TARTU ÜLIKOOL
Arvutiteaduse instituut
Infotehnoloogia mitteinformaatikutele õppekava

Pirgit Pajoma

Plokiahela kasutamine avalikes e-teenustes Eesti näitel

Magistritöö (15 EAP)

Juhendajad: Jan Villemson, PhD
Kristjan Krips, PhD

Tartu 2024

Plokiahela kasutamine avalikes e-teenustes Eesti näitel

Lühikokkuvõte

Eesti on kõrgelt arenenud digitaalse infrastruktuuriga riik, kus suurem osa avalikest teenustest ja toimingutest on kättesaadavad veebis. Üheks edu võtmeks Eesti avalike e-teenuste arendamisel peetakse plokiahela kasutamist. Käesolev magistritöö uurib lähemalt plokiahela kasutamise tegelikku ulatust Eesti avalikes e-teenustes. Uurimismeetoditena kasutati süstemaatilist kirjanduse analüüsi, mille tulemusena valmis kirjanduse ülevaade, ning intervjuusid, mille tulemusena loodi ülevaade plokiahela tegelikust kasutamisest kolmes Eesti avalikus e-teenuses. See uurimus aitab paremini mõista, kas ja kuidas plokiahel on integreeritud Eesti digitaalsetesse teenustesse ja milline on selle kasutamise lisandväärtus süsteemidele.

Võtmesõnad:

Plokiahel, avalikud e-teenused, digitaalne infrastruktuur

CERCS: P175 Informaatika, süsteemiteooria

The Use of Blockchain in Public e-services on the Example of Estonia

Abstract

Today, Estonia is a country with a highly developed digital infrastructure, where most important public services are available online. It is often claimed that one of the keys to success in the development of Estonian public e-services is the use of blockchain. This master's thesis examines in more detail the actual scope of blockchain use in Estonian public e-services. The research methods used were a systematic literature analysis, which resulted in a literature review, and interviews, which resulted in an overview of the actual use of blockchain in three Estonian public e-services. This research helps to better understand whether and how the blockchain is integrated into Estonian digital services and what is the added value of its use to the systems.

Keywords:

Blockchain, public e-services, digital infrastructure

CERCS: P175 Informatics, systems theory

1. Sissejuhatus

Eesti on tuntud kui kõrgelt arenenud digiriik, mis pakub kodanikele laia valikut e-valitsemise lahendusi, mis võimaldavad kasutada erinevaid digitaalseid teenuseid. Tänu riigi digitaalsele infrastruktuurile ja e-teenuste platvormidele saab paljusid olulisi avalikke teenuseid kasutada veebis. Julgen väita, et tuntuse saavutamisel on oma roll olnud ka muljel, justkui põhineksid Eesti digilahendused suures ulatuses plokiahela tehnoloogial.

Plokiahel tõusis maailmas laiema tähelepanu alla aastal 2008, kui Satoshi Nakamoto avaldas *bitcoin*'i-teemalise *white paper'*i ehk dokumendi, kus kirjeldas plokiahela kontseptsiooni kui krüptovaluuta *bitcoin* tehnoloogilist alust. Plokiahela sõna hakati seoses *bitcoin*'i tulekuga laialdaselt kasutama, aga selle sisulise tähenduse üle arutleti tunduvalt vähem.

Kirjandusest võib leida viiteid, mille alusel Eesti on täna tuntud kui digiriik, mis kasutab plokiahela tehnoloogiat riiklikes avalikes teenustes. Selleteemalistes artiklites tuuakse küll välja, et kasutatakse plokiahela tehnoloogiat, aga mis teenustes täpsemalt või mis roll sel on, jääb tihti ebaselgeks. Samuti ei täpsustata sageli, mis tüüpi plokiahelaga on tegemist ning milline on väärtus, mida plokiahela tehnoloogia teenusele täpsemalt annab.

Magistritöö on jagatud kaheks peatükiks. Töö alguses tutvustatakse plokiahelaga seotud põhitermineid ja -mõisteid, et aidata paremini mõista töö sisu. Esimene peatükk annab ülevaate erinevatest plokiahela tüüpidest ning hõlmab süstemaatilise kirjanduse analüüsi tulemusena koostatud ülevaadet e-teenustest, mis väidetavalt põhinevad plokiahelal. Magistritöö teises osas analüüsib autor lähemalt kolme avalikku e-teenust ja nende tegelikku seost plokiahelaga. Analüüs on koostatud intervjuude ja läbi töötatud artiklite põhjal.

Magistritöö lisades on küsimustik, mida kasutati poolstruktureeritud intervjuude läbiviimisel.

1.2 Tänuavaldused

Tänan südamest oma juhendajat Jan Villemsoni sujuva koostöö, kannatlikkuse ja põhjaliku tagasiside andmise eest selle magistritöö kirjutamise protsessi vältel. Jani osalemine intervjuudel aitas intervjuude käigus juhtida tähelepanu detailidele, millele ise ilmselt ei oleks alati osanud viidata. Oli mitmeid väga põnevaid vestlusi, aitäh!
Samuti tänan kaasjuhendajat Kristjan Kripsi magistritöö vorminduse üle vaatamise ja põnevate infoturbe loengute eest õpingute ajal.

Minu suur tänu läheb ka kursusekaaslastele Laurile, Liinale, Pillele ja Lichetteyle kellega nii öösel kui päeval sai ühiselt õpitud ja grupitöid tehtud. Ilma teieta ei oleks see teekond olnud nii nauditav.

Viimaseks tänan ka oma perekonda toe ja mõistmise eest. Erilised tänud koerale Ellile, kellele olen lubanud kõik need arvutis veedetud tunnid korvata seiklustega metsas.

1.3 Uurimisküsimused

Selle magistritöö eesmärk on uurida, millistes avalikes e-teenustes Eestis plokiahela süsteeme kasutatakse, milline on plokiahela roll neis teenuses, millist tüüpi plokiahelat on kasutatud ning missugune on lisandväärtus, mida sellise lahenduse kasutamine teenusele annab. Magistritöö raames analüüsiti süstemaatiliselt olemasolevat kirjandust, et välja selgitada algallikad, mis viitavad laialdasele plokiahela kasutamisele Eesti avalikes teenustes.

Käesoleva magistritöö peamisteks uurimisküsimusteks on:

1. Kuidas on sündinud väited, et Eesti avalikud teenused jooksevad plokiahelal?
2. Milline on tegelik olukord plokiahela kasutamisega Eesti avalikes teenustes?

1.4 Metoodika

Uurimisküsimustele leiti vastused olemasoleva kirjanduse analüüsi ja intervjuude teel. Magistritöö raames viidi läbi poolstruktureeritud intervjuud spetsialistidega, kes on kokku puutunud Eesti avalike e-teenuste projektidega. Valimi moodustamise kriteeriumiks oli intervjueeritavate kokkupuude projektidega, kus väidetavalt kasutatakse plokiahela lahendusi. Isikud, kellega intervjuud läbi viia, leiti kirjandust analüüsides ning kasutati ka intervjueeritavate endi soovitusi. Intervjuud viidi läbi videokõne vahendusel. Intervjueeritavatega võeti ühendust sotsiaalmeedia platvormi LinkedIn ja e-maili teel. Intervjuud leidsid aset veebruaris ja märtsis aastal 2024.

2. Mõisted ja terminid

- **Andmevahetuskiht X-tee** – tehniline ja organisatsiooniline keskkond, mis võimaldab turvalist ja tõestusväärtust tagavat internetipõhist andmevahetust riigiasutuste vahel ja erasektoriga [24].
- **ECC** (inglise keeles *elliptical curve cryptography*) – elliptkrüptograafia ehk avaliku võtmega krüptograafia, mis rakendab elliptkõverate algebralist struktuuri [25].
- **E-ITS** – Eesti infoturbestandard, mis kehtib alates 1. jaanuarist 2023.
- **Etalonturve** – turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks [26].
- **Infosüsteem** – andmeid töötlev, salvestav või edastav tehniline süsteem koos selle normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega.
- **ISKE** – infosüsteemide kolmeastmelise etalonturbe süsteem oli Eesti avaliku sektori andmeturbe standard aastatel 2003–2022.
- **Krüptograafiline räsifunktsioon** [27] – funktsioon, mis peab olema:
    - ühesuunaline (inglise keeles *one-way*), st argumendi väärtus ei ole funktsiooni väärtuse järgi leitav (nõuetest ja keskkonnast sõltuva) mõistliku ajaga;
    - kollisioonivaba (inglise keeles *collision-resistant*), st mõistliku ajaga ei saa leida kaht argumendi väärtust, mis vastaksid ühele funktsiooni väärtusele.
    - Lisaargumendiks võib olla salajane võti.
    - Peamine rakendusala on digitaalsignatuuri moodustamine.
- **KSI** (inglise keeles *keyless signature infrastructure*) – räsifunktsiooni krüptograafial toimiv lahendus, kus verifitseerimisel tuginetakse räsifunktsioonide turvalisusele ja avaliku pearaamatu kättesaadavusele, mida tavaliselt nimetatakse plokiahelaks [28].
- **Loaline hajusraamat** (inglise keeles *permissioned ledger*) – teenuse osutamine on jagatud mitme kindla osapoole vahel, kes tegutsevad vastavalt lepingule või muule õigusaktile [20].
- **Loatu hajusraamat** (inglise keeles *permissionless ledger*) – teenuse osutajad ei ole määratud, sisuliselt võib igaüks hakata teenuse halduriks [20].
- **PKI** (inglise keeles *public key infrastructure*) – avaliku võtme taristu, millesse kuuluvad IT-vahendid, inimesed, poliitikad ja protseduurid avalike võtmete sidumiseks kasutajate identiteetidega, tavaliselt digitaalsertifikaatide abil [29].

