään, jotka ovat alttiita esimerkiksi palvelunestohyökkäyksille, joiden tarkoituksena on kuormittaa palvelin, jotta äänestäminen ei onnistu järjestelmän kautta.

4 Lohkoketjuteknologia

Vuonna 2008 Satoshi Nakamoton keksimä Bitcoin-kryptovaluutta toi lohkoketjun koko maailman tietoon (Wei & Wen, 2018). Lohkoketju on hajautettu kirjanpitoteknologia, johon voidaan lisätä kopioita uusista tilikirjoista, (ledger) jos ne täyttävät lohkoketjun kriteerit (Khanpara ja muut, 2022). Lohkoketju toimii konsensusmenetelmällä, eli se koostuu useista solmuista (node) joilla on tiedossa täysi varmuuskopio kaikista järjestelmässä tapahtuvista muutoksista (Huang ja muut, 2022). Jos yksi solmu kaatuu tai esimerkiksi hakkeri pääsee muokkaamaan solmun tietoja, ei yksittäinen solmu riitä järjestelmän tietojen muokkaamiseen: solmut kommunikoivat keskenään ja tietävät, että vaikka yhdessä solmussa tieto muuttui, suurimmassa osassa se säilyi samana (Huang ja muut, 2022). Jotta hakkeri siis pystyisi hallitsemaan järjestelmää, tulee hänellä olla hallussaan yli puolet solmuista, joka on lähes mahdoton skenaario, jos järjestelmä on perustettu riittävällä määrällä solmuja (Huang ja muut, 2022).

Järjestelmän hajautus siis takaa todella korkean tietoturvallisuuden, mutta sen lisäksi lohkoketju toimii ”append only” -periaatteella, eli sinne voi ainoastaan lisätä kriteerit täyttävää tietoa. Sen jälkeen tietoa on mahdotonta muokata ja näin lohkoketju säilyy muuttumattomana. Koska lohkoketju on hajautettu ja muuttumaton, voidaan turvallisin mielin taata kelle tahansa lupa tarkastella ja tutkia lohkoketjussa tapahtuvaa vuorovaikutusta. Näin ollen julkinen lohkoketju on myös läpinäkyvä. (Huang ja muut, 2022)

4.1 Lohkoketjujen luokittelu

Lohkoketjuja on kolmea erilaista: julkinen, yksityinen ja hybridi (Huang ja muut, 2022). Julkinen lohkoketju ei vaadi lupaa, jos joku haluaa liittyä siihen tai lisätä dataa, kunhan lohkoketjuun asetetut vaatimukset täyttyvät (Huang ja muut, 2022). Kaikilla solmuilla on tasavertainen pääsy lohkojen tietoihin ja lohkoketju on täysin hajautettu. Yksityisessä lohkoketjussa solmulla tulee olla lupa, että se voi kirjoittaa lohkoon ja silloinkin tämä voi kirjoittaa vain yhteen tiettyyn tilikirjaan (Khanpara ja muut, 2022). Hybridilohkoketjussa vain ennalta määrätyt käyttäjät tai organisaatiot pääsevät kirjoittamaan lohkoketjuun (Khanpara ja muut, 2022).

4.2 Konsensusmekanismit

Konsensusmekanismeja on lohkoketjun piirissä monenlaisia, mutta yksinkertaisuuden vuoksi käsittelen tässä kahta yleisimmin käytössä olevaa. Proof of Work (PoW) on kaikkein yleisin konsensusmekanismi jonka lohkoketjuista löytää ja muun muassa Bitcoinin konsensus perustuu Proof of Work-mekanismiin. Verkoston solmut kilpailevat keskenään siitä, että saisivat lisätä uuden lohkon tilikirjaan. Tämä kilpailu, joka tunnetaan myös nimellä ”mining” tapahtuu suorittamalla laskentatehollisesti vaativia tehtäviä. Laskentatehon korkea vaatimus on samalla Proof of Workin vahvuus ja heikkous, sillä siinä missä on käytännössä mahdotonta saada 51 % solmuista hallintaan jotta järjestelmää voisi käyttää mielivaltaisesti, vie uuden tiedon käsittely myös todella paljon aikaa, joka hidastaa koko lohkoketjun toimintaa huomattavasti. (Huang ja muut, 2022)

Uudempi konsensusmekanismi, Proof of Stake (PoS) ei vaadi niin paljon laskentatehoa kuin PoW, mutta samalla se ei ole yhtä turvallinen (Huang ja muut, 2022). Siinä konsensus määräytyy sen mukaan, millä solmulla on eniten osuutta (kolikoita) järjestelmässä (Park ja muut, 2021).

