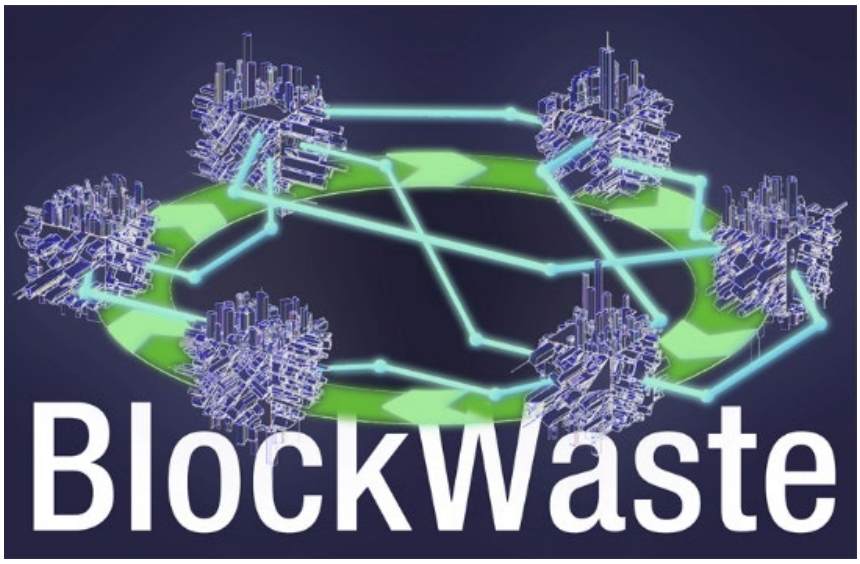
O1.A3 Ringmajanduse strateegiate käsiraamatud, mida rakendatakse olmejäätmete käitlemisel, kasutades Blockchaini tehnoloogiat

II käsiraamat: Blockchain



ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ IKY

Co-funded by the Erasmus+ Programme of the European Union

Väljundi teabeleht:

Rahastamisprogramm	Euroopa Liidu programm Erasmus+
Rahastamine NA	EL01 Kreeka riigi stipendiumifond (IKY)
Projekti täispealkiri	Jäätmekäitluses rakendatav uudne Blockchaini tehnoloogial põhinev koolitus – BLOCKWASTE
Väli	KA2 - Koostöö innovatsiooni ja heade tavade vahetamise nimel KA203 – Kõrghariduse strateegilised partnerlused
Projekti number	2020-1-EL01-KA203-079154
Projekti kestus	24 kuud
Projekti alguskuupäev	10.01.2020
Projekti lõppkuupäev:	30-09-2022

Väljundi üksikasjad:

Väljundi pealkiri: O1: Interdistsiplinaarse Blockchain-MSW õppematerjalid

Ülesande pealkiri: O1/A3. Ringmajanduse strateegiate käsiraamatud, mida rakendatakse olmejäätmete käitlemisel, kasutades Blockchaini tehnoloogiat

Väljundi juht: NTUA

Ülesande juht: Saksioni UAS

Autor(id): Christa Barkel, c.barkel@saxion.nl, Saxion UAS, Holland, Perry Smit, Saxion UAS, p.j.smit.01@saxion.nl, Holland

Arvustanud: Rainer Lenz, rlenz@fh-bielefeld.de, Bielefeldi UAS, Saksamaa, Paraskevas Tsangaratos, National Technical University of Athens, ptsag@metal.ntua.gr, Greece

Dokumendikontroll

Dokumendi versioon	Versioon	Muudatus
V0.1	11/03/2022	Lõplik versioon – 29/04/2022

Co-funded by the Erasmus+ Programme of the European Union

Sisukord

Jooniste loend

Lühendite loetelu

Lühend	**Definitsioon**
CBDC	Keskpanga digitaalne valuuta
CBDC	Keskpanga digitaalne valuuta
DAO	Detsentraliseeritud autonoomne organisatsioon
dApps	Detsentraliseeritud rakendused
DLT	Hajutatud pearaamatu tehnoloogia
dPoS	Delegeeritud osaluse tõend
ERC-20 (protokoll)	Ethereumi kommentaaride taotlus 20 (protokoll)
ICO	Müntide esialgne pakkumine
IEO	Esialgne vahetuspakkumine
MSW	Tahkete olmejäätmete käitlemine
NFT	Mitteasendatav märk
P2P	Peer-to-Peer
PoS	Panuse tõend
PoA	Volitusi tõendav dokument
SPOF	Üksik ebaõnnestumise punkt
STO	Turvamärgi pakkumine
TTP	Usaldusväärne kolmas osapool

Kokkuvõte

Selles käsiraamatus käsitletakse plokiahelat mitmest vaatenurgast. Loodetavasti aitab see lugejal Blockchaini asjakohasust paremini lahata ja selle potentsiaalist sügavamalt mõista. Esimesed põhitõed on selgitatud näitena Bitcoiniga. Bitcoin on esimene rakendus, mis kasutab Blockchaini. Bitcoin kasutab detsentraliseeritud võrku, milles kõik isikud, kes soovivad Bitcoini otsustusprotsessis osaleda, võtavad üheskoos osa otsuste tegemisest. Bitcoini kood on avatud lähtekoodiga, võimaldades igaühel hõlpsasti vaadata, kopeerida ja redigeerida lähtekoodi vastavalt oma maitsele, võimaldades tekkida uusi katseid teiste, võib-olla paremate krüptovaluutavormide või muude rakendustega ja muud konsensuse vormid. Kuigi selgituseks kasutatakse Bitcoini, on oluline märkida, et Blockchain ei mõjuta mitte ainult finantssüsteemi. Blockchaini aluseks olev tehnoloogia pakub uusi võimalusi muude tööstusharude, sealhulgas tahkete olmejäätmete käitlemise ümberkujundamiseks.

See käsiraamat algab Blockchaini ja selle funktsioonide selgitusega. Selgemalt eristatakse krüptovaluuta bitcoini ja Bitcoini võrgustikku ning selgitatakse Bitcoini konsensusmehhanismi Proof-of-Work. Lisaks selles käsiraamatus Bitcoini abil selgitatud plokiahela põhiprintsiipidele nihkub fookus uuema põlvkonna plokiahelatele, mis on spetsiaalselt loodud suure hulga muud tüüpi detsentraliseeritud rakenduste või dAppide loomiseks. Üks konkreetne Blockchain, millele tähelepanu keskendub, on Ethereum, mis võimaldas esimesena nutikate lepingute programmeerimist. Nutikas leping on detsentraliseeritud automatiseerimine ja seda saab määratleda kui lepingut, mille tingimused on koodis sätestatud. Leping on isetäituv, kuna sooritab tingimuste täitmisel vastavad vastavad toimingud.

Lisaks selgitab käesolev käsiraamat lühidalt kahte plokiahela nähtust: detsentraliseeritud rakendused (dApps) ja detsentraliseeritud autonoomsed organisatsioonid (DAO).

Blockchaini saab jagada selle tüüpidesse kolmest vaatenurgast, konsensusprotokollist, juhtimisest ja Blockchaini süsteemide koostöö tüüpidest. Konsensusprotokollid on hajutatud võrgus erinevate osalejate vahelise usalduse tagamiseks hädavajalikud. Peab olema kindel, et osalejad ei ole rikutud ja nende vahel jagatud andmed ei ole rikutud. Järgmiseks tuleb Blockchaini, nagu iga partnerlust, hallata ja kontrollida Blockchaini juhtimisstruktuuri kaudu. Erinevat tüüpi Blockchainide vahelised valikud mõjutavad organisatsiooni kontrolli. Mida rohkem usaldatakse Blockchaini detsentraliseeritud olemust, seda lihtsam on osaleda. Mida suurem on kindlustunne, et valideerijad võivad konsensuse loomisel osaleda tundmatutena, seda läbipaistvam on süsteem.

Kolme vaatenurga kokkuvõtteks võib öelda, et Blockchaini süsteemide vahel on erinevat tüüpi koostööd. Plokiahelat, kus erinevad ettevõtted ja kolmandad osapooled teevad koostööd ilma seda plokiahelat kontrolliva keskse kasutajata, nimetatakse ettevõtte plokiahelaks. Sellise Enterprise Blockchaini ehitamiseks kasutavad ettevõtted Blockchaini platvorme. Need platvormid võimaldavad kasutajatel teatud tehnoloogiaid kasutades rakendusi kirjutada. Nende platvormide ümber on korraldatud mitmesuguseid partnerlusi. Platvormid on kolmas ja viimane viis, kuidas me siin eri tüüpi plokiahelaid vaatleme.

Satoshi Nakamoto üks suurepäraseid leiutisi on juba olemasolevate tehnoloogiate kombinatsioon tasustamissüsteemiga, mis hoiab detsentraliseeritud võrgu töös: krüptoökonoomika . Blockchaini krüptoökonoomika keskne idee seisneb selles, et töötatakse välja protokollid, mis julgustavad inimesi võrgus osalema nii, et võrgu väärtus oleks osalejate jaoks maksimaalne.

Krüptomärgi saab luua plokiahelas ja see kujutab endast ka kaubeldavat vara. Mõnikord luuakse märgid projekti rahastamiseks. Žetooni loomise protsessi nimetatakse tokeniseerimiseks. Nende žetoonidega kauplemine võimaldab alusvara omandiõiguse üle anda. See käsiraamat selgitab eri tüüpi märke ja nende kasutamist.

Kokkuvõtteks on toodud kolm näidet plokiahela kasutamise ja rakendamise kohta, sealhulgas mõnede plokiahela edukaks rakendamiseks vajalike oluliste tingimuste tõlgendamine.

1 Sissejuhatus

1.1 Projekti lühikirjeldus

Projekti BlockWASTE eesmärk on käsitleda jäätmekäitluse ja Blockchaini tehnoloogia koostalitlusvõimet ning edendada selle nõuetekohast käitlemist läbi koolituse, et kogutud andmeid jagataks turvalises keskkonnas, kus kõigi asjaosaliste vahel ei jää ruumi ebakindlusele ja umbusule. Selleks on BlockWASTE projekti eesmärgid järgmised:

- Viia läbi uuringuid linnades tekkivate tahkete jäätmete ja nende käitlemise kohta, et neid saaks kasutada heade tavade infobaasi loomiseks, et tuua jäätmed uuesti väärtusahelasse, edendades intelligentsete ringlinnade ideed.
- Plokiahela tehnoloogia eeliste tuvastamiseks olmejäätmete käitlemise protsessis.
- Koostada õppekava, mis võimaldab koolitada valdkonna organisatsioonide ja ettevõtete õpetajaid ja spetsialiste, jäätmekäitluse, ringmajanduse ja plokiahela tehnoloogia valdkondade kattuvuses.
- Töötada välja plokiahela tehnoloogial põhinev interaktiivne tööriist, mis võimaldab praktikas rakendada olmejäätmetest saadud andmete haldamist, visualiseerides seeläbi andmete plokiahelas juurutamise viisi ja võimaldades kasutajatel hinnata erinevaid haldusvorme.