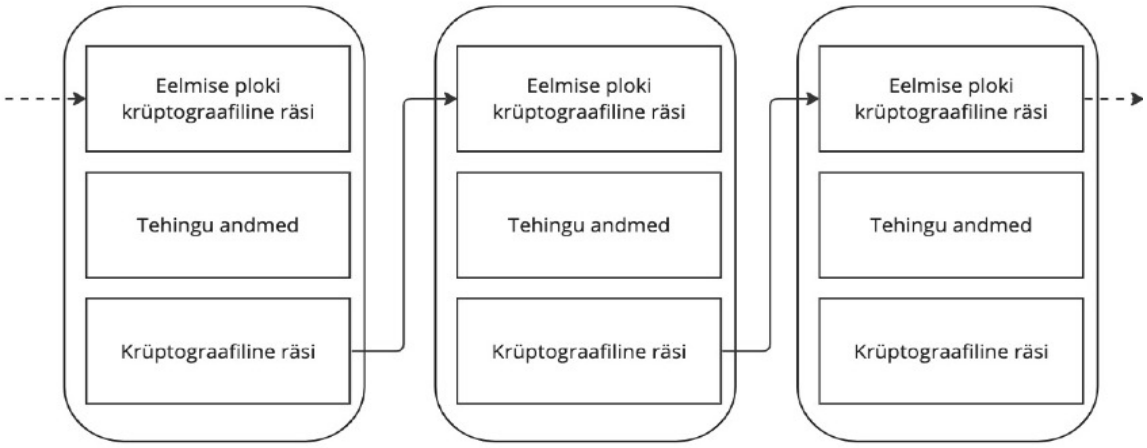
- **Plokiahel** (inglise keeles *block-chain*) – järjestikustest andmeplokkidest koosnev andmestruktuur [20].
- **Rsyslog** – avatud lähtekoodiga sündmuste logimise protokoll [4].
- **Räsifunktsioon** (inglise keeles *hash function*) – deterministlik algoritm, mis saab sisendiks suvalise hulga andmeid ning mille väljund on alati ühepikkune (teatud arv bitte) [30].
- **Räsipuu** – räsidest koosnev puu, nimetatakse ka Merkle'i puuks; räsipuu lehed on kontrollitavate andmeüksuste (näiteks failiplokkide) räsid ja sisetipud on eelmise taseme sidurdatud (inglise keeles *concatenation*) tipupaaride räsid [31].
- **SHA** – räsifunktsioonide sari [32].
- **T3** – ISKE turvamudeli tervikluse kolmas tase; info allikal ning selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas [33].

3. Kirjanduse ülevaade

Esimene peatükk annab ülevaate erinevatest plokiahela tüüpidest ning analüüsib nende eeliseid ja puudusi. Lisaks käsitletakse kirjanduse ülevaates Eestiga seonduvaid plokiahela kasutamise lahendusi ja vaadeldakse avalikke e-teenuseid, mis väidetavalt põhinevad plokiahelal.

3.1 Plokiahel

Plokiahelat defineeritakse kui hajusandmebaasi, mille andmeid uuendatakse läbi matemaatilise konsensuse saavutamise algoritmi. Plokiahel on sisuliselt hulk kirjeid, mis on plokkidena reastatud ning mis seotakse omavahel, kasutades krüptograafilisi räsifunktsioone. Iga ahela plokk sisaldab eelmise ploki krüptograafilist räsi ja tehingu andmeid. Plokiahela räsifunktsiooni tervikluse kaitseks lisatakse plokile kas digitaalsignatuur, räsitud ajatempel koos publitseerimismehhanismiga või interaktsioonita ajatempel [20]. Joonisel 1 on lihtsustatult kujutatud plokke, millest moodustub plokiahel koos nendes sisalduvate andmetega.



Joonis 1. Plokiahel

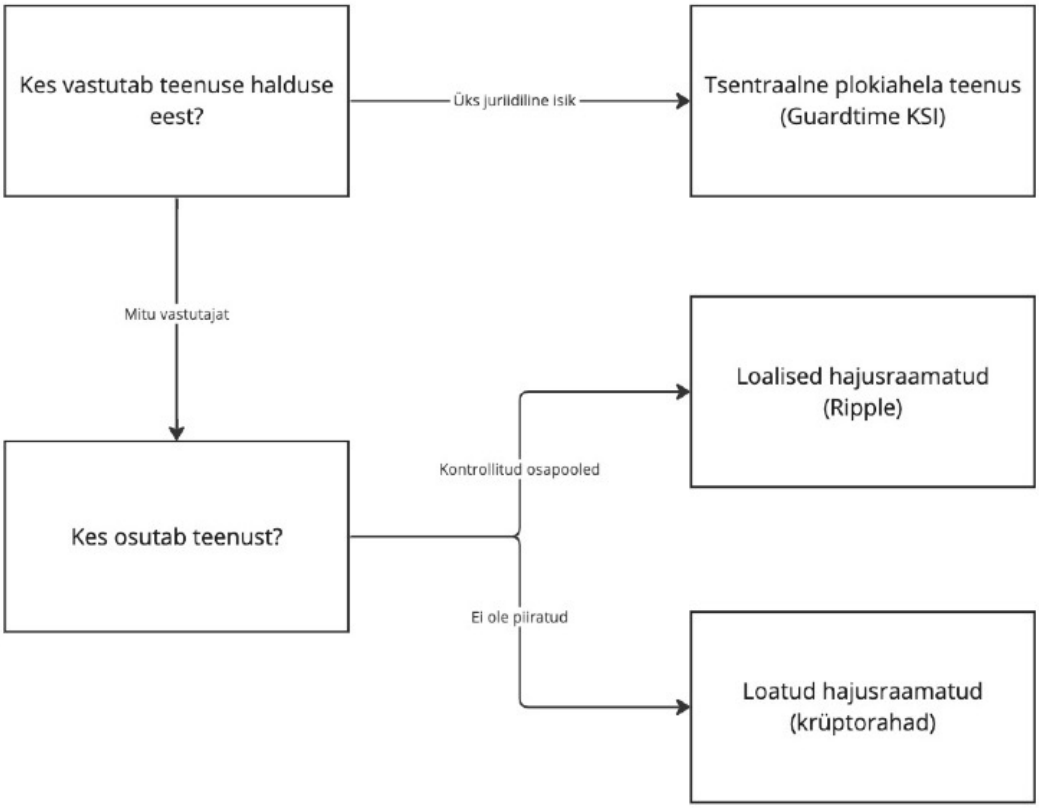
Plokiahela sisuline idee seisneb selles, et selle abil oleks võimalik tõestada andmete õigsust. Selle kasutamise eesmärk on anda kinnitus, et originaalandmeid ei ole mingil ajahetkel tagasiulatuvalt muudetud. Selleks, et teha muudatust mõnes plokis, tuleks muuta ka kõiki järgnevaid plokke.

Traditsioonilise andmebaasi puhul on serverid koondatud ühte kohta ning neid omaval organisatsioonil on kontroll nendes sisalduva info üle. Detsentraliseeritud plokiahela puhul on aga andmebaas hajutatud, mis elimineerib näiteks elektrikatkestuste, internetiühenduse puudumise või erinevate katastroofidega kaasnevad riskid. Plokiahela võtmeteguriks peetakse nõrga lüli, üksiku rikkepunkti puudumist (inglise keeles *single point of failure*), mille tõrke korral lakkaks süsteem töötamast. Risk, et andmebaasi haldajad võiksid manipuleerida andmebaasis sisalduvate andmetega, neid kustutada, muuta või üldse ligipääsu piirata, on maandatud hajusandmebaaside tehnoloogia abil.

Plokiahela süsteemid jagunevad järgnevalt [20]:

1) **Tsentraalseks plokiahela teenuseks** nimetatakse süsteemi, kus üks juriidiline isik vastutab tsentraalse teenusena arvestusraamatute halduse eest. Näiteks Guardtime'i KSI-süsteem on tsentraliseeritud loaline süsteem.
2) **Loalisteks** (ehk privaatseteks) **hajusraamatuteks** nimetatakse süsteeme, kus teenuse osutamine on jaotatud kontrollitud osapoolte vahel vastava lepingu alusel. Sellise süsteemi näiteks võib tuua pankadevahelisi tehinguid pakkuva Ripple'i.
3) **Loatuteks** (ehk avalikeks) **hajusraamatuteks** nimetatakse süsteeme, kus teenuse halduriks hakkamine ei ole piiratud ega kontrollitud. Näiteks krüptorahad põhinevad üldjuhul loatul hajusraamatu süsteemil.

Joonis 2 illustreerib plokiahela süsteemide jaotust.



Joonis 2. Plokiahela süsteemid

Erinevatel plokiahela tüüpidel on omad plussid ja miinused. Esiteks erinevad need teineteisest ligipääsu poolest: loaliste hajusraamatute puhul on ligipääsuks vajalik autoriseerimine, mis

juba loob süsteemile märgatavaid riske. Ligi pääsevad ainult need, kellel on selleks vastav luba, st kontroll on koondunud kindla üksuse kätte, mis tekitab potentsiaalse ohu manipulatsiooni või tsensuuri näol. Teine märgatav erinevus on konsensus: loalistel hajusraamatutel on reguleeritud see, kes saab konsensusprotsessiga liituda ja kes mitte, seevastu loatu plokiahela puhul tagatakse andmete muutumatus sellega, et liitumine ei ole kuidagi piiratud ja kõik saavad vajadusel näha muutmisi või kustutamisi. Potentsiaalne võimalus siiski jääb ka 51% rünnaku jaoks, mis tähendab, et ühe organisatsiooni kontrolli all on enamus räsimäärast, ning see võimaldaks läbi viia andmete muudatusi ahela ajaloos, kuid sellise olukorra tekitamine on väga keeruline. Tsentraalse süsteemi puhul omab andmetele ligipääsu vaid konkreetne selleks määratud rühm inimesi. Sama kehtib andmete käitlemise kohta – tsentraliseeritud plokiahela teenuse puhul on andmete käitlemine lubatud vaid selleks määratud üksusele või inimeste rühmale.

Eesti avalikes teenustes kasutusel olev plokiahela süsteem Guardtime'i KSI on loaline tsentraalne süsteem. See tähendab, et teenuse haldamine on privaatne ning arvestusraamatute halduse vastutus on koondatud Guardtime'i kätte. Krüptoraha *bitcoin* seevastu on loatu ja detsentraliseeritud lahendus. See tähendab, et teenuse halduriks võiks hakata igaüks ning uute *bitcoin*'ide loomine ei sõltu ühestki reguleerivast asutusest.

Nii loatud kui ka loalised plokiahelad on oma olemuselt muutumatud. Mis tähendab, et plokiahelasse salvestatud andmeid tagantjärele muuta ei saa. Küll aga on nende erinevuseks see, et avalikes ehk loatutes plokiahelates on kõigil võimalik plokiahela ketis osaleda. Kui avalikku ketti on plokk lisatud, siis seda tagantjärele muuta oleks väga ressursimahukas, et mitte öelda peaaegu võimatu. Loalise ahela puhul aga jääb alati mingi võimalus, et tehinguid ja isegi terveid plokke on võimalik pearaamatust eemaldada. Ligipääs andmetele võib loaliste plokiahelate kasutamisel samuti olla kompromiteeritud. Kontrolli omav üksus saab väljastada lubasid, kes pääseb andmetele ligi ning kas ainult lugemisõiguse või ka muutmise ja kirjutamise õigusega. Avaliku lahenduse puhul seevastu on kõigil võrdne ligipääs nii lugemiseks kui ka kirjutamiseks, kuid juba salvestatud ahela lülisid muuta on väga keeruline.