PoW on avoin kaikille ja anonyymiys järjestelmässä säilyy. PoS:ssä taas tarvitsee ensin kolikoita, jotta voi sitten osallistua kilpailemaan kirjanpito-oikeuksista. Jotta kolikot voi

alun perin saada, täytyy olla yhteydessä muihin, joka heikentää anonyymiyttä ja vuorostaan nostaa kynnystä osallistua. Tietokonetehoa PoS taas vaatii vähemmän kuin PoW ja sen lisäksi uusien lohkojen luonti verkostoon on nopeampaa. (Huang ja muut, 2022)

4.3 Älysopimus

Älysopimus (smart contract) on automaattinen ennalta määrätty ohjelmistosopimus, joka solmitaan, kun sopimukseen asetetut ehdot täyttyvät (Zhang ja muut, 2020). Konseptin keksi ensimmäisen kerran Nick Szabo vuonna 1994 (Huang ja muut, 2022). Älysopimuksen soveltaminen lohkoketjuteknologiaan on turvallista, sillä konsensusmekanismin ja hajautetun rakenteensa vuoksi lohkoketju pitää huolen siitä, että tieto siellä pysyy muuttumattomana ja se on helppo jäljittää. Älysopimus lohkoketjuteknologiapohjaiseen äänestysjärjestelmään sovellutettuna mahdollistaa sen, että äänien vastaanottamiseen tai laskemiseen ei tarvita turhia välikäsiä, kunhan äänestäjä täyttää sopimuksen asetetut ehdot, kuten täysi-ikäisyyden ja maan kansalaisuuden (Zhang ja muut, 2020).

5 Nykyiset toteutukset lohkoketjuäänestämisestä

Tässä luvussa esittelen lohkoketjukokeiluita, joita on toteutettu ympäri maailmaa antaakseni suuntaa lohkoketjuteknologiaan perustuvien äänestysjärjestelmien nykytilanteesta. En löytänyt artikkeleista viitteitä siitä, että lohkoketjupohjaista äänestysjärjestelmää olisi testattu koko valtion mittakaavassa, vaan kyse on ollut paikallisista tai osittaisista kokeiluista.

5.1 Lohkoketjukokeilut Moskovassa

Vuonna 2014 Venäjällä aloitettiin Moscow's Active Citizens, eli Moskovan aktiiviset kaupunkilaiset-ohjelma, jonka tarkoituksena on lisätä ihmisten osallistumista jokapäiväisten asioiden päättämiseen (Kshetri & Voas, 2018). Asiat voivat koskea esimerkiksi uuden stadionin penkkien värejä tai junien nimeämistä (Huang ja muut, 2022). Poliittisia päätöksiä järjestelmän kautta ei siis tehdä. Moskovassa pidetään vuosittain 5000-7000 kokousta ja ohjelmaan osallistuu yli kaksi miljoonaa käyttäjää. Joulukuussa 2017 järjestelmä uudistettiin ja se toimii nykyään lohkoketjupohjaisessa verkossa (Kshetri & Voas, 2018). Järjestelmä uusittiin, sillä aikasemman järjestelmän avulla kerättyjen äänien paikkansapitävyyttä epäiltiin (Huang ja muut, 2022).

Moskovassa kokeiltiin lohkoketjuäänestämistä myös vuoden 2019 kuntavaaleissa. Ohjelmiston koodia annettiin tietoturva-asiantuntijoiden arvioitavaksi, mutta siitä huolimatta

järjestelmästä löydettiin haavoittuvaisuuksia kahteen otteeseen, vaikka järjestelmään oli ehdotettu korjauksia. (Park ja muut, 2021)

5.2 Agora

Agora on sveitsiläinen startup-yritys, joka perustettiin vuonna 2015 ja se suoritti lohkoketjukokeilun Sierra Leonen vuoden 2018 vaaleissa (Kshetri & Voas, 2018). Kyseessä ei ollut täysin hajautettu eikä täysimittaisen äänestysjärjestelmän toteutus, vaan enemmänkin osittainen kokeilu (Koštál ja muut, 2019). Äänestäjien henkilöllisyys vahvistettiin henkilökortilla ja äänestys toteutettiin paperilla. Saadut äänet lisättiin Agoran yksityiseen lohkoketjuun ja äänet laskettiin sekä käsin että lohkoketjun avulla (Koštál ja muut, 2019). Tarkoituksena oli testata teknologiaa mutta samalla myös tarjota äänestykseen itsenäinen taho äänten laskuun (Kshetri & Voas, 2018).

