kogumile ning järgmistes peatükkides esitatud argumendid püüavad veenda lugejat selliste väidete tõesuses.

Sissejuhatus plokiahela struktuuri

Plokiahela tehnoloogia iseenesest ei kujuta midagi põhimõtteliselt uut ega teadusele senitundmatut. Plokiahela võrkude toimimise mudeli väärtus seisneb eri instrumentide, tehnoloogiate ja põhimõtete kombineerimises nii, et need kindlal viisil kokku sobitatuna moodustavad loogilise ja kaitstud struktuuri andmete hajussäilitamiseks. Mida siis kujutab endast plokiahel? Sisult võiks seda võrrelda suure pearaamatuga, mille lehekülgedele kantakse poolte vahel tehtud finantstoimingud. See raamat on aga koostatud nõnda, et ühtegi sinna tehtud kannet pole edaspidi võimalik mingil viisil muuta ega eemaldada – seda takistavad tehnoloogiasse integreeritud tugevad krüptograafilised algoritmid. Andmeid endid ei hoita mingis kindlas kohas, mis oleks juhtimiskeskuse õigustega. Neid kopeeritakse ja sünkroonitakse ehk teisisõnu paljundatakse süsteemi kõigi osaliste, võrgu sõlmede vahel.

Seetõttu, isegi kui keegi tahab tema juures hoitavaid andmeid muuta, ei võta teised süsteemi osalised neid muutusi arvesse, sest need on tehtud süsteemis kehtivaid reegleid eirates.

Kuidas on selline „pearaamat“ üles ehitatud? Selle „lehekülgi“ nimetatakse plokkideks. Samuti kui leheküljed tavalises raamatus, järgnevad plokid üksteisele kindlas nummerdatud järjestuses. Kui aga tavalise lehekülje võib raamatust välja võtta, soovi korral teise kohta panna või üldse välja visata, siis plokkidega see ei õnnestu. Kõik plokid on omavahel jäigalt seotud spetsiaalsete krüptograafiliste „lukkudega“, mida on isegi teoreetiliselt erakordselt raske lahti murda. Siit tuleneb õigupoolest ka tehnoloogia nimetus

„plokiahel“ ehk inglise keeles *blockchain*. Selleks, et hakata andmete usaldusväärseks hoidlaks, peab iga plokiahelal põhinev struktuur vastama järgmistele kriteeriumidele.

- Sellel peab olema detsentraliseeritud tehnoloogiline alus ehk see peab oskama levitada vajalikke andmeid kõigi võrgusõlmede vahel ja toetama nende ajakohastatud olekut paljundamise ja sünkroonimisega.
- See peab toetama mittekatkestatavat seost andmeplokkide vahel, moodustades igas uues plokis viited sellele eelnenud plokkidele.
- See peab oskama kodeerida andmemassiivid tõhusalt unikaalseteks standardse suurusega teabeplokkideks ehk andmeid räsida.
- See peab kasutama lahtimurdmiskindlaid krüptograafilisi algoritme, mis on vajalikud plokkidesse kirjutatavate andmete kaitseks.
- See peab kasutama matemaatika erilise valdkonna, mänguteooria elemente selleks, et kõik süsteemi sõlmed järgiksid kehtestatud reegleid ning jõuaksid uute plokkide loomisel ja neisse andmete kirjutamisel ühise konsensuseni.

Kõik need eespool loetletud ülesanded moodustavad viis peamist sammast, millel põhinebki plokiahela tehnoloogia. Alljärgnevalt vaatame kõiki neid küllalt põhjalikult. Lugejatel võib tekkida küsimus: kus on plokiahelas tegelikult raha? Kuidas see sinna satub, kus seda hoitakse, kuidas seda saada ja edaspidi kulutada? Ja mis peamine, mil viisil on see raha kaitstud pahatahtlike rünnakute eest? Kõik on kuulnud sõna „krüptoraha“, mis seostub tihedasti plokiahela tehnoloogiaga. Peale selle on inimeste huvi

plokiahela vastu ise tehnoloogilisest vaatepunktist enamasti teisejärguline. Siiski on vaja krüptorahainvesteeringutest tulu saamiseks kas või kõige lihtsamal tasandil mõista nende toimimise põhimõtteid.