Guardtime'i KSI ajatemplite räside valideerimiseks on mõeldud välja neist endist sõltumatu lahendus: selleks kasutavad nad avalikus meedias postitamist. Seega, muudatuste tegemiseks tagasiulatuvalt peaks teoreetiliselt hävitama kõik ilmunud ajalehed, kus ajatemplite räsid on avaldatud, ning asendama need uute väljaannetega.

Avalike ehk loatute plokiahelate miinuseks on see, et need on aeglasemad. See on tingitud suurest kasutajate hulgast detsentraliseeritud võrgu süsteemis, kus tehingud kinnitatakse mitmes sõlmes üle maailma. Plussiks on aga see, et oma läbipaistvuse tõttu on need usaldusväärsemad kui loalised plokiahelad. Loaliste ahelate kasutamise kasuks räägib stabiilsus nii kulude kui ka kasutamise kiiruse mõttes. Kuna avalikes plokiahelates võivad osaleda ja tehingutele ligi pääseda kõik, siis tulenevalt kasvavast nõudlusest võib see protsesse aeglustada. Samuti on avalike ehk loatute plokiahelate kulud sageli kõrgemad kui loalistel. Seega võivad loalised mudelid olla küll tõhusamad, kuid tegelikkuses ei erine need väga tsentraliseeritud andmebaaside lahendusest ning seetõttu tõstatub küsimus: mis on see lisandväärtus, mida annab loalise plokiahela kasutamine?

3.2 Kirjanduse ülevaade plokiahelale rajatud e-teenustest

„See väike Balti rahvas on demonstreerinud uskumatut algatusvõimet plokiahela ümberkujundamisel. Peaaegu kõik Eesti avalikud teenused on digitaliseeritud, sealhulgas identiteet [14:70].“ Väidetavalt on kõige selle aluseks plokiahel, mis muudab andmelekked vähetõenäoliseks ning tervise-, kooli-, finants- ja valitsuse info erinevate keskkondade üleselt kasutatavaks [14].

A. Tapscott ja D. Tapscott on oma raamatus „Blockchain Revolution“ [14] rõhutanud küberturvalisuse olulisust eespool mainitud teenuste juures ning sealhulgas eraldi toonitanud, et Eesti küberturvalisus tuleneb KSI (inglise keeles *keyless signature infrastructure*) plokiahela tehnoloogiast. Veel on nad välja toonud, et tänu elektroonilise ID-kaardi kasutamisele on Eesti vähendanud residentide ja äride administratiivkulusid ning ühtlasi kasutab Eesti nii era- kui ka avalikus sektoris mitme programmi ja andmebaasi ühendamiseks X-tee lahendust, mille toeks on väidetavalt plokiahel. Samas on e-Estonia kodulehel avaldatud plokiahela ja X-tee teemaline postitus, kus on rõhutatud, et X-teed ei tohiks segamini ajada plokiahelaga ning et see kindlasti ei põhine plokiahelal, nagu kirjanduses ekslikult kajastatakse [19]. Nii X-tee kui ka plokiahel kasutavad andmete ühendamiseks krüptograafilisi räsifunktsioone, mis eksisteerisid juba enne mõlema süsteemi leiutamist, kuid see kindlasti ei tähenda, et plokiahel oleks X-tee aluseks.

M. Jun loetles aastal 2018 ilmunud artiklis [6] valitsuse juhitud plokiahela projekte. Väidetavalt juurutas Eesti valitsus artikli [6] kirjutamise ajal plokiahela tehnoloogiat eID ja e-Tervise süsteemidesse. Samas tabelis [Tabel 1] toodi välja e-residentsus kui esimene omataoline riikidevaheline digitaalse identiteedi lahendus, mida alates 2015. aastast on taotlenud üle 27 000 inimese. Kümme aastat hiljem, aastaks 2024 on statistikaameti kodulehe andmetel Eesti e-residendiks saanud 113 341 inimest [34].

Tabel 1. Näited valitsuse poolt juhitud plokiahela projektidest [6]

Nation	Project	Status
Australia	Australian senators launch parliamentary friends of blockchain group.	Announced in August 9, 2017
	The Australian Securities Exchange (ASX) announced that they will use blockchain technology to clear and settle trades by replacing the outdated Clearing House Electronic Subregister System, also known as CHESS.	Announced in December, 2017. The proposed transition is expected to take place in March 2018.
China	Social security funds management system	Announced in 2016
	Mortgage valuations on blockchain	Announced in 2016
	Blockchain-based asset custody system (PSBC)	Successfully executed more than 100 real business transactions on the blockchain since the system went live in October 2016
	Blockchain city project (By Wanxiang Group)	The project was announced by Wanxiang Group in 2016 and backed by Chinese government
Dubai	Government documents management system to be enacted by 2020	Ongoing
	Global blockchain council (GBC) was established in 2016 with 32 members, including government entities, international companies, leading UAE banks, free zones, and international blockchain technology firms	Ongoing
	Digital passport based on blockchain	Announced in June 2017
	Real-time information system about shipments to Dubai	Announced in 2017
Estonia	eID (electronic ID management system)	The government is currently upgrading the existing system with blockchain technology.
	E-health (medical information management system)	The government is currently upgrading the existing system with blockchain technology.
	e-Residency (a first-of-a-kind a transnational digital identity)	Since 2015, more than 27,000 people from 143 countries have applied and 4272 companies have been established as of December 2017

2016. aastal jõudis Eesti e-valitsemise indeksi alusel maailmas 13. kohale. 128 innovatiivsema riigi hulgas sai Eesti 24. positsiooni [10]. Nii väikese riigi kohta on see selgelt silmapaistev tulemus. Ühena põhjustest, mis Eestile sellise tuntuse on toonud, tuuakse artiklis [10] esile väidetav plokiahela tehnoloogia kasutamine riiklikes teenustes. Üks tuntumaid selliste teenuste seas on kindlasti e-tervise infosüsteem, mis töötab allika sõnul plokiahela tehnoloogial [10]. Artiklis on info allikana viidatud Business Insideri artiklile [35], kus tuuakse esile koostöö

tehnoloogiaettevõttega Guardtime ja väidetakse, et Guardtime kasutab juba *bitcoin*'iga seoses tuntuks saanud plokiahela tehnoloogiat. Lühidalt on artiklis esitatud ka plokiahela üldine definitsioon kui hajusandmebaasi tehnoloogia ehk keskse kontrollita andmebaas, mis lubab kasutajate võrgustikul sinna lisatud infot allkirjastada ja inspekteerida [35]. Artikli sõnul annab Guardtime'i tehnoloogia kasutamine Eesti tervisesüsteemile ülevaate kõigist uuendustest terviseandmetes. Plokiahela süsteemi kasutamine tagab selle, et terviseandmeid ei ole võimalik muuta ilma, et sellest märki maha jääks.

Tervishoiusüsteemi plokiahela revolutsiooni kirjeldavas artiklis [36] on järjekordne näide Eestist kui eesrindlikust riigist, kes koostöös Guardtime'iga on loonud digitaalse tervise infrastruktuuri, tänu millele on erinevatel osapooltel võimalik pääseda ligi neile vajalikule infole. Ühtlasi on sellega laiemale avalikkusele tõestatud nii suure ja elutähtsa teenuse plokiahelale rajamise võimalikkus [36]. Lähemal uurimisel selgub, et artiklis kajastatud väited tuginevad ka siin juba varem viidatud Business Insideri artiklile Guardtime'ist [35].

Plokiahela kasutamist e-teenustes on kajastatud artiklis [12] kui väga turvalist ja murrangulist meedet, millel tänu oma detsentraliseeritud süsteemidele on ühtlasi potentsiaal mõjutada nii poliitilisi, majanduslikke kui ka sotsiaalseid suhteid. Tuuakse välja plokiahela potentsiaal lahendada probleemid võimu koondumisega, korruptsiooniga ning usaldamatusega poliitiliste institutsioonide vastu [12]. KSI plokiahela kasutamise väärtusena nähakse märgatavat tõhususe ja produktiivsuse kasvu [10].

Samas on plokiahela kasutamisel nii valjuhäälseid pooldajaid kui ka kriitikuid, kuna tegelikult puudub üldine arusaam ja kokkulepe plokiahelaid ümbritsevate oluliste kontseptsioonide kohta ning selle mõju kohta institutsionaalsele kontekstile, kui räägime plokiahelal põhinevatest valitsemisvormidest. Plokiahela massiline kasutuselevõtt ilma riikliku koordineerimiseta võib viia ühiskonna polariseerumise ning uute oligarhide tekkeni [2, 12]. Lahendusena nähakse sellise plokiahela lahenduse kasutamist, mis toetab institutsionaalsete valitsemisvormide nõutavat kontrolli, kuid pakub samas läbipaistvust andmete omandiõiguse, privaatsuse ja platvormi vastutusega seoses, säilitades sealjuures vajalikud juhtimisstruktuurid [12]. Näiteks on vastakaid arvamusi, kas piiratud ligipääsuga plokiahela kasutamist on korrektne nimetada plokiahela kasutamiseks [12]. Diskussioon plokiahela olemuse kohta on jätkuvalt aktuaalne. Plokiahelat kirjeldati algselt läbi detsentraliseeritud pearaamatu tehnoloogia, mille tõttu

seostatakse seda peamiselt avatud digitaalse arhitektuuriga. Avatust peetakse hajutatud süsteemide tervikluse tagamise põhiomaduseks [12].

Eesti puhul vihjatakse veel plokiahela kasutamisele e-hääletamise turvalisuse tagamisel: oleme pälvinud tähelepanu kui riik, kes suudab valitsuse andmete turvalisuse tagada igas olukorras [7]. Semenzin, Rozas ja Hassan [12] väidavad, et Eesti valitsuse sõnul on plokiahela tehnoloogiate kaasamine digitaalarhitektuuri aidanud kaasa rahva usalduse tõstmisele valitsuse suhtes. „Usaldades plokiahela muutumatust ja detsentraliseeritud olemust, võivad kodanikud olla kindlad, et nende teave on turvatud, ja usaldavad seetõttu valitsust“ [12:390].

Väide usalduse tagamise kohta aga tekitab jätkuküsimusi: kuidas on selline turvalisuse tase saavutatud? Kas ja millised meetmed on selleks rakendatud?