Agora koostuu viidestä eri kerroksesta: Bulletin Board-lohkoketju, Cotena, Bitcoin-lohkoketju, Valeda-verkosto ja Votapp (Mehta ja muut, 2021). Bulletin Board on yksityinen lohkoketju, johon kaikki järjestelmän data on tallennettu. Cotena tallentaa ajoittain tilannekatsauksen Bulletin Boardista julkiseen ja hajautettuun Bitcoin-lohkoketjuun, jonne on vapaa pääsy tarkastella ja varmistaa tallennetut tiedot (Mehta ja muut, 2021). Valeda-verkosto taas laskee ja tarkastaa tuloksen vertailemalla sitä Bitcoin-lohkoketjun tuloksiin. Votapp taas toimii sovelluksen käyttöliittymänä.

5.3 Voatz

Voatz on yritys Bostonista, Yhdysvalloista, jonka lohkoketjujärjestelmän kautta eri organisaatiot voivat äänestää. Voatz toimii joko nettiselaimen tai mobiilisovelluksen kautta ja yritys ylläpitää omaa lohkoketjuverkkoaan, jonka kautta äänestykset järjestetään. Kokeiluäänestyksiä Voatzin kautta on järjestetty Länsi-Virginian osavaltiossa 2018 ja Utahin osavaltiossa vuonna 2020. Äänestys tehdään Voatzin tilin kautta, johon äänestäjä määrittää 8-numeroisen PIN-koodin. Sen jälkeen tili vahvistetaan valtion myöntämällä henkilökohtaisella dokumentilla. Sovellukseen äänestäjä lataa kuvan itsestään. Äänestyksessä tunnistaudutaan joko kasvojen tai PIN-koodin perusteella. (Mehta ja muut, 2021)

Voatzissa on kuitenkin paljon tietoturvaongelmia, liittyen erityisesti kyberhyökkäyksien torjumiseen: Sovellus käyttää rajapintaa välikätenä kommunikoidakseen lohkoketjun kanssa, sen sijaan että se olisi suoraan yhteydessä lohkoketjuun (Mehta ja muut, 2021). Haavoittuvaisuuksien vuoksi hyökkääjä pystyy estämään annettujen äänten laskemista

mutta myös muuttamaan niitä huomaamatta (Park ja muut, 2021). Sovellukseen rekisteröitymisen ja identiteetin vahvistamisen on kuvailtu olevan epäluotettava (Mehta ja muut, 2021).

6 Esitetyt järjestelmät

Tässä luvussa tulen käsittelemään tutkijoiden erilaisia ehdotuksia lohkoketjuun perustuvan äänestämisjärjestelmästä. Kirjallisuus on koottu eri artikkeleista ja konferenssijulkaisuista ja niiden yksityiskohtaisuus vaihtelee.

6.1 Hajautettu verkkoäänestysjärjestelmä

Lalitha ja muut (2022) esittävät hajautettua, Ethereum-pohjaista äänestysjärjestelmää Intian kontekstiin. Siinä hyödynnetään älysopimusta, jolla varmistetaan äänten oikeellisuus ja että jokainen äänestää vain kerran. Järjestelmässä äänestäjän vahvistus toimii monella tasolla: Jotta äänestykseen voi rekisteröityä, täytyy olla ”Aadhar”, eli henkilökohtainen tunnistautumista varten luotu sarjanumero. Intian valtio on vastuussa Aadhar-tunnisteiden jakelusta ja ylläpidosta. Äänestäjä vastaanottaa tekstiviestin puhelinnumeroonsa, jonka hallinto sai Aadharin tiedoista. Tekstiviesti sisältää kertaluontoisen tunnistautumislinkin, jonne syötetään Aadharin sarjanumero. Kun henkilöllisyyden vahvistaminen on valmis, suoritetaan kasvojen tunnistus ja otetaan sormenjälki. Tunnistusten mentyä läpi pääsee suorittamaan äänestyksen. (Lalitha ja muut, 2022)

Äänestäjien anonymiteetti on turvassa, sillä äänestysoikeus on vain niillä, jotka ovat rekisteröityneet Aadhar-tunnusta varten, joiden tiedot säilyttää Intian valtio. Kasvojentunnistus on lisätty järjestelmään, jotta varmistetaan, ettei kukaan äänestä kahta kertaa. Lohkoketju takaa myös äänten muuttumattomuuden ja annettujen äänten vapaan tarkastelun. Yhdeksi ongelmaksi Lalitha ja muut (2022) ovat tunnistaneet sen, että järjestelmä tarvitsee internetyhteyden toimiakseen ja se ei ole aina saatavilla kaikkialla Intiassa. Lisäksi ihmiset, joilla ei ole kokemusta tietotekniikasta voivat vieraantua äänestysjärjestelmästä. (Lalitha ja muut, 2022)