BlockWASTE eesmärk on juurutada rahvusvaheliselt uusi õppesisu eesmärgiga koolitada oma õpilasi partnerriikides ja anda neile vajalikud põhioskused, mis võimaldavad neil selles sektoris tulevaste töötajatena professionaalselt tegutseda, lisades digitaalseid pädevusi, mida vajavad valdkonnaga tegelevad ettevõtted. digitaalse transformatsiooni protsess. Selles mõttes on projekt suunatud:

- Ettevõtted ja VKEd, IT-spetsialistid, urbanistika ja jäätmekäitluse spetsialistid.
- Ülikoolid (professorid, üliõpilased ja teadlased).
- Avalik-õiguslikud asutused

Projekt sisaldab nelja intellektuaalset väljundit:

- O1. Interdistsiplinaarse Blockchain-MSW õppematerjalid
- O2. Euroopa ühtne MSW õppekava, mis rakendab plokiahela tehnoloogiaid ringmajanduse strateegiates
- O3. Blockchain-MSW-l põhinev e-õppe tööriist, mis keskendub ringmajandusele
- O4. BlockWASTE avatud õpperessurss (OER)

See dokument kirjeldab ja selgitab Blockchaini põhiprintsiipe. See kirjeldab, mis on Blockchain, millal saate seda kasutada, millistest komponentidest Blockchain koosneb, milliseid Blockchaini tehnoloogiaid kasutatakse ja kirjeldatakse erinevaid edukaid Blockchaini rakendusi.

1.2 Eesmärgid ja metodoloogiline lähenemine

Selle käsiraamatu “Blockchain” eesmärk on juhendada jäätmekäitlussektori spetsialiste, kuidas nad peaksid IoT-d ja Blockchaini tehnoloogiat ringmajanduse strateegiatena rakendama. Seetõttu on see suunatud praktikutele, kes teavad Blockchaini tehnoloogia kasutamise eeliseid. Selle Blockwaste projekti kolme ühise käsiraamatu eesmärk on anda

lugejatele piisavad teadmised Blockchaini tehnoloogia potentsiaalist, et aidata kaasa tahkete olmejäätmete käitlemise suuremale ringikujulisusele. Käsiraamatut 1 (plokiahel) ja käsiraamatut 2 (ringmajandus) tuleb mõista lühikokkuvõttena ja need annavad ülevaate käsiraamatu 3 (plokiahelapõhine jäätmekäitlus) olulisest sisust – vt joonist 1.

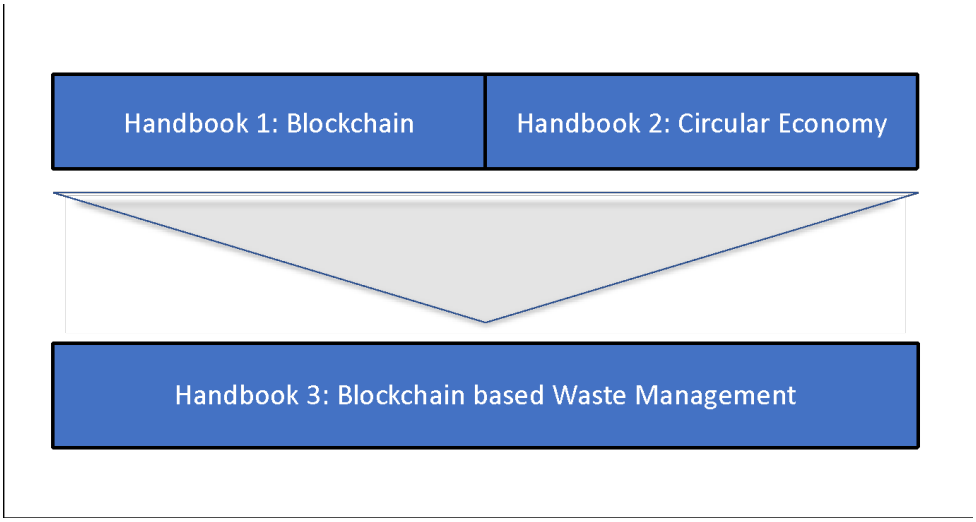


Figure 1:Käsiraamatud BlockWASTE projekt (autorid)

Käsiraamatu ülesehitus järgib deduktiivset loogikat, esitledes esimeses osas (peatükk 1 kuni 4) lühikest Blockchaini ajalugu Bitcoini abil ja Blockchaini tehnoloogia põhitõdesid. Käsiraamatu teine osa (5. peatükk) sisaldab selged juhised Blockchain Technology kasutuste ja rakenduste kohta.

2 Plokiahela põhialused

Blockchaini põhimõtete mõistmine Bitcoini kaudu

"Vabandust, et olen märg tekk. Sellele asjale laiemale publikule kirjelduse kirjutamine on jube raske. Seda pole millegagi seostada.»
- Satoshi Nakamoto (2010)

2.1 Sissejuhatus

Õppeeesmärgid

- Blockchain kõige elementaarsemal tasemel, vaadates Bitcoini.
- Blockchain on sisuliselt hajutatud pearaamat, kuhu saate andmeid salvestada.
- Blockchaini võrgu ja tsentraliseeritud võrgu erinevused.

Sissejuhatus

31. oktoobril 2008 saadeti Satoshi Nakamoto nime all e-kiri Cryptography meililisti. [1]E-kiri sisaldas viidet **valgele raamatule** pealkirjaga *Bitcoin: Peer-to-Peer elektrooniline sularahasüsteem* . Teatele lisatud valge raamat on kõigest 9-leheküljeline dokument, mis kirjeldab Bitcoini tehnilisi toiminguid. See süsteem võimaldab saata Interneti-makseid teistele osapooltele, ilma et selleks oleks vaja finantsasutust.

Selle maksesüsteemi peamised omadused Satoshi sõnul:

1. Kahekordne kulutamine on peer-to-peer võrguga välistatud.
2. Ei rahapaja ega muid usaldusväärseid osapooli.
3. Osalejad võivad olla anonüümsed.
4. Uued mündid on valmistatud Hashcash stiilis töötõendist.
5. Uue müntide genereerimise töötõend annab võrgule ka volitused topeltkulu vältimiseks.

Tehnilised terminid, nagu topeltkulu, peer-to-peer võrk, töötõend, räsiraha, ajatemplid, räsimine ja e-kirjade digitaalallkirjad, muudavad üldsuse jaoks Bitcoini või üldisemalt plokiahela mõistmise keeruliseks. Eriti sel ajal, kui enamiku inimeste jaoks polnud seda millegagi seostada. Selles peatükis käsitleme Bitcoini kui vahendit plokiahela põhiprintsiipide mõistmiseks.

[1]Algse meili leiate aadressilt: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html .

Co-funded by the Erasmus+ Programme of the European Union

2.1.1 Bitcoin vs bitcoin

Üldjuhul teeme vahet (väikest tähtedega) bitcoinidel, digitaalsel rahal, mida nimetatakse ka krüptovaluutaks, ja (suurtähtedega) Bitcoinil, aluseks olevat finantsvõrku, mis võimaldab bitcoine saata ja vastu võtta.

2.1.2 Peer-to-peer võrk

Arvutid, mida nimetatakse ka ***sõlmedeks*** ja mis seda finantsvõrku käitavad, hoiavad ja neil on juurdepääs pearaamatule, kuhu salvestatakse kõik bitcoini tehingud. See Bitcoini pearaamat on kirje kõigi kehtivate tehingute kohta, mis on kunagi võrku edastatud, mis on aluseks olev infrastruktuur, mis koosneb sõlmedest, mis jälgivad, kinnitavad ja ajatemplid kõiki bitcoini tehinguid. Nimetame seda võrku ***peer-2-peer (P2P) võrguks*** .

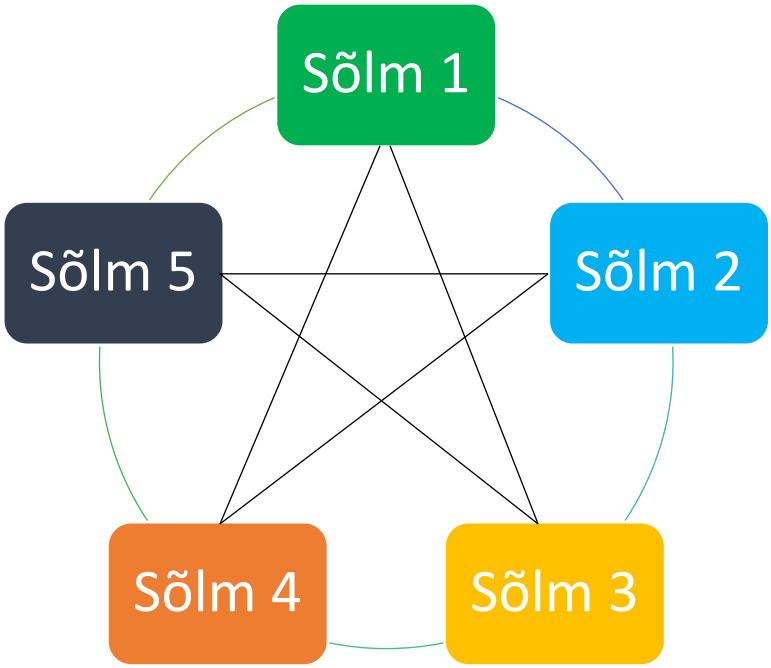


Figure 2: Hajutatud võrgu esitus, kus plokiahel on jaotatud üle täissõlmede võrgu (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 1. peatükk, lk 14).

P2P-võrk on sõlmede võrk, sageli arvuti, mis on võrdselt privilegeeritud. Iga sõlm võib olla nii teenusepakkuja kui ka teenuse tarbija. Igaühel on juurdepääs Bitcoini võrgule ja ta saab vabalt hallata võrgu sõlme. Spetsiaalsed võrgusõlmed, mida nimetatakse ka ***täissõlmedeks*** , säilitavad kogu tehingute ajaloo. Kogu võrgu ja sellele vastava tehinguajaloo mahavõtmiseks tuleks sulgeda kõik sõlmed, mis on peaaegu võimatu, kui võrk koosneb paljudest sõlmedest.

Iga võrgus osaleja järgib Bitcoini protokolli. Bitcoini protokoll on protseduurireeglid, mis reguleerivad Bitcoini võrku. Lisaks puudub kahe erineva sõlme vahel vahendaja. See tähendab ka seda, et puudub keskne osapool, kes saaks teie tehinguid reguleerida, peatada ja külmutada. Selliste vahendajate kõrvaldamine võimaldab teha tõhusamaid ja odavamaid tehinguid.

2.1.3 Klient-server võrk

See P2P-võrk erineb ***klient-serveri võrgust*** (tööjaam-server võrk).

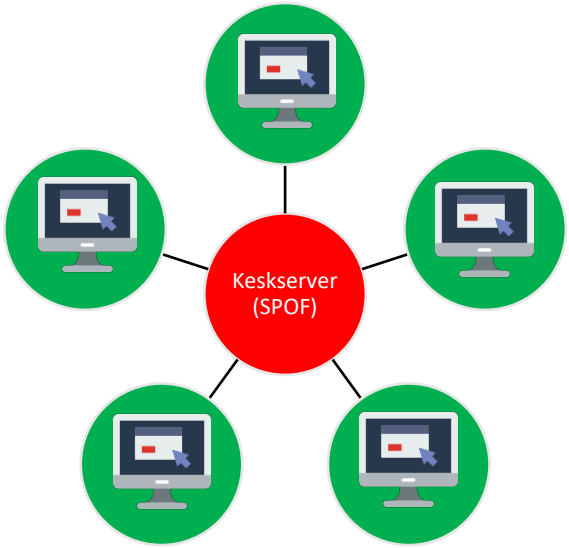


Figure 3:Lihtsustatud otsustuspuu, kas kasutada plokiahelat või mitte (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 1. peatükk).

Klient-server-võrk kasutab tsentraliseeritud servereid, mis pakuvad oma klientidele teenuseid, näiteks e-posti teenust. Server sisaldab sageli andmeid ja rakendusi. Kui kliendid vajavad juurdepääsu nendele ressurssidele, saavad nad serverile päringu esitada. Klient-server võrkude nõrkus on see, et see sisaldab üht ***tõrkepunkti (SPOF)*** . Sel juhul on SPOF keskserver. Kui see on keelatud, ei pääse kliendid enam serveri teenustele juurde.