Artiklis „Blockchain-based application at a governmental level: disruption or illusioon? The case of Estonia“ [12] esitatakse küsimus plokiahela tehnoloogia kasutamise tegeliku ulatuse kohta Eestis. Plokiahela kasutamisest Eesti e-teenustes räägitakse enamasti üldiselt, täpsustamata tegelikult, millist tüüpi plokiahela tehnoloogiat on kasutatud, millises ulatuses seda on tehtud ning missugune on tegelik lisandväärtus, miks seda kasutatakse. Artiklist [12] selgub, et piiratud ligipääsuga plokiahela mudeli kasutamise ajendiks on turvalisus, andmete liikumise jälgitavus, kiirus ning väidetav efektiivsus. Kuna teenuseomanikel peab olema tagatud kindlus ja teadmine, kus nende andmed paiknevad, siis leitigi, et parim lahendus selleks on kontrollitud süsteem, kus infoplokid on hajutatud, kuid nende hoidjad on teenuseomanikele teada [12].

Viimati mainitud artiklis kajastatakse erinevate sidusrühmade ja tehniliste ekspertide seisukohti. Anarhokapitalistide seisukoht on, et Eesti riigi teenustes ei ole kasutatud plokiahelat. Artiklis [12] on viidatud sarnasele seisukohale, toetudes Kivimäki blogipostitusele [18], mis väidab, et Eesti X-tee teenusel ja plokiahelal on ühiseks osaks vaid see, et mõlemas kasutatakse krüptograafilist räsi andmete ühendamiseks. Sarnase alatooniga on artiklis [12] välja toodud ühe e-tervise teenuse projektijuhi arvamus plokiahela teenuse kohta. Tema sõnul nimetatakse teenust räsiahelaks, mitte plokiahelaks, kuna plokiahela puhul on keskseks tunnuseks tsentraalselt juhitava keskkonna puudumine, Eesti näitel on aga alati olemas vastutav üksus, kes räsid ja ajatemplid talletab [12].

Eestist räägitakse sageli kui väga kõrge e-valitsuse arengu indeksiga riigist [10]. 2014. aastal sai plokiahela innovatsioon suurt tähelepanu nii era- kui ka avalike institutsioonide seas. Kolm tähelepanuväärset uuendust seoses plokiahela tehnoloogia kasutamisega on terviseandmete juurdepääsu haldamine, e-residentidele notariteenuste pakkumine ja aktsionäride autentimine koosolekutel e-hääletamiseks [10].

2014. aastal hakati e-residentidele väljastama ka e-ID-kaarte. Seda innovaatilist projekti kirjeldati kui *startup'*ilikku ettevõtmist, mille ulatust ja mõju tol hetkel päris täpselt ei osatud hinnata, kuid loodeti, et seda võiks saata murranguline edu [13]. Projekti ühe eesmärgina toodi välja 10 miljonit e-residenti aastaks 2025.

Startup-ettevõte nimega Guardtime kasutab plokiahela tehnoloogiat andmete verifitseerimiseks ning nende usaldusväärsuse tagamiseks [37]. Oscar Williams-Grut täpsustab Business Insideris avaldatud artiklis [37], et Eesti alustas koostööd Guardtime'iga terviseandmete turvalisuse tagamiseks. Guardtime'i tehnoloogia juurutamine pidi andma kindluse, et iga muudatus ja uuendus terviseandmetes saab plokiahelas registreeritud, seega ei oleks võimalik andmetega salaja manipuleerida.

Michael Kuperbergi artiklis [9] on viidatud e-Estonia kodulehe infole [11], mille kohaselt peaks kõigi allpool kirjeldatud eID teenuste infrastruktuur turvalisuse eesmärgil sisaldama Guardtime'i KSI plokiahela tehnoloogiat. Ühena neist teenustest, mis väidetavalt Guardtime'i KSI lahendust kasutab, on artiklis kirjeldatud residendist eID omaniku võimalust ID-kaardiga dokumente allkirjastada ja krüpteerida. Teise näitena on kirjeldatud väidetavalt plokiahelal toimiva lahendusena võimalust logida sisse erinevatesse veebikeskkondadesse ja kasutada tervishoiuteenuseid veebi vahendusel.

Lisaks tavalisele ID-kaardile on nendel kodanikel, kellel juba on ID-kaart olemas, võimalik saada digi-ID. Erinevus tavalise ID-kaardiga seisneb selles, et digi-ID-kaarti saab kasutada ainult elektroonilistes keskkondades. Kolmas eID lahendus on mobiil-ID, mis on mobiiltelefonidele mõeldud teenus, kus telefonis kasutatakse spetsiaalset SIM-kaarti salajase võtme operatsioonideks. Sarnaselt eelmainitud ID-lahendustega saab mobiil-ID-d kasutada isiku tuvastamiseks ja allkirjastamiseks. Nagu ID-kaardil nii on ka mobiil-ID-l kaks PIN-koodi: üks identifitseerimiseks ning teine allkirjafunktsionaalsuse avamiseks. Mobiil-ID eelis ID-kaardi ees seisneb selles, et puudub vajadus eraldi kaardilugeja järele. Kõikide mainitud e-

teenuste taga seisab artikli [9] väitel Guardtime'i KSI plokiahela tehnoloogia, mis tagab vajaliku turvalisuse, küll aga tuuakse siingi esile, et jääb ebaselgeks, millises ulatuses on plokiahela tehnoloogiat kasutatud.

Kuperbergi artiklis [9] uuritakse ja analüüsitakse plokiahelal põhinevaid riiklikke elektroonilisi ID-teenuseid. Eesti on seal ära mainitud nii oma residentidele kui ka mitteresidentidele mõeldud ID-kaardiga, toetudes allikale [38], kus omakorda viidatakse Forbesis avaldatud P. High artiklile [5]. Üks High artikli jaoks intervjueeritavatest oli Taavi Kotka, kes muu hulgas on tuntud ka kui endine e-residentsuse programmi juht. Intervjuus kirjeldab Kotka, et selleks, et arstidele võimaldada ligipääs patsiendi ravikaardile mitte ainult ühes konkreetses haiglas, vaid kõigis haiglates, on vaja patsiendi infole tagada kõrgendatud turvatase. Vajalik turvatase saavutatakse Eesti tervisesüsteemis plokiahela tüüpi tehnoloogia abiga [5]. Kuperbergi artiklis [9] on välja toodud ka mobiil-ID teenus. Kuperbergi info, et kõik eelmainitud teenused tuginevad Guardtime'i KSI plokiahela tehnoloogiale, pärineb e-Estonia kodulehelt [11]. Virtuaalset riiklikku ID-kaarti ja e-residentsust mainitakse artiklis uuenduslike lahendustena, mis just Eestis esmakordselt kasutusele võeti. Tabelis 2 võttis Kuperberg kokku artikli [9] tulemused.

Tabel 2. Plokiahelal toimivate eID lahenduste võrdlus [9]

Authority that issues eID	United Arab Emirates Governm.	Estonian Governm.	Finnish Immigration Services	Governm. of Luxembourg via LuxTrust	Switzerland City of Zug	Switzerland Canton of Schaffhausen
Rollout status	Pilot starting 2020	In use	In use till 30.04.2019	Pilot phase	Pilot phase	In use
Level	National	National	National	National	Municipal	Canton
Solution used for	Digital passport; "ID locker"	Data integrity, timestamp	Unique Digital Identities	Trusted blockchain identities	Self-sovereign identities	Self-sovereign identities
DLT stores identity data	No	No	No	No	No	No
DLT stores authorizations for eID	Planned	No (but the DLT acts as an access log)	No (but the DLT stores payment transaction history)	No	No	Yes
eID capabilities for DLT cryptogr.	No	No	No	Yes	Yes	Unspecified
GDPR	Compliant	Compliant	Unspecified	Unspecified	Compliant	Unspecified
eID Type	Mobile app	Multiple	Multiple	X.509 cert.	Mobile app	Mobile app
Implem. Partner	ObjectTech	Guardtime	MONI	Intech	uPort and ti&m	Procivis
Blockch. Type	Unspecified (Q1/19)	Private	Unspecified	Public testnet: Kovan	Public	Unspecified
Blockch. Technol.	Unspecified	KSI Blockchain	Ethereum Blockchain	Ethereum; ERC-725 ERC-735	Ethereum + uPort	Unspecified

PWC aruande kohaselt on Eesti kodanikele 99% avalikke teenuseid kättesaadavad e-teenustena, mis kõik justkui toetuvad plokiahela tehnoloogiale [7]. Plokiahelal toimivate teenustena on aruandes välja toodud Eesti riigi kodanike ID-kaart, mille abil saab reisida Euroopa Liidus, Euroopa ravikindlustuskaardi tellimine, digiallkirjastamise teenus, ligipääs terviseandmetele ning digiretseptide tellimise ja haldamise teenus. Nimekiri on muljetavaldav ja tähelepanu tõmbav, kuna see kõik toimib aruande kohaselt plokiahelal põhineva tehnoloogia abil ning on sealjuures saavutanud märkimisväärse tunnustuse just tänu sellele.

Eesti on saanud rohkelt meediakajastust kui esimene riik, mis võttis reaalajasüsteemides kasutusele plokiahela tehnoloogia, et tagada dokumentide, logide ja süsteemide terviklikkus [17]. Artiklis Eesti valitsuse ja Guardtime'i koostöö kohta [17] tuuakse välja, et Eesti on olnud digiühiskonna innovatsiooni esirinnas viimased 20 aastat ja on ühtlasi ainus riik maailmas,

mille rahvastikust enamik kannab kaasas kiipkaarti, pääsemaks ligi rohkem kui tuhandele riigiteenusele.

PWC aruande [7] alguses tuuakse välja järgmised väited Eesti kohta:

- „Enim digiarenenud ühiskond maailmas.“
- „Maailma digitaalseim riik.“
- „Oleksime pidanud eestlastele helistama, kui oma tervishoiu veebikeskkonda üles seadsime.“

Aruandes tuuakse välja nii Eesti digitaalse ID-kaardi olemasolu kui ka selle unikaalsus maailmas, kuna see võimaldab ligipääsu kõigile riigi digiteenustele. Mainitakse ka e-residentsust, mis annab isegi mittekodanikele võimaluse osa saada Eesti e-riigi teenustest. Dokumendis esitatud andmete kohaselt oli Eestis aruande avaldamise hetkel 50 000 e-residenti rohkem kui 165 riigist. Aruande kohaselt on need residendid alustanud üle 5000 ettevõtte. E-residentsus ei anna välisriigi kodanikule reisimise õigust ega päris kodakondsust, kuid võimaldab muu hulgas asutada veebikeskkonnas ettevõtte, digiallkirjastada dokumente, koostada ja esitada maksudeklaratsioone ning viia läbi pangatoiminguid [7].