6.2 Auditable Blockchain Voting System

Pawlak ja muut (2018) käsittelevät artikkelissaan järjestelmää nimeltä Auditable Blockchain Voting System (ABVS). Lohkoketjujärjestelmä koostuu kolmesta osasta:

- *Supersolmu* on suoraan valtion viranomaisten hallinnassa. Supersolmu lisää kaikki saadut äänet lohkoketjuun ja myös äänten lasku tapahtuu sen kautta.
- *Luotetut solmut* ovat lohkoketjussa valtion hyväksymiä solmuja. Luotettujen solmujen tehtävänä on muodostaa konsensus ja kerätä kaikki annetut äänet.
- *Äänestyspaikka*, joissa kerätyt äänet annetaan luotettujen solmujen käsittelyyn. Pawlak ja muut (2018) tarkentavat, että tällä ei tarkoiteta fyysistä äänestyspaikkaa, vaan tietojärjestelmän osaa.

Vaikka Pawlak ja muut (2018) eivät sitä suoraan mainitsekaan, kyseinen järjestelmä on hybridilohkoketju, jolla on omistava, valvova ja hallinnoiva taho, tässä tapauksessa valtion viranomaiset. Tällöin äänestysprosessi ei kuitenkaan ole läpinäkyvä, eivätkä halukkaat kansalaiset pysty seuraamaan äänestystä. Sen sijaan valtio voi määrittää luotetuiksi solmuiksi tahoja, jotka se itse haluaa ottaa mukaan äänten valvontaan ja hallinnoimiseen, kuten esimerkiksi yliopistoja. (Pawlak ja muut, 2018)

Kun äänestämään saapunut henkilö on vahvistanut henkilöllisyytensä äänestyskopissaan, ottaa tämä kirjekuoren, joka sisältää yksilöllisen tunnuksen. Tunnuksen syöttämällä tämä voi antaa äänensä ja ääni lähetetään lohkoketjuun. Onnistuneen äänestyksen jälkeen käyttäjälle tulostetaan vahvistuspaperi, joka toimii äänen tallentamisen varmistumisena. (Pawlak ja muut, 2018)

6.3 Ethereum-äänestysjärjestelmä

Puneet ja muut (2021) esittävät artikkelissaan luonnoksen Ethereum-pohjaisesta äänestysjärjestelmästä, joka on julkinen ja hajautettu. Järjestelmän luonnos käyttää PoW-konsensusmekanismia ja Ethereum-alusta mahdollistaa älysopimusten hyödyntämisen äänten vastaanottamiseen. Äänestys tapahtuu internetin välityksellä, joten se on mahdollista myös älypuhelimella ja tietokoneella. (Puneet ja muut, 2021)

Äänestysjärjestelmä pohjautuu Ethereum Virtual Machineen (EVM), joka sekä suorittaa ääntenlaskun että vahvistaa äänet. Kun järjestelmään lisätään ääni, luodaan sille uusi lohko. Lohkon ääni vahvistetaan oikeaksi, salataan äänestäjän identiteetti ja lisätään osaksi ketjua. Äänten lasku tapahtuu reaaliajassa ja päivittyy joka kerta, kun lohkoketjuun lisätään uusi ääni. (Puneet ja muut, 2021)

6.4 Chaintegrity

Chaintegrity on hybridilohkoketju, joka hyödyntää älysopimuksia äänten vastaanottamiseen (Zhang ja muut, 2020). Vaaleja ylläpitää useampi luotettu taho samalla tavalla kuin ABVS-järjestelmässä (Pawlak ja muut, 2018). Kaikilla ihmisillä ei siis ole lupaa tarkastella lohkoketjuun annettuja ääniä, varsinkaan reaaliajassa. Zhang ja muut (2020) perustelevat artikkelissaan, että yksittäisen solmun ja tapahtuman etsiminen lohkoketjusta olisi äärimmäisen aikaavievää. Zhang ja muut (2020) esittävät luotettujen tahojen lisäksi vaaleissa olevan mukana myös raati, joka ajaa kansan asiaa ja valvoo äänestysprosessin paikkansapitävyyttä.