Tegelikult on krüptorahad ainult üks võimalikest „pealisehitistest" plokiahela struktuuri kohal, täpsemalt üks selle praktilise kasutamise vorme. Ajalooliselt juhtus lihtsalt nii, et esimene selle põhjal teostatud projekt, Bitcoin, on krüptorahapõhine maksesüsteem. Seejuures on tegu funktsionaalsete võimaluste poolest suhteliselt vaese projektiga, mis on esimese projekti puhul muidugi andestatav. Hoolimata sellest, et terminid *bitcoin* ja „plokiahel" ilmusid samal ajal, pole need tähenduselt sugugi sünonüümid, sest esimene neist tähistab krüptoraha, teine aga tehnoloogiat ennast, mille alusel on krüptoraha loodud. Tegelikult ilmus termin „krüptoraha" mitu aastat hiljem kui projekt Bitcoin – 2011. aastal ajakirja Forbes artiklis „CryptoCurrency". Bitcoini autor Satoshi Nakamoto ise andis sellele nimetuse *e-cash* ehk „elektrooniline sularaha". Bitcoinist kui projektist räägime veel lähemalt peatükis, mis on pühendatud plokiahela tehnoloogia praktilistele rakendustele.

Juhtimise detsentraliseerimine

Ükskõik millised süsteemid omavahel vastasmõjus olevate, seotud elementide kogumina vajavad juhtimist. Kusjuures see puudutab igasuguseid süsteeme – alates eri ühiskondade sotsiaalse organiseerumise vormidest kuni riist- ja tarkvaraliste tehnoloogiliste kompleksideni. Vastasel korral ei tagata nende projekteerimisel ja loomisel kavandatud funktsionaalsust, sest suurem osa süsteeme pole tõhusaks iseorganiseerumiseks võimelised. Selliste

juhtimisega seotud küsimustega on inimkond pidanud tegelema kogu oma ajaloo vältel.

Vaadeldes juhtimissüsteemide mitmesuguseid variante, võib need üldjoontes jagada kahte põhivormi: tsentraliseeritud ja detsentraliseeritud.

Ajalooliselt varasem sootsiumi juhtimise vorm kujunes loomulikul teel välja juba ürgajal, mil sugukondades ja hõimudes tekkis range sisemine juhtimishierarhia, kuid kogu rahvastiku juhtimise seisukohalt võib rääkida üksnes puhtast keskvõimu puudumisest. Enamgi veel, suuremal osal juhtudest kujutas iga rühm endast juhtimise mõttes isolaati, seega on keeruline kujutleda kogu *Homo sapiens*'i populatsiooni ühtse, ent detsentraliseeritud süsteemina. Tõepoolest, rühmade vahel puudusid juhtimisseosed, ja kui vastastikused suhted esinesidki, olid need eranditult destruktiivse iseloomuga. Tavaliselt olid need suunatud nõrkade rühmade hävitamisele või paremal juhul assimileerimisele tugevamate rühmade poolt. Sedamööda, kuidas rühmade vahel arenesid sotsiaalsed suhted, hakkasid tekkima püsivad seosed, millest lõpptulemusena kujunesid keerukamad hierarhilised süsteemid, mille eesotsas asusid domineerivad elemendid. Niipea kui hierarhia piires vastastikku suhtlevate rühmade arv kasvas suhteliselt suureks, hakkas süsteem omandama tsentraliseeritud mudeli jooni.

Teisisõnu, inimesed lõid mõiste „riik", mille eesotsas asus ainuisikuline valitseja, olgu siis valitav või päruslik. Selline riikliku ülesehituse vorm osutus küllaltki elujõuliseks, sest on säilinud meie päevini, olles küll läbi teinud mitmesuguseid muutusi.