Väidetavalt plokiahelale rajatud teenuste seas on märkimisväärne ka e-hääletamise lahendus, mis tugineb ID-kaardiga autentimisele. Artiklis „Blockchain Enabled e-voting“ [8] kirjeldatakse lähemalt plokiahela rolli e-valimistes ning mainitakse, et just plokiahela kasutamine tagab krüptograafiliselt turvalised hääletusandmed ja kogu protsessi läbipaistvuse. Eesti on esile toodud oma kodanikele mõeldud ID-kaardi kasutusvõimaluste poolest, samuti on mainitud plaani laiendada ID-kaardi kasutamise võimalust ka e-residentidest mittekodanikele. Nir Kshetri ja Jeffrey Voas kirjeldavad plokiahelal baseeruva e-hääletamise kasutamist [8] LHV panga näitel, kus lahendust kasutatakse näiteks üldkoosolekutel hääletamiseks. Artikli info pärineb Cyberscoopis avaldatud S. Watermani artiklist [15], kus kirjeldatakse e-hääletamise toimimist ning eduka katse tulemusi. Samuti tuuakse välja seos *bitcoin*'i ja plokiahela vahel [15] ning juhitakse tähelepanu sellele, et plokiahela lisamine protsessi ei lahenda kindlasti kõiki e-valimiste probleeme, pigem väga väikese osa nendest.

Kõigi nende edulugude ja vaimustuse kõrval esineb ka omajagu kriitikat. Artiklis „Blockchain in the Government Technology Fabric“ [1] arutletakse plokiahelal baseeruvate teenuste edulugude ning võimalike alternatiivide üle. Tuuakse välja plokiahela klassifitseerimise

küsimus, mida siiani mainitud artiklites väga rõhutatud ei ole: kas kasutatakse piiratud ligipääsuga või avalikku plokiahelat? Eestit on artiklis [1] mainitud kui pioneeri digitaalse identiteedi teemal oma KSI plokiahela lahendusega. Eesti väidetavalt plokiahelal toimiva eID lahenduse kõrval tuuakse alternatiivina välja mõned maailma suurimad digitaalse identifitseerimise süsteemid, mis ei põhine plokiahelal. Võrdluse eesmärk on näidata, et puhtalt projektide mastaapsus või rohkete sidusrühmade kaasatus ise ei nõua, et oleks vaja kasutada plokiahela tehnoloogiat. Samuti ei taga plokiahela kasutamine kõiki lubatud turvagarantiisid. Väite allikaks on e-Estonia enda koduleht, kus kirjeldatakse Eesti kui e-riigi arengut ajateljel, millel on esile toodud, et aastal 2008 töötasid Eesti krüptograafid välja innovaatilise KSI plokiahela lahenduse, millel nüüd jooksevad paljud riiklikud teenused [39].

4. Analüüs ja tulemused

Kirjanduses leiduvate väidete ülevaatamise järel uurime edasi, kuidas tegelikult kõigis neis teenustes plokiahelat kasutatakse. Peatükis „Analüüs ja tulemused“ on lähemalt analüüsitud kolme avalikku e-teenust ja nende tegelikku seost plokiahelaga. Analüüs põhineb intervjuudel ja läbi töötatud artiklitel.

4.1 Plokiahela kasutamine e-tervise infosüsteemis

Eesti e-tervise infosüsteemi plokiahela rakenduste analüüsimiseks ning reaalse ülevaate saamiseks selle kasutusest viidi läbi poolstruktureeritud intervjuud [Lisa 1] spetsialistidega, kes puutusid kokku kõnealuse infosüsteemiga selle loomise faasis.

Nagu eespool mainitud, on plokiahelast rääkimise juures oluline, kuidas plokiahelat defineerida. Esimene intervjueeritav, Eesti e-tervise infosüsteemi projekti arhitekt Artur Novek, alustas vestlust nii (intervjuu toimus 09.02.2024): „Esmalt tuleks kindlasti defineerida, mida me üldse mõtleme plokiahela all. Tihtipeale räägitakse ka jagatud andmetega süsteemidest, mis tegelikult on *distributed ledger*. Plokiahel on siiski natuke üldisem termin ja ma arvan, et Guardtime’i KSI, mille katsetusi meie tegime, võib rahumeeli lugeda plokiahela alla.“ Seega sai kohe vestluse alguses selgeks, et tegemist oli katsetustega.

Eesti e-tervise kontekstis saame rääkida plokiahelast kui ajatempli kinnituse funktsionaalsusest. Küsimusele, kuidas on plokiahel e-tervise projektis kasutusel, vastas teine intervjueeritav, TEHIK-u infoturbespetsialist Lauri Lunt (intervjuu toimus 19.02.2024): „Kui sa küsid, kuidas e-tervise valdkonnas täpsemalt plokiahelat kasutatakse, siis praegu sinna templeid ei lisata. Selle põhjuseks on see, et Guardtime teatas mingi hetk, et nad ei arenda seda edasi. Seega, e-tervise kontekstis ma konkreetselt ei saa rääkida.”

Üks intervjuu küsimus oli kirjeldada probleemi, mida prooviti e-tervise süsteemis lahendada plokiahela kasutamisega. Eesti tervise infosüsteemi endasse on tegelikult juba algselt sisse ehitatud ka räsiaheldamise süsteem. Paralleelselt andmete lisamise või muutmisega andmebaasis tehakse märge auditítabelisse, kus põhitabeli info kopeeritakse ümber ning lisatakse andmebaasi toimingu märge. Toimingu märge sisaldab infot, kas tehti lisamine,

muutmine või kustutamine, koos ajalise märkega, millal muudatus aset leidis. Lisatakse ka X-tee päringu ID, kuna andmevahetus käib üle X-tee. X-tee päringu ID alusel on võimalik tõendada ja tuvastada päringu toimumist. Andmevahetusel erinevate osapoolte vahel üle X-tee tagatakse andmete terviklus, käideldavus ja konfidentsiaalsus [24]. Nende audititabelite peale omakorda on ehitatud räsiahel, mida on teoreetiliselt võimalik tagasiulatuvalt muuta. Et seda ei juhtuks, võeti lisaks kasutusele Guardtime'i ajatemplikinnitus, mille usaldusväärsus tugineb räside perioodilisele avaldamisele trükimeedias.

Intervjuust selgus ka, et e-tervise infosüsteemi sisemise räsiahela terviklust perioodiliselt täna keegi ei kontrolli. Novek täpsustas: „Sinna on minu meelest praegu peale ehitatud käsitsi võimalused verifitseerimisfunktsioone käivitada, mida mitte kunagi minu teada tehtud ei ole." Kui autor küsis, et kas võib öelda, et täna on tegemist pigem heidutusfunktsiooniga, vastas Novek: „Jah, põhimõtteliselt on kogu see asi nagu heidutusfunktsioon, et ei tekiks ka mõtet ega tahtmist midagi tagantjärele ära muuta."

Kõnealune lahendus loodi kooskõlas ISKE rakendusjuhendiga, mis oli kehtiv standard infosüsteemi arendamise ajal. ISKE oli infosüsteemide kolmeastmelise etalonturbe süsteem ehk Eesti avaliku sektori andmeturbe standard, mis kindlustas vajaliku turvataseme infosüsteemides töödeldavatele andmetele [33].

ISKE-s on kirjeldatud kolme turbe taset: madal (L), keskmine (M) ja kõrge (H). Taseme määratlemine sõltub kolmest erinevast turvaosaklassist, mis on määratud töödeldavate andmete turvaklasside kaudu. Viimase määratlemisel omakorda lähtutakse andmete käideldavusest, terviklusest ja konfidentsiaalsusest. Tervise infosüsteem on liigitatud tervikluse turvaosa klassi kõrgeimale tasemele T3. Tervikluse kolmas tase nõuab, et info allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas [26].

ISKE meetmete T3 turvaklassis on kirjeldatud nõue HT.10 „Andmebaasi kannete krüptoaheldamine" [40], mille kohaselt peab andmed siduma kronoloogiliselt, kasutades räsiaheldamise pööramatuse omadust, mis omakorda peab tagama, et andmeid ei oleks võimalik tagantjärele märkamatult muuta. Nõutud on ka see, et spetsiaalselt määratud inimene kontrolliks perioodiliselt ahela terviklust.

Praeguseks on loodud uus standard E-ITS [41], Eesti avaliku sektori infoturbe korraldamise süsteem, mis sarnaselt oma eelkäija ISKE-ga samuti sisaldab räsiaheldamise meedet ME1 [42]. Intervjuudest selgus ka, et sisemise räsiahela tervikluse kontrollimiseks on ehitatud funktsionaalsus, mis käivitab verifitseerimise funktsioonid, kuid teadaolevalt seda praktikas regulaarselt ei rakendata.

Turvasüsteemides kolmanda osapoole lisakinnituse kasutamise lahendusele omaselt ei saa räsiahelas pärast Guardtime'i ajatemplikinnituse lisamist enam muudatusi teha, kuna see ei ole enam algse teenusepakkuja kontrolli all. Teoreetiliselt oleks kolmandal osapoolel (st Guardtime'il endal) võimalik ajatemplimuudatusi teha, kuid nende süsteemi turvalisus on tagatud perioodiliselt ajalehes Financial Times trükitud räsidega, mis tähendab, et tagasiulatuvalt räsisid muuta on sisuliselt võimatu.

Antud e-tervise infosüsteemi lahendus juurutati testkeskkonda, kus reaalse andmestikuga mängiti läbi räsi võtmine, aga Guardtime'i-poolse tervikluskontrolli testimise kohta Novekil vestluse ajal täpne ülevaade puudus. Arendus sellisel kujul kasutusse tegelikult ei jõudnudki. Ilmnes probleem, et Guardtime'i jaoks oli vaja SHA256 räsifunktsiooni, kuid Oracle'i andmebaas kasutas sel hetkel veel ainult SHA1. Vajalikud uuendused said teostatud, kuid kasutusele lahendust sellisel kujul ei võetud. „Me viisime läbi uuendused test- ja *prelive*-keskkondades, kus oli võimalik kõik juba tööle panna, ent *live*-keskkonna puhul tekkisid takistused. Administraatorid kas ei julgenud uuendust ette võtta või olid hõivatud muude prioriteetidega. Seega venis aeg edasi mitme aasta jooksul, kuni lõpuks tuli Oracle'i uuendus. Selleks ajaks aga Guardtime enam meie arendatud lahendust ei toetanud," ütles Novek.

Paralleelselt eespool kirjeldatud arendusega juurutati Guardtime'i templi võtmine ka andmebaasi teistele logidele, milleks olid peamiselt administraatorite tegevuste logid. Antud lahendust laiendati nii, et täna võetakse kõikide TEHIK-u (Tervise ja Heaolu Infosüsteemide Keskus) süsteemi logide peale Guardtime'i KSI ajatemplid. Ja see on ka lahendus, millest saab praegu rääkida kui Guardtime'i KSI plokiahelal toimivast lahendusest, mis on päriselt kasutuses.