Äänestyksessä kansalaisille jaetaan sekä yksityinen että julkinen avain, joita he tulevat käyttämään myös muissa vaaleissa. Näillä avaimilla he tunnistautuvat ja osallistuvat äänestykseen. Käyttäjä voi antaa äänensä, kun tunnistautuminen on mennyt läpi, jonka jälkeen lohkoketjun älysopimus vastaanottaa ja laskee äänen järjestelmään. Kun äänestysaika on ohi ja kaikki äänet on laskettu, lopullinen tulos julkaistaan lohkoketjuun, josta luotetut tahot voivat paljastaa vaalituloksen kansalle. (Zhang ja muut, 2020)

Zhang ja muut (2020) esittävät artikkelissaan, että heidän järjestelmänsä pystyisi vastustamaan yleisimpiä hyökkäyksiä, kuten palvelunestohyökkäyksiä juuri lohkoketjun hajautetun rakenteen ansiosta, mutta tavallisten hyökkäysten lisäksi juuri hajautettuja verkkoja vastaan käytetty ”Sybil”-hyökkäys torjuttaisiin hybridirakenteen avulla, jossa vain vahvistetuilla tahoilla on pääsy lohkoketjuun.

6.5 Voting Management System

Farooqin ja muiden (2022) ehdottama Voting Management System (VMS) on mobiilisovellus- tai selainpohjainen ja se hyödyntää älysopimuksia ja toimii ensisijaisesti PoW-konsensuksella. VMS on yksityinen lohkoketju, joten sitä hallitsee ja valvoo vain yksi taho, tässä tapauksessa valtio. Järjestelmä on viisikerroksinen, jonka lisäksi kaikkia kerroksia valvoo turvallisuuskerros:

- *Käyttöliittymäkerros* on lähimpänä käyttäjää. Se tarjoaa graafisen käyttöliittymän, jonka kautta käyttäjä operoi ohjelmaa.
- *Sovelluskerros* on linkki käyttöliittymän ja lohkoketjun välillä. Se siirtää tiedot lohkoketjun käsiteltäväksi.

- *Luottamuskerros* pitää huolen, että solmujen konsensus muodostuu oikein ja tieto liikkuu turvallisesti älysopimusten välityksellä.
- *Lohkoketjukerros* säilyttää kaiken tiedon äänestykseen liittyen ja pitää huolen, että ketju säilyy muuttumattomana.
- *Tranaktiokerros* tarkastaa uudet solmulisäykset, kun uusi ääni lisätään. Sen lisäksi se on vastuussa solmujen louhinnasta.
- *Turvallisuuskerros* pitää huolen kaikista kerroksista ja suojelee niitä hyökkäyksiltä. Järjestelmä hyödyntää julkisia ja yksityisiä avaimia, joilla se suojelee toimintaansa ulkoisilta uhilta, mutta sen lisäksi algoritmit ja hajautettu lohkoketju turvaavat sisällä liikkuvan datan.

Järjestelmään rekisteröidytään valtiolta saaduilla tunnuksilla. Kun järjestelmään on kirjauduttu tunnuksilla, generoidaan käyttäjälle kertakäyttöinen koodi, jolla vahvistetaan henkilöllisyys vielä kertaalleen. Jokaista äänestystä varten äänestäjille generoidaan yksi kertakäyttöinen kolikko, jolla osallistua äänestykseen. Kolikon käyttämisen jälkeen käyttäjä ohjataan näkymään, jossa äänestäminen tapahtuu. Kun käyttäjä antaa äänensä järjestelmä tarkistaa vielä kerran, onko käyttäjä äänestänyt vaaleissa ja sen jälkeen lähettää äänen lohkoketjuun, jos näin ei ole. (Farooq ja muut, 2022)

6.6 Blockchain-enabled E-voting

Blockchain-enabled e-voting (BEV) on Wein & Wenin (2018) suunnittelema julkinen lohkoketjujärjestelmä, joka toimii joko tietokoneella tai mobiililaitteella. Äänestysprosessia pystyy valvomaan kuka tahansa joten äänten oikeellisuuden varmistaminen on helppoa. Wei & Wen (2018) esittelevät artikkelissaan yksinkertaisen luonnoksen järjestelmän toiminnasta.

Kun äänestysohjelmistoa otetaan käyttöön ensi kertaa, generoidaan käyttäjälle julkinen ja yksityinen avain. Äänestystilanteessa käyttäjä syöttää laitteeseen henkilökohtaiset tietonsa, kuten henkilötunnus, osoite ja syntymäaika. Palvelin vahvistaa tiedot ja generoi käyttäjälle käyttäjän julkisella avaimella kryptatun äänestystunnuksen. Käyttäjän tulee purkaa tunnuksen salaus yksityisellä avaimellaan, ennen kuin tunnusta voi käyttää. Tämä estää identiteettivarkauden, vaikka joku sattuisikin tietämään toisen ihmisen henkilökohtaiset tiedot. Kun annettu ääni ja äänestystunnus on palvelimen päässä vahvistettu, hyväksytään ääni. (Wei & Wen, 2018)