Vajadus usaldada oma andmed kesksele osapoolele ja usaldada, et SPOF ei ebaõnnestu, muudab mudeli haavatavaks. SPOF-võrgu disaini tõttu võivad kannatada ka suured mainekas ettevõtted. Näiteks 2015. aastal oli voolukatkestus ühes PayPali andmekeskuses. Seetõttu ei pääsenud paljud kasutajad enam PayPali veebisaidile, krediitkaarditehinguid ei saanud enam töödelda, inimesed ei pääsenud enam ligi oma isiklikule kontoandmetele või kuvati valed bilansid.[2]

2.1.4 Hübriidvõrgud: Napsteri juhtum

Samuti on olemas hübriidvõrgud. Üks kuulus näide on Napster, muusika allalaadimisteenus, mis kogus tuntust 1990ndate lõpus ja 2000ndate alguses.

[2] https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

1999. aastal käivitasid teismelised Shawn Fanning ja Sean Parker peer-to-peer failijagamisteenuse nimega Napster. Napster võimaldas inimestel hõlpsalt teistelt digitaalseid muusikafaile jagada ja alla laadida. See tekitas palju kära, sest esimest korda jagati muusikat omavahel laialdaselt tasuta. Napster võimaldas inimestel üksikuid laule alla laadida ja kuulata. Varem, kui tahtsid üksikut lugu saada, pidid ostma terve albumi. 2001. aastal suleti Napster pärast kohtuasja Ameerika salvestustööstuse assotsiatsiooniga, kuna digitaalsete muusikafailide levitamist ja allalaadimist peeti autoriõiguse seaduse rikkumiseks. Sellegipoolest on Napster endiselt tuntud kui revolutsiooniline teenus, mis on muusikatööstuse häirinud. Ameerika Ühendriikides saavutas CD-müük haripunkti 2000. aastal, misjärel toimus järsk langus – osaliselt tänu Napsterile ja sellele järgnevatele teenustele nagu BitTorrent ja Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

Figure 4:New Yorgi aja uudised; Napsteril kästi jääda suletuks, 12. juulil 2001.

Napster kasutab teatavasti P2P-võrku. Miks on võimud suutnud Napsteri sulgeda, mis Bitcoiniga on praktiliselt võimatu?

Napster kasutab keskset indeksit, mis jälgib, millisel arvutil on milliseid faile teiste kasutajatega jagada. Kui kasutaja (arvuti A) soovib otsida laulu, näiteks Michael Jackson - Billie Jean, luuakse ühendus registriga ja register otsib, millistes arvutites see lugu on. Kui indeks näitab, et arvutil B on see lugu, luuakse arvutite A ja B vahel otsene võrdõigusühendus, mis võimaldab A-l numbri B arvutist otse alla laadida.

Napster on kliendi-serveri ja peer-to-peer segamudel. Kekseks indeksielemendiks on klient-server, kuid tegelikud failid laaditakse alla peer-to-peer. Keskne registriserver on osutunud Napsteri jaoks tõsiseks Achilleuse kannaks, kuna seda saab hõlpsasti sulgeda, mistõttu Napster lakkab töötamast. Kuna Napsteril on ainult keskne registriserver, mis loetleb, millistel arvutitel on jagatavad muusikafailid, pole Napsteri enda serveris muusikafaile. See on ainult aidanud kasutajatel luua peer-to-peer ühendusi ja jagada muusikat üksteisega.

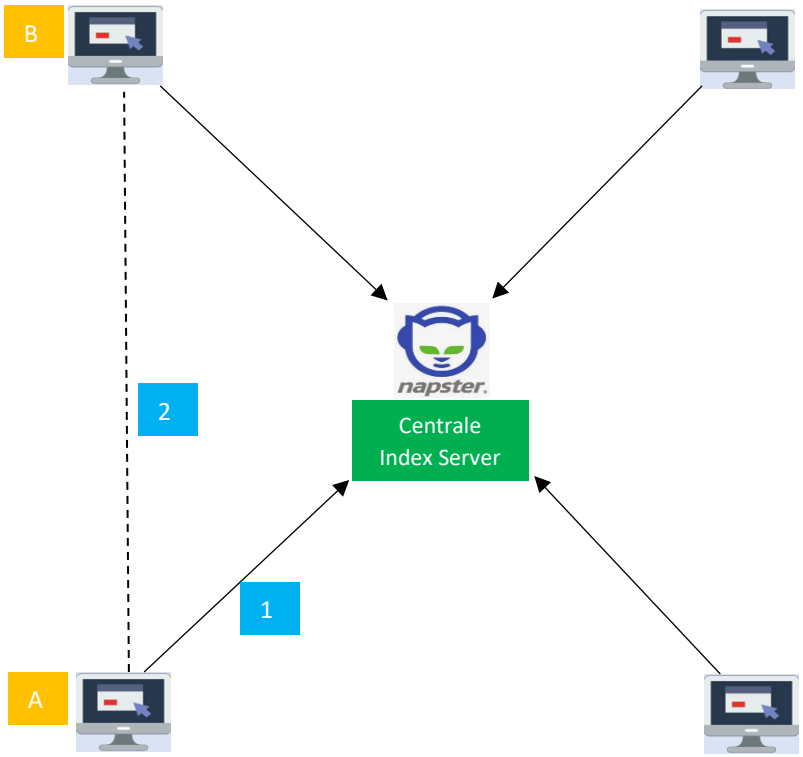


Figure 5:Napsteri võrk. (1) Arvuti A otsib Napsteri kesksest registriserverist Michael Jacksoni – Billy Jeani. Napsteri keskne registriserver otsib võrku ühendatud arvuteid, mille kõvakettal on number saadaval. (2) Arvutil B on number. Arvutitele A ja B paigaldatakse otsene peer-to-peer ühendus, mille järel arvuti A laadib muusikafaili arvutist B alla.

Kuigi muusikafailide jagamine on Napsteriga peer-to-peer, sisaldab see ka keskserveri elementi, mis muudab selle rünnakutele vastuvõtlikuks. Antud juhul suleti see korrakaitsjate poolt. Bitcoini võrguga on kõigil sõlmedel Bitcoini avaliku pearaamatu täpne koopia. Bitcoini võrk koosneb paljudest sõlmedest, mis on levinud üle kogu maailma, mistõttu on nende kõigi asukoha leidmine ja sulgemine keeruline.

2.1.5 Plokiahel

Bitcoini avalikku pearaamatut peetakse detsentraliseerituks, kuna see on jaotatud sõlmede vahel üle kogu maailma. Bitcoini avalikku pearaamatut nimetatakse ka plokkide ahelaks või plokiahelaks, mis sisaldab tehinguandmeid. Kui vaatleme plokiahelat teavet salvestava andmebaasina, on need plokiahela olulised omadused:

1. Andmed on paigutatud andmeplokkidesse.
2. Plokid kasvavad ploki numbrites järk-järgult.
3. Andmed on usaldusväärsed, kuna need on krüptograafiliselt kontrollitavad.

Kett on tehingute andmebaas, mille loovad Bitcoini võrgu kaevandamisprotsessis osalevad sõlmed. Ahela haldab ajatempliserver, mis genereerib tõendi tehingute kronoloogilise

järjekorra kohta. Iga plokk sisaldab räsiviiteid plokile, millele see tugineb, mis loob aja jooksul lineaarse jada. Plokke võib pidada rekordiraamatu üksikuteks lehtedeks.

Kaevurid töötlevad tehinguid pidevalt plokkideks, mille nad ahela lõppu lisavad. Protsessi, mille käigus kaevandajad ahelasse uusi plokke lisavad, nimetatakse ka ***töötõestuseks*** . See protsess väldib ***topeltkulutusi*** .

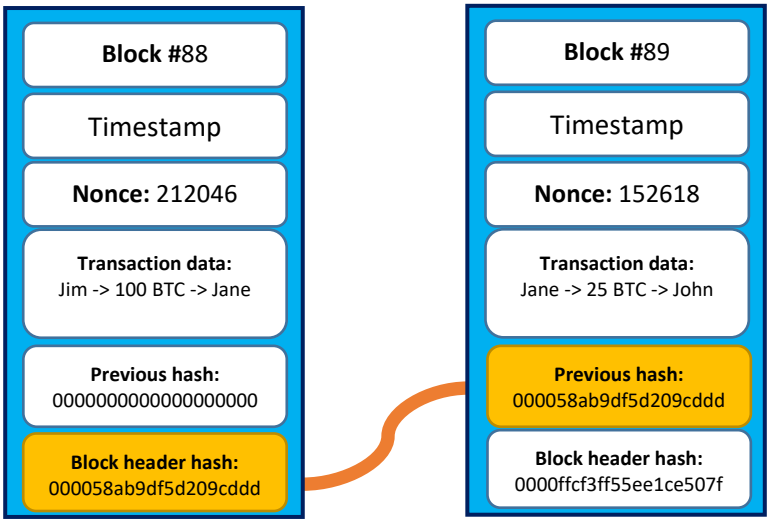


Figure 6:Kehtiva tekkeploki ja ploki nr 2 lihtsustatud esitus, kusjuures mõlemad plokid on aheldatud, kasutades ploki päise räsi ja eelmist räsi. (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 3. peatükk).

2.1.6 Topeltkulu

Oluline probleem, mida peer-to-peer elektrooniline finantssüsteem peab lahendama, on topeltkulutamise küsimus. Topeltkulutamine on bitcoini mitu korda kulutamine. Näiteks kui teil on 1 bitcoin ja kulutate selle korraga inimesele A ja inimesele B. Tsentraliseeritud finantsvõrgustikus saab topeltkulu probleemi lahendada ***usaldusväärne kolmas osapool (TTP)*** mis haldab pearaamatut ja kontrollib kõiki pearaamatus olevaid tehinguid.

Bitcoini võrgus lahendatakse see probleem selle majanduslike stiimulite ja ajatempliserveri kasutamise kaudu. Kaevuritel on tugev stiimul neid tehinguid plokki mitte kaasata, kuna neil on oht, et teised kaevurid lükkavad nende blokeeringu tagasi, ja lisaks osalevad nad kuriteo toimepanemises.

2.1.7 Töötõestus

Lisaks topeltkulutamise vältimisele on töötõendamise eesmärk ka kaitsta võrku ründajate eest ning jõuda konsensusele avaliku pearaamatu seisu osas. Lühidalt öeldes on töötõend mehhanism, mis nõuab, et kaevurid kasutaksid arvutivõimsust, et leida õiged väärtused ploki kallal, mille kallal nad töötavad. Õige räsiväärtuse leidmisel on neil lubatud lisada plokk B - lukuahelasse ja saada tasu bitcoinides. Õige väärtuse leidmise protsessi nimetatakse kaevandamiseks.

Võrku edastatavaid tehinguid ei lisa kaevandaja otse plokki ega salvestata neid otse pearaamatusse. Esmalt satuvad need ***mälukogumisse*** (mempool) koos muude tehingutega, mida kaevandajad peavad veel plokki lisama ja mida võrk peab veel kinnitama. Mempooli võib pidada ootealaks kõigi sissetulevate tehingute jaoks, mida võrk peab veel kinnitama. Igal kaevandajal on oma mempool ja on võimalik, et üksikud mempoolid on kaevandajate lõikes erinevad. Selle põhjuseks on asjaolu, et arvutivõrgus on alati võrgu latentsusaeg: võrku saadetud tehingu kõigi võrgu kaevuriteni jõudmiseks kulub alati veidi aega.