Lunt kirjeldas plokiahela süsteemi kasutamist järgmiselt: „Mina kasutan Guardtime'i KSI lahendust logide juures ja rsyslogi juures, kus rsyslogi on mulle ära teinud selle osa, kuskohas ta võtab logid ja paneb nad ahelasse, kasutades Merkle'i *tree*'d. Seal kõrval on nii-öelda

Guardtime'i KSI välja arendatud *library*, mis siis käib ja võtab sult sinna sellele puu tipule peale templi." Logidesse, millele ajatempel peale võetakse, lähevad nii andmebaasi muudatuste kirjed kui ka rakenduse auditlogid kuni administraatori tegevuste logideni välja.

Küsimusele, mis on selle lahenduse lisandväärtus, vastas Lunt, et KSI templite kasutamine annab tõenduspõhise logi. See tähendab võimalust näidata ja tõestada, kus mingi logikirje täpselt asub. „Kui on vaja kuskile, kas kohtutele või kellelegi muule, tõestuseks anda, siis sa võtad selle logi osa sealt välja. Sealt arvutatakse sulle puu tipp. KSI ajatemplit saad sa laiendada kuni selleni, mida nad prindivad kas Twitteris või ajalehes."

KSI laiendamise all mõeldakse teabe lisamise võimalust ajatemplile, nagu näiteks meedias avaldatud räsid. Intervjuu toimumise hetkeni ei olnud logide tõestamist kellelgi otseselt vaja läinud, kuid KSI ajatempli lahendus annab vajaduse tekkimisel võimekuse tõestada, et logisid ei ole tagasiulatuvalt muudetud.

Vastates küsimusele Guardtime'i KSI lahendusega iga päev töötamise kohta, tõi Lunt veel esile, et tema hinnangul sellist lahendust, nagu täna TEHIK-us kasutatakse (rsyslog ja Guardtime koos), ilmselt maailmas väga ei leidu. Ta põhjendas oma seisukohta, viidates vigade ja probleemide hulgale, mis nende koos kasutamisel on ette tulnud. Kui see lahendus oleks maailmas laialt kasutuses, oleksid paljud elementaarsed vead oluliselt kiiremini ilmnenud ja parandatud. Näitena tõi Lunt puuduva asünkroonse infovahetuse võimekuse.

Projekt, mis tänaseks enam kasutuses ei ole, kuid mis oli näide edukast plokiahela KSI kasutusest, oli Eesti COVID-19 digitaalne vaktsineerimistõend QR-koodi kujul. Tõend sisaldas KSI plokiahela templiga sertifikaati, mis võimaldas tõendada sertifikaadi ehtsust ja ajatempli usaldusväärsust. Lahendus oli üles ehitatud nii, et kogu sertifikaadi info paiknes tervise infosüsteemi serveris, kust oli võimalik sertifikaati kontrollimas käia. Kontrolli käigus vaadati, kas juures olev tempel vastab KSI ahela templile. Sellise lahenduse eelduseks oli võimekus viia läbi päringuid sidusrežiimis. Lahendusele sai saatuslikuks Euroopa Liidu (EL) soov mitte kasutada Guardtime'i KSI-d ning süsteem tehti ümber PKI (*public key infrastructure*) ehk avaliku võtme infrastruktuuri peale, mida kasutati kogu EL-is. Üleeuroopaline vaktsineerimistõend hakkas kandma nimetust roheline digitõend ning see võimaldas pandeemia ajal kodanikel EL-i riikides liikuda [3]. EL-i digitaalse COVID-19-tõendi määrus oli kehtiv kuni 30. juunini 2023. Alates 1. juulist 2023 võttis WHO (World Health

Organisation) ehk Maailma Terviseorganisatsioon kasutusele EL-i digitaalse COVID-19 sertifitseerimise süsteemi eesmärgiga luua ülemaailmne süsteem, mida saab kasutada inimeste kaitseks erinevate pandeemiate ja terviseohtude korral [23].

4.2 Plokiahela kasutamine LHV pangas

Kirjanduse ülevaate peatükis esitatud väidete verifitseerimiseks plokiahela kasutamisest LHV pangas viisime läbi intervjuu Jüri Lauriga (intervjuu toimus 13.03.2024), kes oli aastatel 2015 ja 2016 LHV krüptovaluuta tootejuht. Tema vastutusalasse kuulusid hajutatud pearaamatu tehnoloogial (plokiahelal) toimivad teenused.

Eesti kodanikest või e-residentidest LHV grupi osanikud said Nasdaqi plokiahelal toimivat hääletuslahendust kasutada LHV üldkoosolekul hääletamiseks, autentides end riikliku ID-kaardiga [8]. Lahenduse väidetavalt edukas katsetamine on mainitud ka kirjanduse ülevaate peatükis.

LHV panga enda plokiahela katsetused algasid suhteliselt varakult krüptovaluutade ajastul, juba 2013. aastal. Esimest korda Eestis kasutasid nad plokiahelat makseteenuste valdkonnas. Algne plaan oli kasutada krüptovaluutat igapäevaste jaemaksete jaoks eesmärgiga pakkuda odavamat alternatiivi tavapärastele pangatehingutele. Idee seisnes *bitcoin*'i-laadse digiraha loomises plokiahela peale. Algne plaan oli kasutada *bitcoin*'i plokiahelat, kuid *colored coin*'i ehk nn värvitud münti. Põhimõtteliselt võib seda nimetada *bitcoin*'i-tolmuks: väga väikesed *bitcoin*'i osakesed, millel endal sel ajal suurt väärtust ei olnud, lisati tehingule metaandmetena kaasa ja need defineerisid tehingu väärtuse.

Projekti algfaasis oli *bitcoin*'i väärtus nii madal, et majanduslikus mõttes oli mõistlik liigutada väga väikesi *bitcoin*'i osakesi. Selleks hetkeks, kui projekt oli nii kaugel, et hakati reaalseid tehinguid läbi viima, oli *bitcoin*'i hind sedavõrd palju tõusnud, et osakeste saatmise ehk tolmu kontseptsioon ei olnud enam otstarbekas. Esialgsest plaanist pakkuda tavapärasest pangandusest odavamaid valuuta liigutamise võimalusi sai lahendus, mis oli tegelikkuses kümme korda kallim.

Projektiga edasiminekuks kaaluti alternatiivina *side chain*'i ehk enda plokiahelat, mis oleks perioodiliselt lingitud *bitcoin*'iga. Selline lahendus oleks olnud seotud plokiahelaga, kuid teisalt oleks olnud tegu lahendusega, mis on sarnane traditsioonilise pangandusega, kus tehingud toimuvad sisemises süsteemis ning neid kajastatakse perioodiliselt mingis universaalses süsteemis.

Küsimusele, mis on sellise lahenduse puhul lisandväärtus, mida sai saavutada plokiahelaga, aga mitte traditsiooniliste meetoditega, vastas Laur, et tegelikkuses seda lõpuni läbi ei mõeldudki. Liiguti samm korraga ja eesmärk oli suurem osa tehingutest süsteemist välja viia, mis aitaks *unit cost*'i ehk ühiku maksumust kontrolli alla saada. Plaan oli luua rahvusvaheline süsteem, kus väärtuse ülekanne toimuks kliendi jaoks reaalajas.

Täpsustavale küsimusele, miks mitte luua eraldiseisev plokiahel, mis ei oleks *bitcoin*'iga seotud, vastas Laur, et otsust mõjutas mitu aspekti. Esiteks oli eesmärgiks LHV panga infrastruktuuri kulud võimalikult madalal hoida, et nad ise ei peaks seda tsentraalselt juhtima, ning teine põhjus oli finantsinspektsiooni kehtestatud nõuded ja piirangud, mis oleksid kehtinud täiesti iseseisva krüptoraha väljaandmisele. „Üks põhjus oli katse enda infrastruktuuri kulud võimalikult madalal hoida, et me ise ei pea tsentraalselt seda kuskil püsti hoidma. Teine oli see tsentraliseeritud *versus* detsentraliseeritud lahenduse küsimus. Krüptotööstus vaatas meid nagu napakaid sellepärast, et tsentraliseeritud on halb, et see ei hakka teil kunagi tööle. Finantsmaailm – nemad ei vaadanud meid üldse, sest nad ei saanud aru, mis toimub. Ja pangasiseselt pärast suhtlemist finantsinspektsiooniga oli selge, et mingisugust krüptoraha me ise väljastama hakata ei saa, kuna see keelatakse ära. Sellepärast me otsisime sellist vaheteed," selgitas Laur. Alternatiivse *side chain*'i lahenduse teostamiseni ei jõutud.

Veel üks katsetamise käigus ilmnenud probleem seisnes kasutajakogemuses: tehingute protsess oli aeglane ja selle kiirendamiseks tuli maksta suuremaid teenustasusid, mis muutis kogu lahenduse kulukamaks. Lisaks oli kaupmeestele ebaselge, kas tehing oli edukas, kuna vastuse kajastamine võttis aega.

Kui kõik varem mainitud probleemid oleksid olnud tehniliselt lahendatavad, siis suuremaks takistuseks kujunesid katsetuste käigus ilmnenud kasutajate käitumisharjumused. Veel ei olnud kasutusel viipemaksed, keegi ei maksnud mobiiltelefoni ega Apple Pay või Google Payga. Harjumuspärased makseviisid olid pangakaart ja sularaha. Kuid siis hakkasid viipemaksekaardid järk-järgult levima ning krüptomakse kogemusega võrreldes oli viipemakse oluliselt kiirem ja mugavam.

„Kui sa võrdled viipemakse kogemust krüptomakse kogemusega, siis see krüptomakse eeldas, et sa võtsid telefoni lukust lahti, tegid äpi lahti. See äpp oli üsna robustne, laadis tükk aega, sest seal oli vaja oodata *blockchain*'i sünkroniseerimist. Ja siis sa skaneerisid mingit QR-koodi.

Eestis ei ole QR-koodiga maksmise kogemust mitte kellelgi," rääkis Laur. Lisaks ei olnud QR-koodiga maksed integreeritud müügipunktide süsteemidesse, mis tähendas kaupmeestele lisaseadme kasutamist. „Me andsime esimese hooga tasuta tahvli, et näete, ärge muretsege, saate kõik tehtud." Kogu protsess aga oli kõigi kasutajate jaoks ebamugav. „See oli ebamugavus teenindaja jaoks. Kõik sai alguse sellest, kui ohkav teenindaja võtab sahtlist kuskilt mingi tahvli, mille aku võib-olla on tühjaks saanud vahepeal, ja siis sina oled seal kliendina, seisad selle õnnetu äpiga… Sul tekib lihtsalt ebameeldiv emotsioon, et nüüd ma tekitan kellelegi pahameelt, et mina maksan sellega. See lihtsalt ei töötanud. Ja siis tulid viipekaardid peale," kirjeldas Laur.