7 Käytännön toteutuksen haasteita

Lohkoketjun käyttö äänestämiseen ei kuitenkaan ole täysin ongelmatonta. Kuten esittelemistäni kokeiluista kävi ilmi, jopa paikallisiin tai alueellisiin lohkoketjutestauksiin on liittynyt erilaisia haasteita (Park ja muut, 2021; Mehta ja muut, 2021). Yksi keskeinen asia, joka jäi artikkeleissa ja laadituista äänestysjärjestelmissä usein huomiotta, on järjestelmän skaalautuvuus. Khudoykulov ja muut (2021) julkaisussaan esittävätkin, että pieniin kokeiluihin lohkoketju voi toimia hyvin, mutta kasvaessaan järjestelmä hidastuu valtavasti ja sen käyttö maksaa enemmän. Tämä johtuu lohkoketjun hajautetusta luonteesta ja konsensusmekanismista, sillä kasvaessaan jokaisen solmun on louhittava läpi kaikki uudet lisäykset ketjuun (Jafar ja muut, 2021). Nykyisellään, Ethereum-pohjainen äänestysjärjestelmä voi ottaa vastaan vain viisi ääntä minuutissa (McCorry ja muut, 2021). Tämä on luonnollisesti täysin riittämätön, kun kansallisiin äänestyksiin osallistuu miljoonia tai jopa satoja miljoonia äänestäjiä. McCorry ja muut (2021) käyttävät esimerkkinä Ison-Britannian vuoden 2016 äänestystä, jossa äänestettiin EU:n jäsenmaana pysymisestä. Äänestyksessä tuli postitse 5.2 miljoonaa ääntä, joiden laskemisessa Ethereum-järjestelmällä menisi 722 päivää (McCorry ja muut, 2021).

Parkin ja muiden (2021) mukaan lohkoketjun hajautettu rakenne tuo myös hallinnollisia vaikeuksia. Koska järjestelmä on jaettu pieniin osiin, voi ongelmien ja puutteiden paikkaaminenkin heidän mukaansa viedä todella paljon aikaa, mutta sen lisäksi vaatii erityistä koordinointia, jotta ongelmat saadaan korjattua. Esimerkkinä he mainitsevat erään Bitcoin-verkoston haavoittuvaisuuden, joka mahdollisti palvelunestohyökkäyksen järjestelmän solmuja kuormittamalla. Tieto haavoittuvaisuudesta julkistettiin vuonna 2018 ja kaksi vuotta myöhemmin 27 % Bitcoin-pohjaisista järjestelmistä eivät olleet korjanneet haavoittuvaisuutta.

Park ja muut (2021) kyseenalaistavat myös koko tarpeen hajautetuille vaaleille, sillä vaaleja järjestää keskitetyn vallan taho, eli maan hallitus. Saman huomion nostavat esille myös Khudoykulov ja muut (2021) sekä Jafar ja muut (2021): Saisiko kansallisten vaalien hajauttaminen itsenäisille osapuolille ikinä suurta tukea maan hallitukselta, joka hyötyy vaalien keskittämisestä? Monet toteutetut lohkoketjutestit, kuten Agora (Koštál ja muut, 2019; Mehta ja muut, 2021) ja Voatz (Mehta ja muut, 2021) ovat kuitenkin olleet yksityisiä lohkoketjuja yhden tahon hallinnassa. Lisäksi esitellyistä järjestelmistä useimmat ovat joko hybridejä tai täysin yksityisiä lohkoketjuja. McCorry ja muut (2021) ovat sitä

mieltä, että näin kuuluukin olla, sillä kansalliset äänestykset ovat luonnostaan keskitettyjä.

Teknologian nuoruus on myös otettava huomioon: lohkoketjut ovat olleet tiedossa vasta muutamia vuosia ja sen ymmärtäminen varsinkin tavallisten ihmisten keskuudessa on hyvin alhaista (Khudoykulov ja muut, 2021; Jafar ja muut, 2021). Jotta uuden teknologian käyttöönotto ei vieraannuta äänestäjiä pois, on tutkimuksella ja tiedottamisella vielä pitkä matka edessään. Park ja muut (2021) viittaavat tutkimuksiin, joiden tulosten mukaan elektronisen äänestämisen käyttöönotto saattaa jopa laskea äänestysprosentteja vaaleissa. Lisäksi on huomattu, että elektronisiin vaaleihin osallistuminen on todennäköisempää korkeatuloisten ja korkeasti koulutettujen parissa (Park ja muut, 2021). Tämä epätasaarvo on huomioitava paperiäänestyksestä pois siirryttäessä.

8 Keskustelu

Jotta lohkoketjupohjainen äänestysjärjestelmä voidaan ottaa käyttöön, on tutkimuksella ja käytännön kokeiluilla vielä pitkä matka edessään. On tärkeä huomioida, että kaikki tähän mennessä suoritetut lohkoketjuäänestykset ovat tapahtuneet paikallisella tai alueellisella tasolla, joten ei ole tietoa siitä miltä laajentuminen kansalliselle tasolle tapahtuisi.