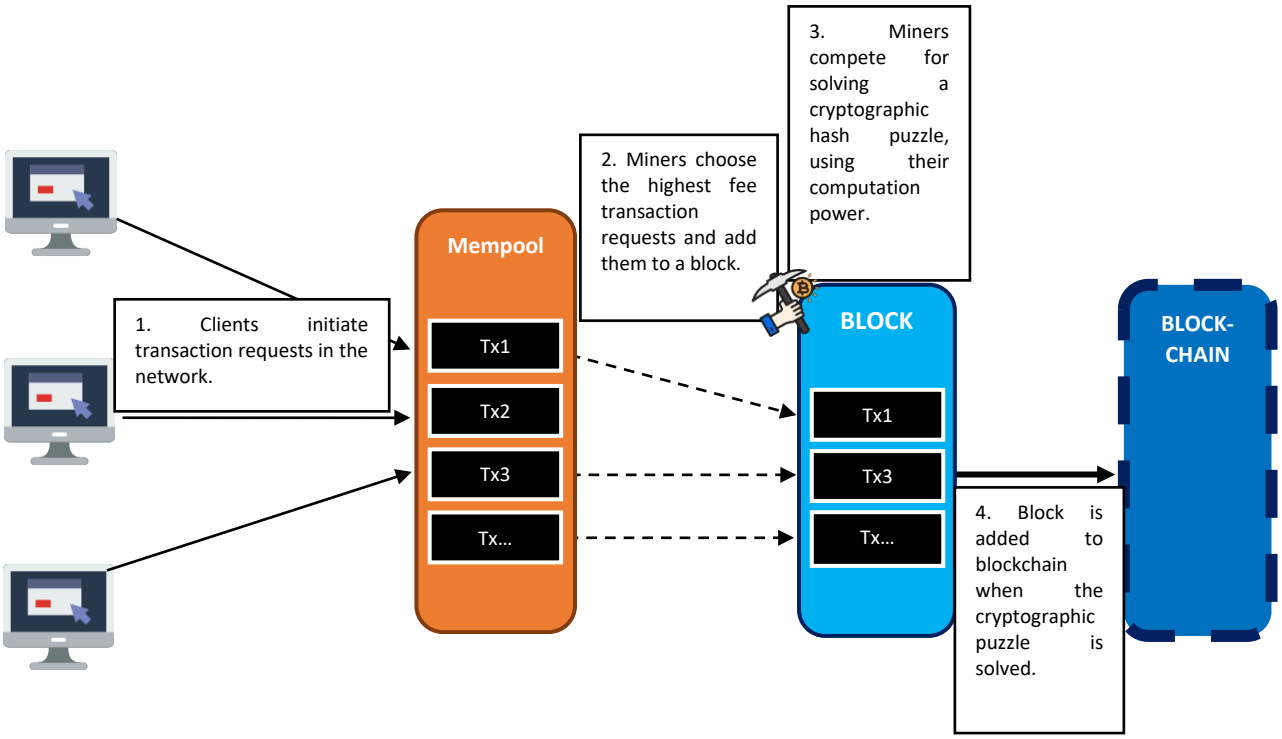


Figure 7:Skemaatiline esitus selle kohta, kuidas tehing plokiahelasse lisatakse. Mempool on koht, kus kinnitamata tehingud sisenevad ja neid hoitakse. Kaevurid valivad mempoolist, milliseid tehinguid nad soovivad plokki lisada. Seejärel proovivad nad lahendada krüptograafilise mõistatuse. Kui need on lahendatud, saavad nad plokipreemia bitcoinides. (Allikas: raamat: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 4. peatükk).

Iga tehing nõuab tehingutasusid. Kaevureid julgustatakse majanduslikult lisama oma plokki kõrgeima tasuga tehinguid, sest nad koguvad need tasud siis, kui nad leiavad esimesena ploki jaoks kehtiva räsi. Lisaks tehingutasudele saavad kaevurid ka plokipreemiat, mis iga 210 000 ploki kohta poole võrra väheneb.

Süsteem on turvaline seni, kuni ausad sõlmed juhivad ühiselt rohkem arvutusvõimsust kui mis tahes koostööd tegev ründajasõlmede rühm.

2.1.8 Detsentraliseerimine

Mõisteid "detsentraliseeritud võrk" ja "hajutatud võrk" kasutatakse sageli vaheldumisi. [3]Detsentraliseerimine näeb ette veel ühe olulise turvafunktsiooni, mis on seotud iga üksiku sõlme hävitamisega, mis majutab andmeid SPOF-ina. Tavalised lahendused, mis ettevõtetel on, on hoida kogu süsteemi/rakenduse jaoks mitu koopiat, mida majutatakse mitmes kohas asuvates andmekeskustes. See on tohutu kulude dubleerimine, mida on vaja andmete turvalisuse tagamiseks, mille Bitcoin saavutab ainult oma loomuliku arhitektuurilise disainiga.

- **Detsentraliseeritud plokiahel nõuab uute andmete kinnitust teistelt sõlmedelt**

Tsentraliseeritud serveriga on suhteliselt lihtne andmebaasi lisada uusi andmesüste. Uued andmed peab lisama vaid üks osapool. See on detsentraliseeritud võrgu puhul erinev. Kui kaevandaja lisab uued andmed plokiahelasse, peavad need andmed siiski kontrollima teised täissõlmed ja seejärel lisama need ka teiste sõlmede hostitud plokiahelatesse.

- **Detsentraliseeritud Blockchain nõuab konsensust**

Kuidas on lood võrguprotokolli uute värskendustega? Detsentraliseeritud plokiahel nõuab konsensust värskenduste ja kokkulepete sõlmimiseks plokiahela õige oleku kohta.

- **Detsentraliseeritud plokiahelat on raske häkkida**

Kuna plokiahelat hoitakse erinevates sõlmedes, mis võivad asuda erinevates maailma paikades, on keeruline võrgu üle kontrolli üle võtta. Võrgu juhtimiseks peate suutma luua pikima ahela, mida saab saavutada ainult suurema arvutusvõimsusega. See võimaldab teil leida kehtivaid plokkide räsi kiiremini kui ülejäänud võrk kokku. Rünnakut, mis põhineb enamuse arvutusvõimsusel, nimetatakse ka ***51% rünnakuks*** . [4]51% rünnak võimaldab teil topelt kulutada.

- **Detsentraliseeritud plokiahel muudab tsensuuri ja pettuse keeruliseks**

Kui Blockchain on piisavalt kaugel ja laialt jaotatud, on see võltsimiskindel. Siiski on võimalik andmeid muuta või kustutada, kui võrgus on üksmeel selle tegemiseks. Kui eeldame, et võrk on hästi detsentraliseeritud, võime öelda, et Blockchaini tsenseerimist on raske teostada.

2.1.9 Privaatsus

Satoshi Nakamoto märkis oma esimesel Bitcoini võrgustiku teatel, et bitcoin on anonüümne, kuid see pole tegelikult tõsi. Bitcoin on pseudonüüm. See tähendab, et see on privaatne, kuid mitte anonüümne. See avaldab kõik avalikus plokiahelas olevad tehingud selgetekstis, et igaüks saaks auditeerida ja käivitada selliseid asju nagu masinõppe algoritmid, et teha sellel jälgimisanalüüsi. See on siiski privaatne, mis tähendab, et kui pole vaja teada (nagu

[3]Kuna Blockchain on erinevate serverite vahel jaotatud andmebaas, nimetatakse seda tehnoloogiat ka ***hajutatud pearaamatu tehnoloogiaks*** (DLT). Blockchaini võib pidada DLT-ks, kuid DLT ei pea alati olema plokiahel.

[4]Kuigi 51% rünnak on tuntuim, on võimalikud ka paljud muud rünnakud. Tsentraliseeritud võrkudes toimuvad regulaarsed rünnakud, nagu põhiarendajate rikkumine, valesti kirjutatud koodi vead või serveritele juurdepääsu võimaldavate võtmete varastamine, esinevad ka plokiahelatega.

kohtumäärus) ja kui kasutaja kasutab seda kavatsusega hoida oma finantstehing privaatsena (ei kasutata oma avalikke aadresse mitu korda), kuna privaatsus on sisseehitatud.

Privaatsust säilitatakse endiselt avalike võtmete ja sellele vastava rahakoti aadressi pseudonüümidena hoidmisega. Avalik pearaamat võimaldab kõigil näha, milline aadress millise tehingu on teinud, kuid seni, kuni teie aadressid on teadmata ega ole seotud teie isikuandmetega, saate tehinguid teha pigem "anonüümselt".

Bitcoini valges raamatus mainis Satoshi ka seda, et privaatsuse säilitamiseks lisatulemüürina tuleks iga tehingu jaoks kasutada uut võtmepaari, et vältida nende sidumist ühise omanikuga. Mõningane linkimine on siiski vältimatu mitme sisendiga tehingute puhul, mis ilmtingimata näitavad, et nende sisendid kuulusid samale omanikule. Risk seisneb selles, et võtme omaniku selgumisel võib linkimine paljastada muid samale omanikule kuulunud tehinguid.

Peamine arvamus, et Bitcoin on anonüümne valuuta, on seega faktiliselt vale. Vastupidi, see toimib läbipaistva avatud pearaamatuna ja see lõi ruumi täiesti uuele krüptovaluutade komplektile, mis keskenduvad anonüümsusele nagu monero, zcash ja mõned teised. Paljud riigid tegelevad tegelikult juba aktiivselt seadusandlusega.

Traditsiooniline pangandusmudel saavutab teatud privaatsuse taseme, piirates teabele juurdepääsu asjaosalistele ja usaldusväärsele kolmandale osapoolele. Kõigist tehingutest avalikult teatamise vajadus välistab selle meetodi, kuid privaatsust saab siiski säilitada, katkestades teabevoo mõnes teises kohas: hoides avalikud võtmed anonüümsena. Avalikkus näeb, et keegi saadab summa kellelegi teisele, kuid ilma tehingut kellegagi seostava teabeta. See sarnaneb börsidel avaldatava info tasemega, kus avalikustatakse üksikute tehingute aeg ja suurus, "lint", kuid ei öelda, kes olid osapooled.

2.1.10 Kokkuvõte

Kuigi plokiahelaid on palju erinevat tüüpi ja erineva detsentraliseerimistasemega, võime järeldada, et üldiselt on detsentraliseeritud plokiahela võrgul järgmised atribuudid:

1. Single Point of Failure (SPOF) pole olemas.
2. Uued andmed peavad kinnitama teised sõlmed.
3. Värskenduste tegemiseks ja Blockchaini õiges olekus kokkuleppimiseks on vaja teatud konsensust.
4. Seda on raske häkkida.
5. See muudab plokiahela andmete tsenseerimise või muutmise keerulisemaks.
6. Tegemist on peer-to-peer võrguga, mis ei eelda usaldust keskerakonna vastu.

Lõppsõna

- Plokiahelad erinevad traditsioonilistest andmebaasidest.
- Põhjus, miks Napster ebaõnnestus, on see, et sellel oli SPOF. Blockchainil seevastu pole SPOF-i ja seetõttu on seda keerulisem välja lülitada.
- Blockchain on peer-to-peer võrk.

Kasutatud ikoonid

Arvuti, mille on teinud Prettycons saidilt www.flaticon.com

Stripi kaevandus saidilt www.flaticon.com

2.2 Blockchain 2.0 ja nutikad lepingud

„Tahame tervet jada ettevõtteid: digitaalne pealkiri, digitaalsed meediavarad, digitaalsed aktsiad ja võlakirjad, digitaalne ühisrahastus, digitaalne kindlustus. Kui teil on Interneti-usaldus, nagu Blockchain pakub, saate leiutada välja põllu järel välja järel. **– Marc Andreessen (2014)**

2.2.1 Sissejuhatus

Õppeeesmärgid

- Mis on Blockchain 1.0 ja miks on Blockchain 2.0 vaja.
- Ethereum on Blockchain 2.0 näide.
- Mis on targad lepingud.
- Mis on detsentraliseeritud rakendused (dApps).
- Mis on detsentraliseeritud autonoomsed organisatsioonid (DAO).