Projekti käigus analüüsiti ka teiste krüptorahade kasutamist, mille puhul oleksid tehingutasud väiksemad või isegi olematud olnud, aga analüüsi tulemusena jaemaksete jaoks ideaalset lahendust ei leitud.

4.3 Plokiahela kasutamine Eesti eID süsteemis

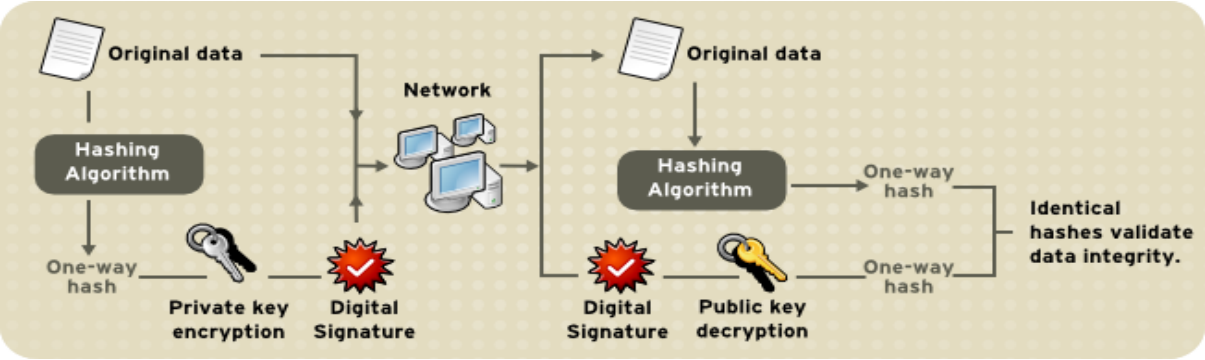
Väidetavalt plokiahelal toimivate teenuste peatükis on välja toodud Michael Kuperbergi artikkel [9], mis püüab vastata küsimusele, millised eID teenused (kui üldse) rajanevad plokiahela tehnoloogial või sisaldavad vähemalt osaliselt plokiahelal põhinevaid funktsionaalsusi. Artiklis tuuakse välja muu hulgas plokiahelal toimivad Eesti ID-lahendused ning artikli kokkuvõte algab lausega: „Enim arenenud ja toimiva eID ja plokiahela lahenduse võib leida Eestist, milleks on KSI plokiahelale juurutatud ja valitsuse eestvedamisel loodud e-ID-kaart“ [9:9].

Artikli väidete kontrollimiseks töötati läbi teemakohased publikatsioonid ning tehti päring ka RIA (Riigi Infosüsteemi Amet) turvaarhitektile Tõnis Reimole. Mõlemast lähemalt järgnevates lõikudes.

Eesti elektrooniline identiteet on kogum andmeid, mis seovad isiku identiteedi elektroonilises keskkonnas tema füüsilise isikuga [43]. eID kandjaks võib olla ID-kaart, elamisloakaart, diplomaatiline ID, mobiil-ID, digi-ID või e-residendi digi-ID ning RIA kodulehe andmetel [43] on kogu eID toimimise aluseks PKI (inglise keeles *public key infrastructure*) ehk avaliku võtme infrastruktuur.

Päringule, kus oli viidatud Kuperbergi artikli väitele [9] plokiahelal toimivast eID lahendusest, vastas Reimo üheselt, et Eesti eID süsteemides ei ole kasutusel KSI lahendust. M. Pisa ja M. Judeni artiklis [21], millele ka Kuperberg allikana on viidanud, on kirjeldatud Eesti ID-lahendust kui enim arenenud riiklikku ID-süsteemi, mis kasutab avaliku võtme krüptograafiat. ID-kaart, mis on üks eID kandja tüüp, sisaldab kiipi, mille sisse on ehitatud salajaste võtmetega failid ning mis kasutab 384-bitist ECC (inglise keeles *elliptical curve cryptography*) avaliku võtme krüpteerimist, on piisavaks tõendiks isiku identiteedile elektroonilises keskkonnas [22]. ID-kaardil olev kiip sisaldab salajasi võtmeid autentimiseks ja allkirjastamiseks, mis on sinna paigutatud nii, et neid ei ole võimalik välja lugeda, eksportida ega kopeerida [44].

Avaliku võtme krüptograafial põhinevat ID-kaarti kasutatakse muuhulgas digiallkirjade andmiseks, e-hääletamiseks, terviseandmete kontrollimiseks, retseptiravimite väljastamiseks, maksudeklaratsiooni esitamiseks. Joonisel 3 on kujutatud andmete tervikluse kinnitamist digitaalse allkirja abil [44], ehk läbi andmete krüpteerimise salajase võtmega. Kuna salajane võti ei lahku kiipkaardi seest, krüpteeritakse andmeräsi kiipkaardi sees. Allkirja kontrollimiseks arvutatakse nüüd juba allkirjastatud dokumendi räsi kasutades sama räsifunktsiooni. Seejärel dekrüpteeritakse salajase võtmega krüpteeriud räsi, kasutades allkirja andnud isiku avalikku võtit. Kui need kaks räsiväärtust on identsed, on andmete terviklus tõestatud [44].



Joonis 3. Andmete tervikluse tõendamine digitaalse allkirjaga [44]

M. Jun on aastal 2018 ilmunud artiklis [6] väitnud, et Eesti valitsus juurutas artikli kirjutamise ajal plokiahela tehnoloogiat eID süsteemidesse. Artikli allikate loetelus on Jun välja toonud A. Tapscotti ja D. Tapscotti raamatu [14], kus on viidatud, et kogu selles raamatus avaldatud informatsioon ja statistika Eesti e-lahenduste kohta pärinevad Eesti valitsuse kodulehelt www.e-estonia.com. Kontrollides e-Estonia kodulehel aastal 2015 olnud infot [16], leiab sealt ülevaate Eesti e-teenustest – meie digitaalse ühiskonna alustala moodustavatest komponentidest. Loetletud komponentide hulgas on näiteks eID kõrvuti samas loetelus oleva KSI tehnoloogiaga, mida kirjeldatakse kui vahendit, millega tagatakse Eesti digitaalses ühiskonnas kogu andmete ja süsteemide terviklikkus. Võib eeldada, et selle põhjal ongi järeldatud, et kõigi kodulehel loetletud Eesti valitsuse avalike teenuste alusena on kasutatud KSI plokiahela lahendust, ning sellele tugines ka Jun hiljem oma artiklis.

Lisaks on A. Tapscott ja D. Tapscott oma raamatus [14] viidanud president Toomas Hendrik Ilvese ja D. Tapscotti vestlusele 2015. aasta maailma majandusfoorumil Abu Dhabis, mille täpset sisu ei ole avaldatud, kuid on esile toodud Eesti laialdane tunnustatus valitsuse

digitaalsete lahenduste poolest. Veel oli viidatud intervjuule selle magistritöö jaoks läbi töötatud allikates korduvalt mainitud isikuga, Guardtime'i asutaja ja CEO Mike Gaultiga, mis leidis aset samuti aastal 2015. Viimasena mainitud intervjuust Mike Gaultiga on välja toodud, et terviklus on peamiseks küberturvalisuse probleemiks, millele eestlased on tähelepanu juhtinud ja lahendust otsides ehitanud tehnoloogia, mis lubab kõiki valitsuse andmeid verifitseerida ja välistab võimaluse, et valitsus saaks oma rahvast petta [14]. A. Tapscott ja D. Tapscott jätkavad raamatus väitega, et Eesti digilahendused tulenevad küberturvalisuse lahendusest, mis omakorda tugineb KSI-l.

5. Kokkuvõte

Käesolevas töös uuriti plokiahela kasutamist Eesti avalikes teenustes. Töö põhieesmärk oli välja selgitada, kas ja mil määral kasutatakse plokiahelat Eesti avalikes teenustes. Samuti uuris autor, kuidas on tekkinud väited, et Eesti avalikud teenused jooksevad plokiahelal, ja milline on tegelik olukord plokiahela kasutamisega Eesti avalikes teenustes.

Vajadus sedalaadi uurimistöö järele tekkis, kuna plokiahel on jätkuvalt piisavalt tundmatu nähtus inimeste jaoks, kes IT-valdkonnaga hästi kursis ei ole. Kuigi sõna „plokiahel“ on enamikule juba tuttav, ei pruugita selle sisulist tähendust alati täpselt mõista. Seda ära kasutades on lihtne luua moonutatud arusaam plokiahela kasutamisest ja tegelikust väärtusest, mida see pakub.

Töö jagunes kaheks suuremaks peatükiks, kus esimeses avati töös kasutatavaid põhitermineid ja mõisteid ning anti täpsem ülevaade plokiahela definitsioonidest. Samas peatükis sisaldus ka kirjanduse ülevaade, milles käsitleti erinevaid väiteid Eesti e-teenustes plokiahela kasutamise kohta. Töö teises osas viidi läbi avalike e-teenuste analüüs, selgitamaks välja nende seotus plokiahelaga. Täpsemalt analüüsiti kolme väidetavat kasutusjuhtu, milleks olid e-tervise infosüsteem, LHV panga plokiahela katsetused ja eID süsteemid.

Kirjanduse analüüsi käigus selgus, et suurest hulgast artiklitest joonistub välja pilt Eesti eduloost plokiahela tehnoloogial põhinevate avalike teenustega. Selgusid ka allikad, millele sageli algallikana viidati. Enim viidatud algallikad olid e-Estonia ametlik veebileht ja Oscar-Williams Gruti kirjutatud artikkel, mis räägib Guardtime'i koostööst Eesti valitsusega plokiahela tehnoloogia kasutamisel. Autori hinnangul võib kirjanduses korduvalt tsiteeritud Guardtime'i artiklite põhjal järeldada, et ettevõte Guardtime on teinud edukat reklaamikampaaniat KSI plokiahela tehnoloogiale, kuid korduvalt samale infole viidates on hiljem tekkinud ebatäpsed tõlgendused. Kirjanduse analüüsi käigus selgunud kasutusjuhte uuriti töö teises pooles lähemalt ning viidi selleks läbi poolstruktureeritud intervjuud teemaga kursis olevate spetsialistidega.

E-tervise infosüsteemi intervjuude käigus selgus, et lahendus, mis kasutas KSI ajatembeldamist, arendati küll välja, kuid see ei jõudnud kunagi kaugemale testkeskkonnas testimisest. Seetõttu on praegu väär väita, et e-tervise süsteemid jooksevad plokiahelal. Küll aga selgus, et peamiselt andmebaasi administraatorite tegevuste logidele võetakse täna Guardtime'i KSI ajatemplid. Viimane lahendus on praeguseks laiendatud kõigile TEHIK-u süsteemi logidele.