Seega võib tõdeda, et ühiskonna varase arengustaadiumi pealesunnitud detsentraliseeritud juhtimisvorm arenes tollal edumeelsemaks tsentraliseeritud meetodiks.

Tsentraliseerimine lõi võimalused ressursside koondamiseks, mis omakorda võimaldas projekte ellu viia riiklikul tasandil:

pidada vallutussõdu või tegeleda suuremahuliste ehitustöödega, kusjuures üks ei välistanud sugugi teist. Hea näide on siinkohal selliste vanade riikide nagu Babüloonia või Egiptuse ajalugu. Esmapilgul on tsentraliseerimine ainus õige ja kõige tõhusam juhtimissüsteemi variant. Juba keskajal hakkasid aga ilmuma ka muud juhtimisvormid. Siinkohal ei räägi me juhtimispõhimõtete arengust, kuid teatud juhtudel ei võimaldanud poliitilised olud tõhusaid tsentraliseeritud juhtimismudeleid lihtsalt luua.

Sobiv näide on katoliku kirik, millest sai – küll alles pärast mitu sajandit kestnud võitlust – keskaegses Euroopas sõltumatu riikideülene institutsioon. Ja kuigi katoliku kiriku sisemine struktuur oli ise rangelt hierarhiline ja selle juhtimine suuresti tsentraliseeritud, olid kirikupea valimised Euroopa suurriikide vahelise poliitilise konsensuse tulemus.

Varasel uusajal tekkinud protestantism tõi uue usustruktuuri korraldusse täieliku keskvõimu puudumise.

Vastandina traditsioonilisele, tsentraliseeritud piiskoplikule juhtimisele ilmus kirikukogukondade presbüterlik juhtimine.

Ka riigid ei jäänud oma ülesehituse korraldamises ajast maha: 1291. aastal ilmus keskaegse Euroopa kaardile tõeliselt detsentraliseeritud riik, Šveitsi Konföderatsioon – mitme iseseisva kantoni liit, kus keskne poliitilise juhtimise institutsioon tegelikult puudus. Tänapäeval oskame seda ammust sündmust väärtuslikult hinnata: Šveits mitte ainult ei kaotanud sajandite vältel oma suveräänsust, vaid suutis ühtlasi tõusta üheks suurima sotsiaalse heaoluga riigiks maailmas. Teiselt poolt tunneb ajalugu näiteid, kus keskvõimu puudumine feodaalse killustatuse kujul lõppes riigi nõrgenemise, mõnel pool aga koguni hukkumisega.

Need näited kõnelevad sellest, et väide, just nagu oleks üks juhtimissüsteem parem kui teine, pole sugugi ühemõtteliselt selge. Kahtlemata on kummalgi juhtimisviisil omad plussid ja miinused.

Proovime oma analüüsi ühiskondliku korralduse vormidelt üle kanda tehnoloogilistele süsteemidele. Sotsiaalse ja tehnoloogilise juhtimisviisi sarnasus põhineb ühisel printsiibil, mis toob kaasa subjekti juhtimistegevuste tervikliku rakendamise objektile. Tehnoloogilise näitena vaatame ülemaailmse arvutivõrgu interneti struktuuri juhtimist. Kui internet tungis kõikjal inimeste ellu, hakati seda aktiivselt kasutama mitmesuguste – äriliste, riiklike, sotsiaalsete – teenuste korraldamiseks. Huvitav on see, et internet ise on detsentraliseeritud struktuur, ehkki see on olemuselt hierarhiline, eriti kasutuse madalamatel tasanditel.