Sissejuhatus

Eelmises peatükis käsitleti peamiselt Blockchaini põhiprintsiipe Bitcoini kaudu. Selles peatükis pöörame tähelepanu uuemale põlvkonnale plokiahelatele, mis on spetsiaalselt ette nähtud suure hulga muud tüüpi detsentraliseeritud rakenduste või dAppide loomiseks. Üks konkreetne Blockchain, millele keskendume, on Ethereum, mis reklaamib end ka kui maailma detsentraliseeritud arvutit.

2.2.2 Blockchain 1.0 ja 2.0

Blockchainide esimene põlvkond on tuntud ka kui ***Blockchain 1.0*** , mis keskendub peamiselt digitaalsele rahale. Vitalik Buterinil tekkis idee töötada välja uus Blockchain Ethereum, millele saaks luua uusi münte, tingimuste ja nõuetega lepinguid ning isegi täisväärtuslikke ***detsentraliseeritud rakendusi*** (dApps). Selliste võimalustega plokiahelaid tuntakse ka kui 2. põlvkonna plokiahelaid: ***Blockchain 2.0*** .[5]

2.2.3 Ethereum

Ethereumi tutvustas esmakordselt Vitalik Buterin raamatus "Ethereum White Paper: a next generation Smart Contract & decentralized Application Platform" (2013). Valges raamatus selgitab Buterin, et Bitcoini võib kirjeldada kui "esimest failisüsteemi", milles tehingute järjekord on üliioluline. Tehniliselt võib Bitcoini pidada lihtsaks olekusiirdesüsteemiks, kus (a) "olek" koosneb kõigi olemasolevate bitcoinide omandiõigusest ja (b) "olekusiirdefunktsioonist ", mis võtab oleku ja tehingu ning väljastab uue oleku. mis on tulemus. Siiski on keeruline täita

[5]Need on plokiahelad, mis on lahendanud hulga probleeme, millega Blockchain 2.0 ikka veel tegeleb. Selliste probleemide näideteks on skaleeritavus, koostalitlusvõime, privaatsus ning jätkusuutlikkus ja valitsemine (Ackermann & Meier, lk 1). EOS, Cosmos, Cardano, Avalanche, Terra on näited plokiahelatest, mida võiks pidada Blockchain 3.0-ks.

tehinguga seotud lepinguid, mis võivad hõlmata mitut riiki. Näiteks on vaevalt võimalik edasi anda loogikat, mis ütleb, et Bob võib oma raha Alice'ile saata, kuid Alice saab seda nõuda alles pärast seda, kui ta on midagi vastu andnud. (Buterin, 2013, lk 12)

Ethereumi eesmärk on pakkuda arendajatele võimalust arendada rakendusi suvaliste tingimuste alusel. Spetsiaalselt Ethereumi jaoks välja töötatud programmeerimiskeelt nimetatakse ***Solidityks*** .

2.2.4 Ethereumi tehingud ja gaas

Ethereumi plokiahela aluseks olev krüptovaluuta on eeter (ETH). Ethereumi võrgus tehingu tegemiseks on vaja ***gaasi*** . Gaasi väljendatakse krüptovaluutas Ether. Ethereumi võrgu gaas on põhimõtteliselt sama, mis tehingukulud. Selle arvutamiseks kasutatakse standardkulusid arvutusvõimsuse ühiku kohta x ühikute arv. Saate määrata iga sooritatud tehingu jaoks konkreetse gaasisumma või tehingukulud. Kasutaja peab tehingu eest tasuma vastava koguse gaasi. Kui gaasi makstakse liiga vähe, ei pruugi kaevandajad tehingut plokki lisada ja seega seda tehingut ei täideta. Lisaks plokipreemiale saab kaevandaja ka kõik gaasitasud, mis ploki tehingutega kaasas olid.

Krüptomajanduslik põhjus, miks gaas on Ethereumi võrku kasutusele võetud, seisneb selles, et see seab olulised tehingud prioriteediks. Plokis on ruumi ainult piiratud arvu tehingute jaoks. Gaasisüsteem tagab, et energiat ei raisata rämpsposti või väheväärtuslike tehingute peale.

2.2.5 Nutikad lepingud

Nutikas leping on detsentraliseeritud automatiseerimine ja seda saab määratleda kui lepingut, mille tingimused on koodis sätestatud. Leping on isetäituv, kuna sooritab tingimuste täitmisel vastavad vastavad toimingud.

Näiteks võib nutikas leping olla tööleping, kus Alice soovib maksta Bobile 500 eurot veebilehe arendamise eest. Leping võiks toimida järgmiselt:

1. Alice paneb lepingusse 500 eurot ja raha pannakse lukku.
2. Kui Bob on veebisaidi välja töötanud, saadab Bob lepingule sõnumi raha vabastamiseks.
3. Fond vabastatakse, kui Alice nõustub.
4. Kui Bob otsustab veebisaiti mitte lõpetada, saab Bob oma töö tühistada, saates lepingule sõnumi, misjärel tagastatakse fond automaatselt Alice'ile.
5. Kui Bob väidab, et on veebisaidi lõpetanud, kuid Alice ei nõustu, võidakse pärast 7-päevast ooteaega kutsuda kohtunik, kes teeb otsuse Alice'i või Bobi kasuks. (Buterin, 2014)

Nutikate lepingute eelised

Nutikad lepingud pakuvad palju eeliseid. Chaintrade (2017) on loetlenud järgmised üksteist:

1. Täpsus: kõik tingimused tuleb üksikasjalikult fikseerida nutikas lepingus. Kui teatud tingimused on välja jäetud, võib see kaasa tuua nutika lepingu soovimatu käitumise.
2. Läbipaistvus: kõik tingimused on täielikult nähtavad ja kättesaadavad kõigile asjaosalistele. Kui leping on sõlmitud, ei saa te seda enam vaidlustada.
3. Selge kommunikatsioon: vajadus täpselt määratletud nutikate lepingute järele tagab, et suhtlus lepingus on selgelt paika pandud, nii et ei tekiks ruumi valesti suhtlemiseks ja valesti tõlgendamiseks.
4. Kiirus: nutikad lepingud võivad traditsioonilisi äriprotsesse automatiseerida ja oluliselt kiirendada. Ühtegi taotlust ei pea esitama kinnitamiseks ning dokumente ei pea töötlema ega kinnitama üksikisikud.
5. Turvalisus: nutikad lepingud töötavad Blockchaini platvormidel ja kasutavad andmete krüptimist.
6. Tõhusus: tänu täpsusele ja kiirusele teostavad nutikad lepingud äriprotsesse tõhusamalt või isegi kõrvaldavad need täielikult.
7. Paberivaba: nutikate lepingute täitmiseks ei ole vaja paberimajandust.
8. Salvestus ja varundamine: nutikad lepingud ja nende andmed salvestatakse püsivalt Blockchaini. Seetõttu ei saa neid kaduma minna ja neid on lihtne leida.
9. Kulude kokkuhoid: nutikad lepingud võivad säästa palju kulusid, kuna lepingute tõlgendamiseks ja jõustamiseks on vähem vaja vahendajaid, nagu juristid, tunnistajad ja pangad.
10. . Usaldus: asjaosalised võivad usaldada, et nutikaid lepinguid – kui need on õigesti koostatud – täidetakse õiglaselt, ilma andmetega manipuleerimise ja eelarvamusteta.
11. **11. Garanteeritud tulemused: isetäitvaid lepinguid kasutades järgivad osapooled nutika**

2.2.6 Detsentraliseeritud rakendused

Detsentraliseeritud rakenduse (dApp) määratleme kui rakendust, mis kasutab plokiahela detsentraliseeritud andmesalvestust. Rakendust ei käivitata keskserveri, vaid sõlmede detsentraliseeritud võrgu kaudu. Nii nagu tavalisel rakendusel, on sellel sageli esiots ja kasutajaliides. Liides pakub kasutajale lihtsamat suhtlemist nutikate lepingute ja plokiahelaga. Kui salvestate ja täitke dApp-i põhikoodi moodustavad nutikad lepingud detsentraliseeritult, pole ühtegi tõrkepunkti. Rakenduse tööd ja rakenduse andmeid ei saa lihtsalt tsenseerida ega eemaldada.

2.2.7 Detsentraliseeritud autonoomne organisatsioon (DAO)

Detsentraliseeritud autonoomseid organisatsioone (DAO-sid) võib määratleda kui mittehierarhilist organisatsiooni, mis täidab ja registreerib rutiinseid ülesandeid plokiahelas. Reeglid, millest DAO järgib, salvestatakse ka plokiahelasse. Lisaks sõltub DAO sisemiste sidusrühmade vabatahtlikest panustest, et juhtida organisatsiooni läbi demokraatliku konsultatsiooniprotsessi. (Hsieh jt, 2018, lk 2)

DAO eristab tsentraliseeritud organisatsioonist põhimõtteliselt see, et sellel ei ole tippjuhtkonda ega tegevjuhti. Sellel pole ka filiaale, töötajaid ega tütarettevõtteid. Selle asemel eksisteerib DAO detsentraliseeritud kasutajate ja sõlmede võrgus, mis koguvad, kontrollivad ja värskendavad plokiahelas tehinguid. Otsused koodeksi muutmise kohta tehakse demokraatliku hääletusprotsessi teel. See on kardinaalselt erinev viis äriorganisatsiooni loomiseks. Oma autonoomse olemuse tõttu – on ju tegemist isemajandava ja iseorganiseeruva süsteemiga – võib Bitcoini iseloomustada kui DAO-d, sest ta (a) juhib maksesüsteemi, (b) kasutab alltöövõtjaid, kes töötavad kaevuritena ja (c) maksab neile alltöövõtjatele äsja levitatud bitcoinidega (Vigna & Casey, 2015, lk 229). Lisaks saavad kaevurid oma arvutusvõimsuse abil hääletada protokolli täiustamise ettepanekute poolt. DAO-sid kontrollib sidusrühmade kollektiivne otsustusprotsess detsentraliseeritud protokolli kaudu ja neid ei mõjuta keskne juhtorgan.

Lõppsõna

- Blockchain 2.0 abil saab luua hulgaliselt uut tüüpi rakendusi.
- Ethereumis saate arendada nutikaid lepinguid, kus tingimused on nii selgelt paika pandud, et lepingu rikkumise korral ei ole enam vaja kolmandate osapoolte tõlget.
- Bitcoin on esimene failisüsteem.
- Bitcoin on esimene detsentraliseeritud autonoomne organisatsioon (DAO).

3 Plokiahela tüübid

Selles peatükis jagame Blockchaini selle tüüpideks kolmest vaatenurgast, konsensusprotokollist, juhtimisest ja Blockchaini süsteemide koostöö tüüpidest.

3.1 Plokiahela tüübid vastavalt konsensusprotokollile

Konsensusprotokollid on hajutatud võrgus erinevate osalejate vahelise usalduse tagamiseks hädavajalikud. Peab olema kindel, et osalejad ei ole rikutud ja nende vahel jagatud andmed ei ole rikutud. Selle usalduse tagamiseks peavad osalevad sõlmed kontrollima sõnumite või tehingute õigsust ja neutraliseerima teised osalejad, kes on rikutud ja eksitavad: lahendus Bütsantsi kindralite probleemile, mida käsitleti eelmises peatükis.