LHV panga varajasi plokiahela katsetusi ei ole samuti tänaseks kasutusele võetud. Nende esimene plokiahelal toimiva lahenduse katsetus tehti makseteenuste valdkonnas, kuid siis selgus, et teenuse hind tõusis seoses *bitcoin*'i väärtuse tõusuga hüppeliselt, ja lahendus ei täitnud enam oma eesmärki. Teiseks tugevaks argumendiks, miks mitte projektiga jätkata, oli negatiivne kasutajakogemus, mis makseteenusega kaasnes.

Viimaseks analüüsitud lahenduseks oli plokiahela kasutamine Eesti eID süsteemis, kuna kirjanduse ülevaates oli mitu korda väidetud, justkui põhineksid ka need plokiahelal. Lähemal uurimisel jõuti samuti tõdemuseni, et Eesti eID lahendused kasutavad avaliku võtme krüptograafiat, mitte KSI-d ehk võtmeta allkirjade infrastruktuuri.

Seega võib siinses töös analüüsitud kolme põhilise näite põhjal järeldada, et plokiahela kasutamise peamine lisandväärtus näib olevat selle sõna kasutamine ja tänu sellele suurema kõlapinna saavutamine. Praeguseni ei ole plokiahela kasutamine tõestanud end olulise lisandväärtusena avalike teenuste jaoks ning teenustes ja lahendustes, kus KSI plokiahel on hetkel kasutusel, toimib see pigem heidutusena.

Viidatud kirjandus

[1] Anwitaman Datta. 2019. Blockchain in the Government Technology Fabric. Vaadatud 4.11.2023 http://arxiv.org/abs/1905.08517

[2] Primavera De Filippi and Benjamin Loveluck. 2016. The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. *Internet Policy Rev.* 5, 3 (September 2016). https://doi.org/10.14763/2016.3.427

[3] Directorate-General for Communication (European Commission). 2021. *Roheline digitõend*. Publications Office of the European Union. Vaadatud 13.04.2024 https://data.europa.eu/doi/10.2775/104523

[4] Rainer Gerhards. 2024. rsyslog. *rsyslog*. Vaadatud 13.04.2024 https://www.rsyslog.com/

[5] Peter High. Lessons The Most Digitally Advanced Country In The World. *Forbes*. Vaadatud 28.01.2024 https://www.forbes.com/sites/peterhigh/2018/01/15/lessons- -the-most-digitally-advanced-country-in-the-world/

[6] MyungSan Jun. 2018. Blockchain government - a next form of infrastructure for the twenty-first century. *J. Open Innov. Technol. Mark. Complex.* 4, 1 (March 2018), 1–12. https://doi.org/10.1186/s40852-018-0086-3

[7] Arp Karm. Estonia – the Digital Republic Secured by Blockchain. Vaadatud 11.04.2023 https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

[8] Nir Kshetri and Jeffrey Voas. 2018. Blockchain-Enabled E-Voting. *IEEE Softw.* 35, 4 (July 2018), 95–99. https://doi.org/10.1109/MS.2018.2801546

[9] Michael Kuperberg, Sebastian Kemper, and Cemil Durak. 2019. Blockchain Usage for Government-Issued Electronic IDs: A Survey. . 155–167. https://doi.org/10.1007/978-3-030-20948-3_14

[10] Adegboyega Ojo and Samuel Adebayo. 2017. Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries. In *Public Administration and Information Technology*. 283–298. https://doi.org/10.1007/978-3-319-63743-3_11

[11] Harle Pihlak. 2017. eGoverment and Blockchain: Enabling Trust in public services in a digital environment. *e-Estonia*. Vaadatud 19.11.2023 https://e-estonia.com/egoverment-blockchain-guardtime/

[12] Silvia Semenzin, David Rozas, and Samer Hassan. 2022. Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. *Policy Soc.* 41, 3 (September 2022), 386–401. https://doi.org/10.1093/polsoc/puac014

[13] Clare Sullivan and Eric Burger. 2017. E-residency and blockchain. *Comput. Law Secur. Rev.* 33, 4 (August 2017), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016

[14] Don Tapscott and Alex Tapscott. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Penguin.

[15] Shaun Waterman. 2017. Nasdaq says Estonia e-voting pilot successful. *CyberScoop*. Vaadatud 27.11.2023 https://cyberscoop.com/nasdaq-estonia-evoting-pilot/

[16] 2015. Keyless Signature Infrastructure - e-Estonia. Vaadatud 05.05.2024 https://web.archive.org/web/20150910034729/https://e-estonia.com/component/keyless-signature-infrastructure/

[17] 2016. Estonian Government Adopts Blockchain To Secure 1 Mln Health Records. *Cointelegraph*. Vaadatud 04.11.2023 https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records

[18] 2018. Nordic Institute for Interoperability Solutions — There is no blockchain

technology in X-Road. *Nordic Institute for Interoperability Solutions*. Vaadatud 11.11.2023 https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-road
[19] 2018. Weekly press review | X-Road not to be confused with blockchain - e-Estonia. Vaadatud 27.04.2024 https://e-estonia.com/why-x-road-is-not-blockchain/
[20] 2018. Wayback Machine. *https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf*. Vaadatud 18.02.2024 https://web.archive.org/web/20180723152320/https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf
[21] 2019. Wayback Machine. Vaadatud 27.04.2024 https://web.archive.org/web/20190329174218/https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf
[22] 2021. ID-card - e-Estonia. Vaadatud 05.04.2024 https://e-estonia.com/solutions/e-identity/id-card/
[23] 2022. ELi digitaalne COVID-tõend - Euroopa Komisjon. Vaadatud 13.04.2024 https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_et
[24] Andmevahetuskiht X-tee | RIA. Vaadatud 13.04.2024 https://www.ria.ee/riigi-infosusteem/andmevahetuse-platvormid/andmevahetuskiht-x-tee
[25] elliptic curve cryptography - AKIT. Vaadatud 27.04.2024 https://akit.cyber.ee/term/844
[26] ISKE-rakendusjuhend-8.00.pdf. Vaadatud 05.04.2024 https://www.ria.ee/sites/default/files/documents/2022-11/ISKE-rakendusjuhend-8.00.pdf
[27] hash function - AKIT. Vaadatud 11.04.2024 https://akit.cyber.ee/term/703-rasifunktsioon
[28] KSI_data_sheet_201509.pdf. Vaadatud 05.04.2024 https://m.guardtime.com/files/KSI_data_sheet_201509.pdf
[29] public key infrastructure - AKIT. Vaadatud 21.04.2024 https://akit.cyber.ee/term/609-public-key-infrastructure
[30] Infoturve - Kursused - Arvutiteaduse instituut. Vaadatud 05.04.2024 https://courses.cs.ut.ee/2022/infsec/spring/Main/PKI
[31] hash tree (1) - AKIT. Vaadatud 05.04.2024 https://akit.cyber.ee/term/2634
[32] SHA - AKIT. Vaadatud 05.04.2024 https://akit.cyber.ee/term/1478
[33] Infosüsteemide turvameetmete süsteem ISKE | RIA. Vaadatud 08.03.2024 https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/infosusteemide-turvameetmete-susteem-iske?view_instance=0&current_page=1
[34] E-residendid on Eestis loonud üle 30 000 ettevõtte | Statistikaamet. Vaadatud 28.04.2024 https://www.stat.ee/et/uudised/e-residendid-eestis-loonud-ule-30-000-ettevotte
[35] Estonia is using the technology behind bitcoin to secure 1 million health records. *Business Insider*. Vaadatud 06.04.2024 https://www.businessinsider.in/estonia-is-using-the-technology-behind-bitcoin-to-secure-1-million-health-records/articleshow/51246942.cms
[36] Blockchain technology in healthcare: The revolution starts here | IEEE Conference Publication | IEEE Xplore. Vaadatud 04.11.2024 https://ieeexplore.ieee.org/document/7749510?denied=
[37] Guardtime Puts 1 Million Estonian Health Records on Its “Industrial Blockchain.” Vaadatud 04.11.2023 https://www.businessinsider.com/guardtime-estonian-health-

records-industrial-blockchain-bitcoin-2016-3?op=1https://www.businessinsider.com/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3?op=1
[38] e-Residency+2.0+white+paper+English.pdf. Vaadatud 27.01.2024 https://s3.eu-central-1.amazonaws.com/ereswhitepaper/e-Residency+2.0+white+paper+English.pdf
[39] Story. *e-Estonia*. Vaadatud 03.12.2023 https://e-estonia.com/story/
[40] ISKE-meetmed-8-06_0.pdf. Vaadatud 05.12.2023 https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/infosusteemide-turvameetmete-susteem-iske
[41] Eesti infoturbestandard (E-ITS) | RIA. Vaadatud 13.04.2024 https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its
[42] E-ITS. Vaadatud 04.05.2024 https://eits.ria.ee/
[43] Elektrooniline identiteet eID | RIA. Vaadatud 21.04.2024 https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/elektrooniline-identiteet-eid
[44] Infoturve - Kursused - Arvutiteaduse instituut. Vaadatud 21.04.2024 https://courses.cs.ut.ee/2020/infsec/spring/Main/ID-kaartJaMobiil-ID?jwsource=cl

Lisa 1

Intervjuu küsimustik

1. Projekti lühikirjeldus: mis oli probleem, mida plokiahela abil püüti lahendada?
    a. Kuidas hakati probleemi lahendama?
2. Milline oli teie roll projektis?
3. Millises funktsioonis plokiahelat kasutati?
    a. Mudelid / Kirjeldus?
4. Millist lisandväärtust andis plokiahel eelnimetatud funktsionaalsusele?
5. Milline oli see väärtus, mida plokiahel andis, mida muud moodi ei oleks saanud lahendada?
6. Milliseid alternatiive kaaluti?
    a. Erinevaid plokiahela tüüpe?
    b. Kas analüüsiti läbi näiteks Viable, Valuable, Vital?
    c. Kuidas jõuti lahenduseni?
7. Kuidas näete täna võimalikke lahendusi/alternatiive?
    a. Kui Teil oleks täna võimalik see otsus uuesti teha, kas jääksite sama lahenduse juurde?
8. Kas on veel midagi, mida tahaksite oma asutuse plokiahela projektiga seoses öelda?

Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks
Mina, Pirgit Pajoma

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose
Plokiahela kasutamine avalikes e-teenustes Eesti näitel,
mille juhendajateks on Jan Villemson ja Kristjan Krips,
reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Pirgit Pajoma
14.05.2024