Lõppkasutaja ühendub võrku teenusepakkuja kaudu, millel on aga omakorda, kui tegu on väikese organisatsiooniga, ainult üks väliskanal suurema operaatori juurde. Mida suurem on võrgu subjekt, seda rohkem on sellel ühendusi teiste suurte subjektidega nii otseühenduste kaudu kui ka võrguliikluse vahenduspunktide kaudu. Kõige suurematel võrguoperaatoritel on oma magistraalkanalite taristu kogu maailmas ja nad tagavad edastatavate andmete jaoks kõige suurema osa läbilaskevõimest. Sellest hoolimata puudub internetil üksainus „murdepunkt". See tähendab, et süsteemi ühe osalise, isegi küllaltki suure osalise väljalülitamine ei põhjusta võrgu kui terviku töö katkemist, välja arvatud selles segmendis, mis oli täielikult võrgust välja langenud suure sõlme taga. Kusjuures nimetatud segmendi elemendid võivad säärasel juhul ümber lülituda reservkanalitele ja naasta võrku.

Just sellise murdumispunkti puudumine ongi üks detsentraliseeritud süsteemide peamiseid eeliseid. Tuleme tagasi Šveitsi näite juurde: teame, et ei liidupresidendil ega ühelgi teisel selle riigi poliitilisel institutsioonil pole õigust anda välise sõjalise sissetungi korral kapitulatsioonikäsku. Ja kui selline käsk antakski, keelab seadus riigi elanikel kategooriliselt selle täitmise. Seetõttu tuleb agressoril tegeleda peaaegu iga šveitslasega eraldi. Sama käib ka

interneti kohta. Isegi kui mõni riik tahab oma poliitilise otsusega interneti välja lülitada, on selle tehnoloogiline teostamine suure tõenäosusega võimalik ainult oma territooriumil (välja arvatud sõlmed, mis on internetiühenduses satelliitside kaudu, kui satelliit kuulub teisele riigile). On võimalik, et kannatavad ka kasutajad teistes riikides, kust tulevad magistraalkanalid on ühenduses transiitsõlmedega globaalsest võrgust eralduda soovivas riigis. Kogu ülejäänud võrk maailmas säilitab aga oma töövõime.

Õigupoolest on interneti hävitamiseks vaja välja lülitada peaaegu kõik selle sõlmed, mis on juba iseenesest nii korralduslikult kui ka tehnoloogiliselt sedavõrd keerukas, et plaani elluviimine on niisama hästi kui võimatu. Seega võime rääkida ilma ühtse juhtimiskeskuseta hajustopoloogiaga võrgu teoreetilisest haavamatusest. Kui aga läheme interneti baasil ehitatud teenuste tasandile, siis näeme, et suurem osa neist toimib klient-server-tehnoloogial – see tähendab tsentraliseeritud tehnoloogial.

Me kõik oleme juba ammu harjunud kasutama mitmesuguseid internetiteenuseid.

Portaalid, mis pakuvad elektronpostiteenust, andmete (näiteks dokumentide ja fotode) pilves hoidmise süsteemid, juurdepääs pank-klient-süsteemile oma arvete majandamiseks ja maksete tegemiseks, hotellide ja lennukipiletite broneerimine, kauplemisplatvormid tehinguteks finantsturgudel ja palju muudki – kõik need teenused on ehitatud tsentraliseeritud taristu põhjal. Kõigi selliste süsteemide kasutamiseks on vaja ressurssidele ja teenustele juurdepääsuks minna konkreetse teenuseosutaja veebilehele, sisestada oma kasutajanimi ja parool ning luua ühendus kesksserveriga, kus hoitakse kliendi andmeid või vara. Kui aga teenuseosutaja kesksever on mingil põhjusel maas, ei saa me seda teenust kasutada ja meil tuleb oodata, kuni serveri töövõime taastatakse. Sellisel juhul puutume kokku tsentraliseeritud süsteemi suurima

probleemiga – selles on murdumispunkt. Teenuse tõrge võib olla tingitud mitmesugustest teguritest: tehnoloogilisest probleemist, näiteks seadme rikkest, tarkvaraveast, kuritarvitustest teenuseosutaja enda struktuuris, mitmesugustest häkkerirünnakutest või arvutiviiruste tegevusest. Sugugi mitte vähetähtsat rolli võivad mängida ka riiklike jõu- ja järelevalvestruktuuride repressiivtoimingud sel territooriumil, kus teenusteosutaja füüsiliselt asub.