Kuna konsensusprotokoll puudutab seega Blockchaini süsteemi olemust, kasutatakse seda siin ühe võimalusena plokiahela tüüpide eristamiseks.
Eelmises peatükis tutvustati esimest konsensusprotokolli **Proof-of-Work** , kasutades näitena Bitcoini. Selle protokolli kohaselt võib andmeploki plokiahelasse lisada ainult siis, kui ploki kehtiv räsi on leitud. Kuna Bitcoini kaevurid astusid arvutusvõimsuse alal karmi konkurentsi, et saada esmalt kehtiva räsi leidmise eest tasu, on Bitcoini võrgu elektritarbimine tekitanud muret Blockchaini negatiivsete mõjude pärast keskkonnale. Sellest tulenev Bütsantsi kindralite probleemile jätkusuutlikumate lahenduste otsimine on viinud alternatiivsete konsensusprotokollideni.
Üks peamisi alternatiive Proof-of-Workile on Proof-of-Stake, mida on nüüdseks rakendatud erinevates Blockchaini projektides koos märkimisväärse näitega Ethereum, mis läheb 2022. aastal üle Proof-of-Stake'i.

Kui Proof-of-Worki kaevuritel on lubatud toota uusi plokke, kui nad leiavad kehtiva räsi, siis Proof-of-stake'i plokitootja valitakse (a) juhusliku valiku protsessi ja (b) **panuse alusel.** nagu tal on müntide arv. Selle tulemusena ei vaja te osalemiseks arvutusvõimsust. Vaja on vaid tavalist arvutit, internetiühendust ja mündi olemasolu. Proof-of-Stake'i plokkide tootjat ei nimetata seetõttu kaevandajaks, vaid ***võltsijaks*** . Kuna **võltsija** saab uue ploki valmistamisel ka tasu, võite võltsimisel näha ka panuse tõendamist kui meetodit, mille abil teenite oma müntidelt passiivset tulu. Mida suurem on teie panus, seda suurem on võimalus, et saate järgmise ploki toota. Lisaks plokkide tootmisele valideerivad võltsijad ka tehinguid, aidates sellega võrku turvata.

Lisaks energiatõhususele on Proof-of-Stake of Proof-of-Work eelisteks see, et panustamise lihtsus võimaldab Blockchaini paremini jaotada ja 51% rünnaku läbiviimine on vähem ahvatlev.

Proof-of-Stake'is on erinevaid variante, millel on oma ainulaadsed omadused. Esiteks saavad kõik, kellel on münt, hääletada tunnistajate ja delegaatide poolt **.** Tunnistajad kinnitavad tehinguid ja toodavad uusi plokke, mille eest nad saavad tasu. Delegaadid jälgivad Blockchaini protokolli juhtimisstruktuuri. Selle tulemusel saab delegeeritud Proof-of-take hakkama rohkemate tehingutega sekundis kui plokiahelad, mis on detsentraliseeritumad.
Teiseks, **liisitud Proof-of-stake'is** saavad kõik oma münte mängusõlmpunktides rentida, suurendades seeläbi panusesõlmede võimalust plokki toota. Panusesõlmed jagavad oma tasu proportsionaalselt enda ja rentnike vahel. Selle tulemusena julgustab see protokoll inimesi panustamise protsessis osalema.

Kolmandaks premeeritakse **Proof-of-stake Velocity kasutajaid (a) nende käes olevate müntide arvu ja (b) selle eest, kui aktiivselt nad oma münte kasutavad.** Seetõttu julgustatakse kogukonda mitte ainult münte alles hoidma, vaid neid ka tehinguteks kasutama.

Neljandaks, **volituse tõendamise abil** autenditakse ja kinnitatakse plokitootjad (volitussõlmed) nende identiteedi ja maine alusel. Seoses maine identiteediga stimuleerivad autoriteedisõlmed näitama head käitumist ja mitte kaasama plokiahelasse pahatahtlikke tehinguid. Kui nad seda teevad, kahjustab see mainet. Proof-of-Authority on näide Proof-of-stake variandi loomisest, kus uue ploki loomise võimalus ei sõltu täielikult panustatud müntide arvust.
Pidage meeles, et on kaheldav, kas volituse tõendamine kuulub mängu tõestamise alla. Mõnikord peetakse seda osaluse delegeeritud tõendi vormiks ja seda kasutatakse sagedamini suletud, lubatud plokiahelates.

Üks konsensusprotokollide abil Blockchaini tüpiseerimise eelis on see, et see aitab selgitada **plokiahelate skaleeritavuse erinevusi** . Üldiselt sõltub see skaleeritavusest konsensusprotokollide mõjust plokiajale, ploki suurusele, plokiahela jaotuse või detsentraliseerimise tasemele ning viisile, kuidas plokke toodetakse, tehinguid plokiahelasse saadetakse ja tehinguid kontrollitakse. Selle skaleerimise parandamiseks testitakse erinevaid lahendusi, näiteks tehingute eemaldamist ahelast. Tuntud näited selle kohta on välkvõrk, plasma (mõlemad nn 'Layer 2' lahendused) ja sharding.

3.2 Plokiahela juhtimine ja kes saavad millises rollis osaleda

Plokiahelat, nagu iga partnerlust, tuleb hallata ja kontrollida. Saadud Blockchaini juhtimisstruktuur pakub teist võimalust Blockchaini tüüpide tuvastamiseks, mida siin arutatakse.

Märkimisväärsed juhtimiselemendid on :

1. **Õigus** esitada, ellu viia ja jälgida otsuseettepanekuid **grupi** või kõigi poolt.
2. **Vastutus** ja õigus jälgida otsuseid ja käitumist ning olla vastutav oma kohustuste eest.
3. **Stiimulid** ja osalejate julgustamine Blockchaini säilitama.

See, kuidas neid elemente tõlgendatakse, sõltub partnerluse eesmärkidest ja seega ka vajalikust valitsemisviisist.

Üks juhtimisvajadusi võib olla see, et keskne inimeste rühm teostab kontrolli ja dikteerib tingimusi (**keskse** kontrolli mõtteviis **)** , võrreldes suurema grupi vajadusega teha koostööd võrdsetel alustel ilma hierarhia või keskse kontrollita (**detsentraliseeritud** kontrolli mõtteviis).

Kasutatava kontrolli tüüpi kasutatakse otsustamaks, kellele antakse luba plokiahelas osalemiseks või mitte. Kui keskasutused annavad juurdepääsu, on Blockchain **privaatne** plokiahela tüüp. Kui juurdepääs on korraldatud kõigile, nimetatakse plokiahelat **avalikuks** plokiahelaks. Avalik ja privaatne plokiahela tüüp on ühendatud **konsortsiumi** plokiahela tüüp, vahepealne vorm, mis on tsentraliseeritud kui avalik plokiahel ja detsentraliseeritum kui privaatne plokiahel.

Konsortsiumis töötavad mitmed organisatsioonid plokiahela seadistamiseks koos ja konsensust juhivad sõlmede valik. Konsortsium otsustab kogu võrgustiku jaoks, kes millise

rolliga saab osaleda, millised tehingud on avalikult nähtavad või teiste osalejate eest kaitstud ja kuidas peaks juhtimine olema üles ehitatud.

Peamiselt kasutate **avalikku Blockchaini** , kus kõiki koheldakse võrdselt, kui soovite, et grupp sarnaselt mõtlevaid inimesi koos töötaks. Koostöö on siin tagatud konsensuse mehhanismiga, mis toimib „usaldusmasinana". „Juurdepääs kõigile" toob kaasa suurema arvu sõlmede arvu, mis suurendavad usaldust Blockchaini süsteemi vastu. Avalik plokiahel näitab vähem usaldust asutuste vastu, kes juhivad plokiahelat teiste nimel. Selline suhtumine usaldusesse ja usaldusse soosib otsust detsentraliseerituma olemusega konsensusprotokollide kasuks, usaldust selle plokiahela avatud lähtekoodiga olemuse vastu ning otsuste tegemise täieliku läbipaistvuse soovi. Selline suhtumine suurendab seega kindlustunnet võõraste liitumise ja partnerluses osalemise suhtes. Usaldus peitub ju süsteemis, mitte kasutajas.

Üldiselt soovib ettevõte, mis kaldub **privaatse Blockchaini poole** , teada, kes on Blockchaini süsteemis. Mõelge sisevõrgule, kus kontrollite sõlme, andmeid ja lähtekoodi. Teate kõiki ja kõiki tehinguid saab vajadusel vaadata, kuid kaitsete inimesi ka teatud tehingute kontrollimise või nägemise eest. See on kasulik, kui andmed on ettevõttetundlikud. Avalikus süsteemis on see võimalik ka tehniliselt sisse ehitada, kuid praktikas osutub see esialgu väljakutseks.

Seetõttu on privaatses Blockchainis oluline olla teadlik kõigist rollidest, mille määrate osalejatele, kellele andsite juurdepääsu. Üks oluline roll on võimalus **säilitada konsensusmehhanism** . Kas see võimalus tuleks anda kõigile Blockchainis osalejatele või ainult valitud rühmale?

Vastus sellele küsimusele viib **loata** ja **lubatud** plokiahela tüüpide juurde.

Kui igal plokiahelasse sisenejal on lubatud konsensusmehhanismi säilitada, puudutab see **lubadeta** Blockchaini tüüpi. Kui konsensusmehhanismi säilitamise roll on reserveeritud valitud rühmale, räägime **lubatud** plokiahela tüübist.

Konsensuse säilitamise kõrval on rollid, mis võimaldavad teil plokiahelas tehinguid teostada, vaadata ja kohandada, plokiahelat tehniliselt hooldada või ideede üle hääletamisel osaleda. Need rollid ei ole loata või lubadega süsteemi vahel valiku tegemisel asjakohased. Need rollid on aga partnerluse olemuse seisukohast olulised. See on asjakohane, sest kui ametiasutused ei hooli sellest, kes süsteemile ligi pääseb, ja usaldavad süsteemi ennast, kalduvad nad suurema tõenäosusega tagama osalejatele anonüümsuse. Praegusel ajal klasside haldamise juhtimissüsteeme kasutavad ettevõtted eelistaksid siiski teada inimesi, kellele nad juurdepääsu annavad, samuti teada, millised rollid on seal ja millisele osalejale nad saavad rolli anda.

Rollide eraldamisega saavad need ettevõtted kasutada oma organisatsioonilist struktuuri. Seega saavad nad oma ettevõtte identiteeti oma plokiahelas jõustada, kuna nad kontrollivad nii isikute profiili kui ka nende rolle. Lisaks osalisele usalduse ülekandmisele süsteemile saavad nad jätkata oma organisatsiooni juhtimist, oma juhtimiskontrollisüsteemi nagu spetsiifiline personalijuhtimine.

See aitab selgitada, miks lubadeta süsteemis tehakse koostöö soodustamiseks kättesaadavaks krüptomärgid.