Tutkijat ovat myös esitelleet monia itse luonnostelemiaan malleja, joista jokainen on kirjottajiensa mielestä paras mahdollinen järjestelmä. Monet artikkeleista ovat enemmän yleisiä esityksiä tietojärjestelmän rakenteesta ilman syvempää pureutumista esimerkiksi tietoturvallisuusongelmiin. Ehkä pieni epäkriittisyys omaa suunnitelmaa kohtaan näkyi joissakin artikkeleissa.

Lisäksi luonnosteltujen järjestelmien ja oikean elämän kokeilujen välillä oli valtava ero: konferenssijulkaisuja ja artikkeleita suunnitelluista toteutuksista löytyi paljon, joista muutaman yksityiskohtaisimman esittelin aiemmin. Oikeasti suoritetuista äänestyskokeiluista löysin maininnan vain noin kymmenestä, joista kaikista löytyi hyvin rajallinen määrä tietoa. Mielestäni tämä kertoo lohkoketjuteknologian nuoruudesta ja siitä, että kaikki ovat innoissaan esittelemässä oman äänestysmallinsa, mutta käytännön toteutus ja todellinen aiheeseen pureutuminen on jäänyt vähälle.

Artikkeleissa jätettiin kokonaan huomiotta eräs maailmassa vallitseva tosiasia eli ilmastokriisi. Samalla, kun planeettamme lämpenee liiallisesta kulutuksesta ja fossiilisten polt-

toaineiden käytössä, ehdotetaan käyttöön äänestysjärjestelmää, joka pohjautuu energiaintensiivisten laskelmien suorittamiseen. Mietin, että jos todella tällainen äänestysjärjestelmä otettaisiin käyttöön, mistä saadaan energia näiden laskujen suorittamiseen ja onko se todella kannattavaa.

Lisäksi artikkeleissa toistui ajatus siitä, että lohkoketjuäänestämisellä saataisiin pelastettua laskeneet äänestysprosentit, jotka ovat olleet vuosia laskussa ja että sillä voidaan innostaa kansalaiset osallistumaan päätöksentekoon. Vaikkakin äänestäminen älylaitteella tai tietokoneella olisi varmasti helpompaa kuin äänestyspaikalle meneminen, en näe tätä vaivan arvoisena tavoitteena, sillä esimerkiksi Suomessa eri vaaleja järjestetään yhden tai kahden vuoden välein. Näkisin laskevat äänestysprosentit ennemmin järjestelmällisenä ja poliittisena kriisinä kuin äänestystavan kriisinä. Tietokoneella tai puhelimella tapahtuva äänestäminen on mielekkäämpää niille, joilla on kokemusta laitteiden käytöstä. Ne, joilla ei ole tietoteknistä osaamista ovat vaarassa vieraantua äänestämisestä. Lisäksi on otettava huomioon, että lohkoketju on vielä uusi teknologia, eikä ihmisillä ole yleisesti aavistustakaan siitä, miten se toimii. Miten lohkoketjuun pohjautuva järjestelmä voisi siis nauttia kansan luottamusta?

9 Yhteenveto

Paperiäänestysprosessissa on pakko olla mukana paljon työntekijöitä, joka lisää tahallisen tai tahattoman virheen mahdollisuutta esimerkiksi ääntenlaskussa (Farooq ja muut, 2022; Huang ja muut, 2022). Elektroninen äänestäminen voisi olla ratkaisu automatisoimaan äänestysprosessin, mutta keskitettynä tietojärjestelmä on äärimmäisen haavoittuvainen erilaisille hyökkäyksille (Khanpara ja muut, 2022).

Lohkoketjuteknologia voisi tarjota hajautetun vaihtoehdon, jossa tietojärjestelmällä ei ole yhtä ainoaa hallitsijaa, vaan ylläpitovastuu on jaettu lukuisille solmuille. Rakenteensa ansiosta se on suojassa tavallisilta hyökkäyksiltä, sillä hyökkääjän olisi saatava hallintaansa yli puolet järjestelmän solmuista pystyäkseen muuttamaan tulosta. Lisäksi äänestysprosessi voitaisiin pitää julkisena ja avoimena kaikille halukkaille tarkastelijoille. (Huang ja muut, 2022)