Kõik need tegurid, mille tagajärg on teenusetõrge, panevad mõtlema sellest, mil viisil saaks sääraseid olukordi tehnoloogiliste või töökorralduslike meetmetega ära hoida. Vastuseks sellele küsimusele saigi detsentraliseeritud andmehoiu ja -vahetussüsteemina ehitatud plokiahela tehnoloogia ilmumine, mis välistab kõik tsentraliseeritud teenuste puhul loomupäraselt ilmnevad negatiivsed tegurid. Võrgu tähttopoloogia asemele, milles kõigist sõlmedest-kasutajatest lähtuvad kiired kohtuvad kindlasti keskpunktis – sõlmserveris, tuli võrgu korraldusviis, kus keskserver kui selline üldse puudub, kõik sõlmede-klientide vahelised vastastikused toimingud tehakse aga otse omavahel. Selliseid võrkusid nimetatakse võrdvõrkudeks. Enamasti on kõik sõlmed sellises võrgus võrdõiguslikud ja igaüks neist võib täita nii kliendi kui ka serveri funktsioone. Selline detsentraliseeritud võrgutopoloogia kõrvaldab murdumispunkti teguri ning suurendab süsteemi usaldusväärsuse ja töökindluse peaaegu täiuslikuks.

Ometigi võib lugejatel siinkohal tekkida täiesti mõistlik küsimus: kui serverid võrgus üleüldse puuduvad, kus hoitakse siis sellises võrgus ühisandmeid, kuidas neid võrgus levitatakse ja mil viisil on need kaitstud lubamatu juurdepääsu ja muutmise eest? Samuti, mil viisil selliseid süsteeme hooldatakse ja arendatakse, kui kõigil võrgu osalistel on võrdsed õigused? Plokiahela tehnoloogia annab vastuse enamikule neist küsimustest.

Andmeid paljundatakse (kopeeritakse) süsteemi kõigi sõlmede vahel. Kaitse muutmise või lubamatu juurdepääsu eest andmetele tagavad asümmeetrilise krüptograafia matemaatilised algoritmid. Kogu süsteem töötab ette antud reeglite alusel, millega kõik süsteemi osalised nõustuvad. Juhul, kui on vaja teha olulisi muutusi, võetakse otsus vastu süsteemi osaliste üldhääletusel.

Tuleb märkida, et detsentraliseeritud süsteemide haldamine on tsentraliseeritutest suurusjärgu võrra keerulisem. Seda tuleb aga käsitleda kui hinda nende eeliste eest, mida pakub detsentraliseerimine. Praegu pole lahendatud sugugi kõik probleemid, mis detsentraliseeritud süsteemide juhtimisel ilmneda võivad. Järgmistes peatükkides tuleme seetõttu nende teemade juurde veel korduvalt tagasi.

Andmete räsimine

Andmete räsimine on meetodina plokiahela tehnoloogia tähtis ja lahutamatu osa. Räsimist kasutatakse plokiahela süsteemides adresseerimiseks, teadete elektrooniliste allkirjade moodustamiseks, kuid ka krüptomüntide hankimiseks ehk kaevandamiseks (ingl *mining*) mõnes plokiahela projektis, mis põhinevad „töö tõestamise“ põhimõttel. Enne kui uurime lähemalt eespool nimetatud plokiahela süsteemi elemente, on meil vaja selgeks saada, mis on õigupoolest andmete räsimine ja missugustel põhimõtetel see protseduur töötab.

Alustame mõistest. Räsimine on meetod suvalise suurusega andmekogumi teisendamiseks spetsiaalse algoritmi abil standardseks, fikseeritud pikkusega reaks. See tähendab, et kui võtame mingi andmekogumi, näiteks sellesama raamatu teksti, siis saame luua selle digitaalse jäljendi pikkusega näiteks 10 sümbolit.