Tänapäeva plokiahelates kasutatakse kombineeritult erinevaid plokiahela tüüpe:

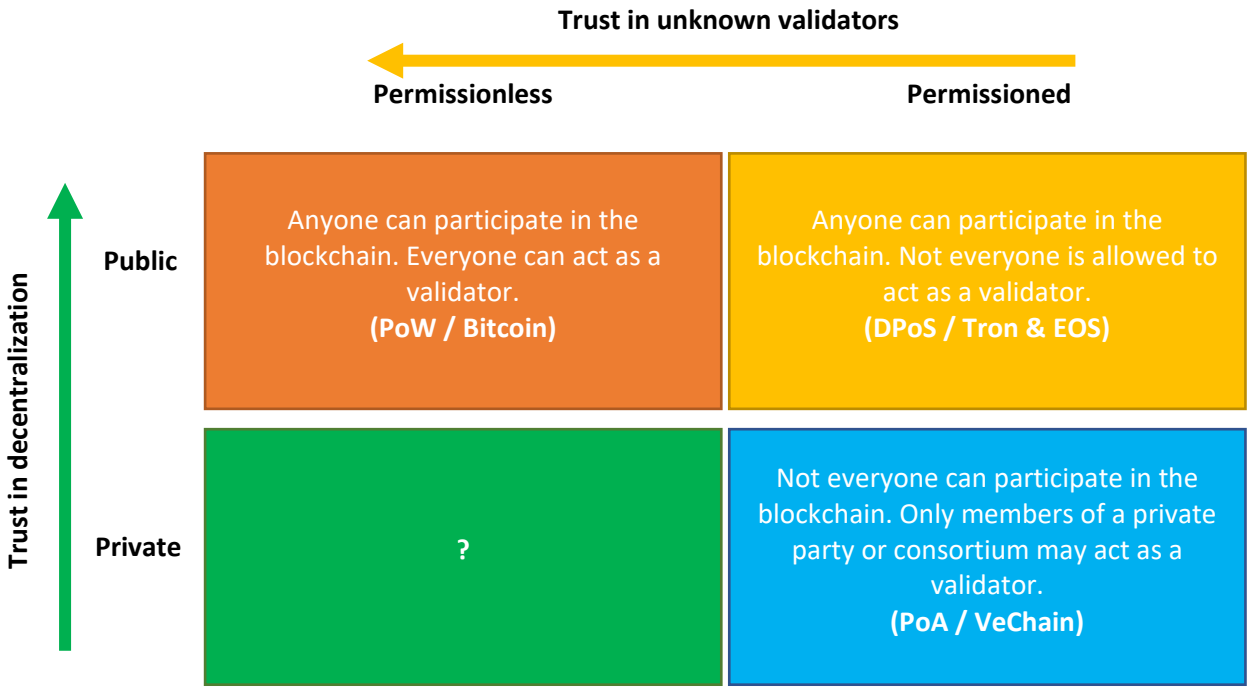


Figure 8: Ülevaade erinevatest plokiahela tüüpidest, väljendatuna loata, lubadega, privaatses ja avalikus (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 9. peatükk).

Kui usaldatakse avalike plokiahelatega süsteemi, peetakse vähem tähtsaks küsimust "kes kirjutab andmeid plokiahelasse", "kes loeb plokiahelast andmeid" ja "kellel on lubatud plokiahelat hooldada". See omakorda viib selleni, et enamik avalikke plokiahelaid on loata. Võrguga liitumise madala barjääri tõttu on sellised plokiahelad kõige detsentraliseeritumad.

Osalejad määravad Blockchaini toimimise vastavalt grupi motiividele nagu avatus, neutraalsus ja vabadus. Avalikus Blockchainis saavad kõik osaleda ka kõigi valitsemisküsimuste otsuste tegemisel.

Avalik **Blockchain** ei ole ettevõtetele alati soovitav, eriti reguleeritumas keskkonnas, kus muu hulgas eeldatakse, et nad teavad kõigi osapoolte identiteeti, kes Blockchaini andmeid kirjutavad.

See keskerakond on sageli loonud mitmeid sõlme, mis ise haldavad ja hoiavad Blockchaini koos töötamas. Kõige äärmuslikumal juhul on parteil üks sõlm, millel Blockchain töötab. See ei paku aga eeliseid tsentraliseeritud võrgu ees, mis on ühtlasi SPOF.

Erinevat tüüpi Blockchainide vahelised valikud mõjutavad organisatsiooni kontrolli. Mida rohkem usaldatakse Blockchaini detsentraliseeritud olemust, seda lihtsam on osaleda. Mida suurem on kindlustunne, et valideerijad võivad konsensuse loomisel osaleda tundmatutena, seda läbipaistvam on süsteem. Lõppude lõpuks saavad kõik seejärel käivitada täieliku sõlme ja aidata kõiki andmeid valideerida. Detsentraliseeritud olemuse tõttu on sellistel süsteemidel sageli palju validaatoreid ja osaliselt seetõttu on neil endiselt probleeme skaleeritavusega. Samuti on sellised plokiahelad suhteliselt kallimad kui vähem detsentraliseeritud ja lubatud variandid.

Pikemas perspektiivis peaks aga lubadeta avalik plokiahel muutuma üha tõhusamaks, nii et professionaalsemad osapooled valivad sellised plokiahelad. Need plokiahelad tuleb seejärel korraldada nii, et rollid, mida osalejad saavad ärirakenduste jaoks võtta, oleksid täpselt määratletud ja vastaksid ärinõuetele. Näiteks saavad loata avalikke plokiahelaid kasutavad ettevõtted andmeid nullteadmiste tõendite abil anonüümseks muuta ja rakenduse tasemel osalejatel võib paluda oma identiteeti näidata.

3.3 Platvormid ja konsortsiumid

Plokiahelat, kus erinevad ettevõtted ja kolmandad osapooled teevad koostööd ilma seda plokiahelat kontrolliva keskse kasutajata, nimetatakse ettevõtte plokiahelaks. Sellise Enterprise Blockchaini ehitamiseks kasutavad ettevõtted Blockchaini platvorme. Need **platvormid** võimaldavad teil kirjutada rakendusi teatud tehnoloogiate abil. Nende platvormide ümber on korraldatud mitmesuguseid partnerlusi. Platvormid on kolmas ja viimane viis, kuidas me siin eri tüüpi plokiahelaid vaatleme.

Plokiahela **platvormid** võimaldavad teie rakendusel teha koostööd teiste rakendustega, näiteks omas või jagatud programmeerimiskeeles, dokumente salvestatakse või jagatakse ning saadakse juurdepääs kindlale võrgule. Kaks silmapaistvamat platvormi on praegu Ethereum ja Hyperledger, kusjuures Corda on enim silmapaistvam.

Igal platvormil on oma ainulaadsed funktsioonid. Ethereum on üldiselt avalik plokiahel, Hyperledger pakub plug-and-play-mooduleid, mis kasutavad erinevaid tehnoloogiaid, ja Corda on detsentraliseeritud pearaamatutehnoloogia, mis on spetsialiseerunud rohkem finantsteenustele. Liikmed, kes on liitunud ühe platvormi partnerlusega, on sageli ka teiste platvormide partnerluste liikmed. Platvormid ise on avatud lähtekoodiga. Ethereum ja Hyperledger on viimastel aastatel püüdnud nende kahe vahel suurema integratsiooni poole, eesmärgiga rakendada Blockchaini süsteeme kõikjal ettevõtetes.

Kui partnerlussuhted on seotud plokiahelate koostöövormiga, milles uued tulijad on teada ja neile on määratud kindlad rollid, töötavad nad struktuurides, mida segadusttekitavalt nimetatakse ka konsortsiumideks (vt eespool lõik 3.2), kuid teisest vaatenurgast segades avaliku ja erasektori plokiahelate omadusi. ainult. Koostööd tegevad osapooled võivad olla erinevad valitsusasutustest, huvirühmadest ja tundmatutest kuni tarnijate, klientide ja otseste konkurentideni.

Lisaks aitavad siinsed konsortsiumid osapooltel ületada neli peamist väljakutset, millega organisatsioonid Blockchaini juurutamisel kokku puutuvad. Esiteks jagavad konsortsiumid teadmisi riiklike järelevalveasutuste kohta ja hoiavad nendega aktiivset kontakti. Seejärel aitavad konsortsiumid muu hulgas seadusi ja määrusi selgitada.

Teiseks aitavad konsortsiumid organisatsioonidel riske erinevate osapoolte vahel hajutada, jagades ressursse Blockchaini süsteemide arendamiseks.

Kolmandaks annavad konsortsiumid koostöö kaudu kriitilise massi stabiilse toimimissüsteemi vastuvõtmiseks.

Ja neljandaks annavad konsortsiumid võimaluse luua uusi detsentraliseeritud partnerlussuhteid usaldusväärsete ja ebausaldusväärsete osapooltega, ilma et osalevad organisatsioonid kaotaksid liiga palju oma autonoomiat. See pakub konkurentidele näiteks standardprotseduure andmete loomiseks ja vahetamiseks või üksteise klientide ja tarnijatega

koostöö tegemiseks. Kuna aga osalevad osapooled peavad koos töötamiseks üksteist usaldama, tagavad nad oma usalduse tavaliselt ühiste ressursside, otsuste tegemise, sanktsioonide, tundliku teabe ja vastastikuse andmete jagamise lepingutega. Need lepingud suurendavad nii konsortsiumiga liitumise kui ka konsortsiumist lahkumise takistust. Tõenäoliselt eksisteerivad koos erinevad konsortsiumid. Konsortsiumisisesel ja -vahelisel koostalitlusvõimel on selles oluline roll.

4 Krüptovaluutad ja märgid

Satoshi Nakamoto üks suurepäraseid leiutisi on juba olemasolevate tehnoloogiate kombinatsioon tasustamissüsteemiga, mis hoiab detsentraliseeritud võrgu töös. Nagu varem mainitud, makstakse tasu Bitcoinides kaevandajale, kes toodab ploki.

Tokeneid tuntakse meie praeguses ühiskonnas vautšerite ja müntidena – näiteks lojaalsuspunktid, kasiinomündid ja kinkekaardid. Teame ka IT-s tokeneid, mis annavad võrgule juurdepääsuõigusi ülesande täitmiseks või alusvara õiguste esitlustena. Bitcoin, mida võiks näha ka krüptograafilise märgina, erineb eelnimetatud žetoonidest selle poolest, et see esindab väärtust. Krüptograafilisi märke saab kasutada mitmel põhjusel. Blockchaini maastikul teenindavad need peamiselt väärtuste **Internetti,** kus väärtusi saab usaldusväärsel viisil vahetada detsentraliseeritud Interneti kaudu.

Krüptograafiliste žetoonidega, nagu Bitcoin, saate maksta või säästa, kuid võite ka sammu edasi liikuda. Näiteks Bitcoini saab teenida uute plokkide tootmiseks arvuti toiteallikaga. Seega loob see majanduse, kus mitut osalejat julgustatakse aitama võrku turvata krüpto eest. Krüptomärkide kasutamine osalejate teatud käitumise stimuleerimiseks ja vale käitumise eest karistamiseks konsensusprotokolli kaudu on osa **krüptoökonoomikast** .

Selles peatükis kirjeldatakse 4.1-s esmalt **krüptoökonoomikat** kui aluskontseptsiooni, milles žetoonid on osutunud kasulikuks rolliks. Seejärel 4.2. kirjeldab **, mis on märgid** , ja **liigitab** need. See klassifikatsioon hõlmab dApp-märke ja krüptovaluutat, aga ka erinevust vahetatavate ja mittevahetatavate tokenite vahel ning seda, kuidas need krüptomajandust toetavad. Peatükki jätkatakse jaotises 4.3, kus antakse ülevaade sellest, kuidas žetoone saab kasutada raha kogumiseks esmase mündipakkumise, turvamärgi pakkumise ja esmase vahetuspakkumise kaudu.

4.1 Krüptomajandus

Krüptograafilised märgid teenivad erinevaid eesmärke, nagu juurdepääs süsteemile või teabe esitamine füüsiliselt objektilt. See annab žetoonidele **väärtuse** , mida saab plokiahelas erinevate osapoolte vahel vahetada. Seda uut distsipliini, mis uurib rikkuse ülekandmist arvutivõrkude, krüptograafia, mänguteooria ja tarkvaraarenduse kaudu koos rikkuse loomise ja tarbimisega, nimetatakse **krüptoökonoomikaks.**

Figure 9:Krüptoökonoomika multidistsiplinaarsed aspektid. (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 10. peatükk).

Arvutivõrgud on kujundatud teatud reeglitega, mis toimivad omamoodi seadusena kõigile, kes osalevad. Need seadused on aga välja töötanud erapooled/kogukonnad ja osaliselt jõustavad neid pigem tarkvara kui valitsused. Nende seaduste raames tehakse eeldused selle kohta, kuidas osalejad võivad võrgus käituda ja valesti käituda.