Aiheesta on julkaistu paljon tieteellistä tutkimusta ja monet ovatkin esittäneet oman mallinsa, jonka mukaan äänestysjärjestelmä tulisi rakentaa. Käytännön kokeilut ovat kuiten-

kin rajattuja, käsitellen pelkästään paikallisia tai alueellisia testejä. Vaikka kokeilut ovatkin olleet vain pienen mittakaavan toteutuksia, on niissä silti havainnoitu tietoturvallisuusriskejä (Park ja muut, 2021; Mehta ja muut, 2021). Lohkoketjuteknologian skaalautuvuus kansallisen äänestyksen kontekstiin on hyvin epävarmaa (Khodoykulov ja muut, 2021). Lohkoketjun korkea tietoturvallisuus on saavutettu laskennallisesti intensiivisten yhtälöiden ratkaisemisella, joten miljoonien äänestäjien osallistuessa kansalliseen äänestykseen järjestelmä hidastuisi merkittävästi (Jafar ja muut, 2021). Lisäksi näiden laskujen suorittamiseen tarvittaisiin valtava määrä energiaa.

Lohkoketjuteknologia on vielä todella nuori teknologia ja ymmärrys sen toiminnasta on vähäistä. Jotta lohkoketjulla toimiva äänestysjärjestelmää voitaisiin harkita, tulisi kansan tietoisuus siitä olla paljon nykyistä laajempi, sillä muuten se vieraannuttaa äänestäjät. Aiheesta on tehtävä enemmän tutkimusta ja laajempia testauksia, ennen kuin voidaan sanoa, onko lohkoketjuteknologia käyttökelpoista äänestysjärjestelmän pohjaksi.

Lähdeluettelo

Farooq, M., Iftikhar, U. & Khelifi, A. (2022). A Framework to Make Voting System Transparent Using Blockchain Technology. *IEEE Access*, 10, 59959–59969. https://doi.org/10.1109/ACCESS.2022.3180168

Huang, J., He, D., Obaidat, M., Vijayakumar, P., Luo, M. & Choo K. (2022). The Application of the Blockchain Technology in Voting Systems: A Review. *ACM Computing Surveys, 54*(3), 1-28. https://doi.org/10.1145/3439725

Jafar, U., Aziz, M. & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*, 21(17), 5874. https://doi.org/10.3390/s21175874

Khanpara, P., Patel, S. & Valiveti, S. (2022). Blockchain-based E-Voting Technology: Opportunities and Challenges. *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, 855-861. https://doi.org/10.1109/ICCES54183.2022.9835721

Khudoykulov, Z., Tojiakbarova, U., Bozorov, S. & Ourbonalieva, D. (2021). Blockchain Based E-Voting System: Open Issues and Challenges. *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, 1–5. https://doi.org/10.1109/ICISCT52966.2021.9670245

Koštál, K., Bencel, R., Ries, M. & Kotuliak, I. (2019). Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain. *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, IEEE, 592–595. https://doi.org/10.1109/ICSESS47205.2019.9040770

Kshetri, N. & Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE Software*, 35(4), 95–99. https://doi.org/10.1109/MS.2018.2801546

Lalitha, V., Samundeswari, S., Roobinee, R. & Swetha, L. (2022). Decentralized Online Voting System using Blockchain. *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 1387–1391. https://doi.org/10.1109/ICAAIC53929.2022.9792791

McCorry, P., Mehrnezhad, M., Toreini, E. Shahandashti, S. & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, 2(4), 1–13. https://doi.org/10.1145/3461461

Mehta, C., Mehta, A., Gada, S. & Kadukar, N. (2021). Demystifying Democracy: Incentivizing Blockchain Voting Technology for an enriched Electoral System. *2021 International Conference on Communication Information and Computing Technology (ICCICT)*, IEEE, 1–8. https://doi.org/10.1109/ICCICT50803.2021.9510158

Park, S., Specter, M., Narula, N. & Rivest, R. (2021). Going from bad to worse: from Internet voting to blockchain voting. *Journal of cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyaa025

Pawlak, M., Poniszewska-Marańda, A. & Kryvinska, N. (2018). Towards the intelligent agents for blockchain e-voting system. *Procedia Computer Science*, 141, 239–246. https://doi.org/10.1016/j.procs.2018.10.177

Puneet, Chaudhary, A., Chauhan, N. & Kumar, A. (2021). Decentralized Voting Platform based on Ethereum Blockchain. *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 1–4. https://doi.org/10.1109/ICAECT49130.2021.9392580

Wei, C. & Wen, C. (2018). Blockchain-Based Electronic Voting Protocol. *International Journal on Informatics Visualization, 2*(4-2), 336-341. https://doi.org/10.30630/joiv.2.4-2.174

Zhang, S., Wang, L. & Xiong, H. (2020). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, 19(3), 323–341. https://doi.org/10.1007/s10207-019-00465-8