Blockchaini krüptoökonoomika keskne idee seisneb selles, et töötatakse välja protokollid, mis julgustavad inimesi võrgus osalema nii, et võrgu väärtus oleks **osalejate jaoks maksimaalne** . Võrguväärtust saab maksimeerida vaid siis, kui võrk ja seal toimuvad tehingud on samuti **kaitstud** . Selle saavutamiseks kasutatakse **krüptograafiat** võrgus tehtavate tehingute turvamiseks **tarkvara** , näiteks räsifunktsioonide ja digitaalallkirjade kaudu. Lisaks makstakse preemiaid osalejatele, kes aitavad võrgu turvalisust nt kaevandamise või panustamise kaudu. Selle mõtteviisi kombinatsiooni ilmestab näiteks Bitcoini roll märgina, mis stimuleerib inimesi koostööd tegema ja aitab seega säilitada iseorganiseeruvat krüptomajandussüsteemi. Krüptomajandus on oluline eeldus toetamaks ideed jätkusuutlikust ja soovitavalt iseorganiseeruvast süsteemist, ilma et keskerakonnad inimesi teatud viisil tegutsema ärgitaksid. Selle eelduse jaoks on oluline **mänguteooria ,** uuring selle kohta, kuidas luua konkurentsikeskkonnas optimaalsed tingimused, et osalejad valiksid alati oma valikutes hea käitumise, kuna see toob rohkem kasumit kui halb käitumine. Üks viis osalejate heale käitumisele julgustamiseks on krüptomärgi preemiad.

4.2 Blockchaini žetoonide klassifikatsioon

Internet loodi algselt selleks, et omavahel teavet vahetada. Seda tuntakse ka **teabe Internetina** . Selle sees on keeruline väärtust salvestada ja teisaldada ilma usaldusväärse

vahendajata (Tapscott, 2016), kes peamiselt kontrollib, kas väärtust, näiteks eurot, ei kulutata kaks korda (Satoshi, 2008, lk 2). Blockchaini tulekuga saate vahendajate vajadusest mööda minna ja peer-to-peer väärtust otse kaubelda. Seda tuntakse ka kui **väärtuste Internetti** . Krüptomärgid mängivad selle krüptomajandussüsteemi toetamisel keskset rolli. Krüptomärgi saab luua plokiahelas ja see kujutab endast ka kaubeldavat vara. Mõnikord luuakse ICO-s või STO-s märgid projekti rahastamiseks. Tokenite loomise protsessi nimetatakse **tokeniseerimiseks** . Nende žetoonidega kauplemine võimaldab teil alusvara omandiõiguse üle anda.

Krüptomärkide vaatamisel on erinevaid vaatenurki. Järgmises vormingus on kapseldatud kõik erinevad märgid, mille lisaeelis on käsitleda märkide tulevast rolli väärtuste Internetis:

Rakendus	Märk rakenduse kasuks	Token varana
Vahetatavad märgid	Võrk: eeter dApp: august	Vara: kuld Turvalisus: osa Shell Krüptovaluuta : Bitcoin
Mittevahetatavad märgid		Vara: sünnitunnistus Tagatis: eralaen

Figure 10: Kahekordne žetoonide vorming. Ühelt poolt selleks, et eristada tokeneid, mida kasutatakse Blockchaini võrgus hooldamiseks ja omandiõiguse demonstreerimiseks ja üleandmiseks. Teisest küljest, et eristada vahetatavaid ja mittevahetatavaid märke. (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021, 10. peatükk).

Pidage meeles, et žetoonidel võib olla kahe märgi struktuur, kus neil on korraga mitu eesmärki. Näiteks Bitcoini kasutatakse võrgu või rakenduse märgina ja varana.

Rakenduse hüvesid kasutatakse kõige elementaarsemal tasemel, et julgustada inimesi Blockchaini rakenduses osalema ja seda võrku töös hoidma. See võrk võib olla platvorm, millel töötavad detsentraliseeritud rakendused, dApps. Siin kasutatakse **võrgumärke , et premeerida** osalejaid võrgu säilitamiseks tehtud töö eest. Need märgid hõivavad plokiahelas keskse koha, kuna organisatsioonilise ideena toetavad nad hajutatud usaldusväärset võrku ja kujundavad seega Blockchaini krüpto-majanduslikku süsteemi. Lisaks rakendusele võib võrk olla ka **platvorm** , millel rakendused töötavad nagu Ethereum või Cardano oma ETH- ja ADA-märkidega, et saavutada konsensus ja premeerida tehingusüsteemi . Mõeldes sammu edasi, näete, et plokiahelas on valida, kas kasutada žetoone või ignoreerida žetoonide kasutamist koos.

dApp märgid või **utiliidi märgid** , on kasulikud ainult nende enda rakenduses ja neid kasutatakse sellele utiliidile juurdepääsuks. Väljaspool seda rakendust pole neist kasu. Saate nendega kaubelda ka väljaspool rakendust. Siiski ei ole need alati programmeeritud valuutaks

või võrgus jagamiseks. Näiteks Siacoin (SC), kus inimesed saavad teenida SC-d, kui nad teevad oma vaba kettaruumi teistele võrgus osalejatele kättesaadavaks.

Ethereumi dApp-märgid tehakse vastavalt protokollile **Ethereum Request For Comments 20** (ERC-20). Protokoll määratleb teatud reeglid ja standardid, mis on seotud žetoonide väljastamisega Ethereumi võrgus. Kõik ERC-20 järgi valmistatud dApp-märgid on oma rakenduse jaoks ainulaadsed ja nendega saab kaubelda Ethereumi võrgus.

Rakenduste huvides kasutatavad märgid erinevad žetoonidest, mis tiirlevad väärtuste hõivamise ja vahetamise ümber plokiahela rakendustes, millega nad näitavad selle väärtuse omamist ja võimaldavad sellele väärtusele õiguse üle anda, **žetoonid kui vara** . Selle saab jaotada varamärkideks, turvamärkideks ja krüptovaluutadeks.

Varamärgid esindavad alusvara, nagu kuld või nafta, aga ka maja, kirjaklambri või krüptokogumisobjektide, nagu mänguavatarid või digitaalsed kunstiteosed, õiguste ja kohustuste kirjeid. Need märgid võivad esindada tühiseid kuni väga suuri alusväärtusi. Varažetoonide oluline tingimus on omaniku isiku tuvastamine. Varade krüptomärgid võivad olla kasulikud tänu võimalusele neid programmeerida (**nutikad märgid**) ja nendega kaubelda madala hõõrdumise ja kõrge turvalisusega:

1. Saate hõlpsasti jagada varasid ja teha need väikestes ühikutes kättesaadavaks. Selle **fraktsioneerimise näide** on Mona Lisa omandiõiguse esindamine 1000 müügi-/rendimärgis.
2. Saate programmeerida krüptograafilise loa õigusi ja jõustada neid nutikate lepingute kaudu. Näiteks määrake oma Mona Lisa žetoon müüma ainult mittetulundusühingutele või määrake, et edasimüük sisaldab automaatselt 2% vahendustasu algsele müüjale.
3. Vähendate ostu-müügi hõõrdumist, osaliselt tänu kiiretele ja odavatele mikrotehingutele. Näiteks nutikülmik skaneerib teatud ajavahemike järel kõige odavamat elektrit.
4. Saate märgisse salvestada kogu asjakohase teabe alusvara kohta. Näiteks kontrollige oma kasutatud masina eelmisi omanikke, parandades sellega jagamismajandust.
5. Saate hõlpsasti ise luua vara, näiteks kodukontserdi sissepääsupileti.

Lühidalt öeldes edastavad nutikad märgid lihtsalt väärtust, teavet, ideid, õigusi ja kohustusi nutikate lepingute kaudu.

Väärtpaberimärgid tähistavad võlakirju, aktsiaid, laene, futuure, optsioone ja muid kaubeldavaid finantsvarasid. Kuigi need kuuluvad varamärkide hulka, mainitakse neid eraldi. Turvamärkidele saab anda igasuguseid õigusi. Näiteks õigus väärtpaberit mitte kõigile edasi müüa või oma hääleõigust ettevõtte suuna kohta ajutiselt kellelegi laenata.

K üptovaluuta märgid kuuluvad samuti varamärkide hulka ja neid käsitletakse eraldi, arvestades nende suurt eeldatavat finantsmajanduslikku mõju. Bitcoin on krüptovaluuta tuntuim näide. Sel juhul on žetoon mõeldud rahana toimima. Aeglaselt, kuid kindlalt **stabiilsed mündid** pälvivad tähelepanu, kuna need näitavad võimalikke viise krüptožetoonide väärtuse stabiliseerimiseks ja võivad seetõttu muu hulgas olla fiat-valuutade detsentraliseeritud alternatiivid või esindused. Stabiilseid münte saab tagatiseks panna mitme varaga, nagu fiat-valuuta või kuld või krüpto, või neid ei saa üldse tagatiseks anda.

Mitmed keskpangad katsetavad stabiilseid münte, mida nimetatakse **keskpanga digitaalseks valuutaks** (CBDC). Kuigi CBDC saab kasutada Blockchaini elemente, ei pruugi see olla Blockchaini rakendus. CBDC-d on diametraalselt vastupidised Bitcoini detsentraliseeritud päritolule, kuna CDBC on tsentraalselt reguleeritud valuuta.

Tekib küsimus, kuidas krüptomärke rakendada majandussüsteemis, kus toimub vahetus. Üks võimalus seda teha on vaadata **sümboolset asendatavust** . Mõned märgid saab lihtsamini teise vastu vahetada. Näiteks 1 kg jahupaki saab vahetada teise 1 kg jahupaki vastu. 10-eurose rahatähe saab vahetada ka kahe 5-eurose rahatähe vastu. Sama kehtib ka **asendatavate žetoonide kohta** : üksikud üksused on üksteisest eristamatud ja neid saab omavahel vahetada. Näiteks Polkadot: 1 Polkadoti märgi saab vahetada teise vastu ja kaks poolikut Polkadoti märgi saab vahetada 1 terve Polkadoti vastu.

Sellele vastanduvad **mittevahetatavad märgid** kus märgid on iseenesest ainulaadsed ja seetõttu napid. Mõelge näiteks isikutele, riikidele ja sünnitunnistustele, mida ei saa teiste isikute vastu vahetada, riigi- ja sünnitunnistustele.

Eelkõige sobib plokiahel nende žetoonide tõhusaks hõivamiseks ja nendega kauplemiseks, isegi kui žetoonidel on vaid väike väärtus ja/või need on ainulaadsed. See on oluline, kuna digitaalses maailmas on digitaalsest kaubast lihtne koopiat luua. Seega, kui esinduseks on žetoon, pole mitte ainult võimalus reaalsest maailmast pärit kaupadega hõlpsalt kaubelda. See annab teile ka võimaluse anda igale füüsilisele kaubale autentne digitaalne esitus, ükskõik kui väike või rumal see kaup ka poleks, ja sellega kaubelda. Lisaks on nappide žetooni loomine majanduslikult huvitav, kui soovite hinda kõrgel hoida, võttes arvesse adagioot: "mida väiksem on žetoonide pakkumine, seda suurem on puudus ja seega ka kõrgema hinna võimalus".
Mitmed varade krüptožetoonide puhul varem mainitud eelised, nagu fraktsioneerimine ja nutikate žetoonide loomine, toetavad mittevahetatavate žetoonide kasutajajuhtumit, kuna need võivad muutuda mis tahes (digiteeritava) objekti väga individuaalseks esituseks, mis on loodud ja millega kaubeldakse madal barjäär (kõik saavad siseneda, kõik saavad osaleda) turvaline võrk, väärtuste Internet. Internet, mille abil saab läbipaistvalt mõõta teie mõju keskkonnale ja mis tõukab teid toetama suurema kogukonna eesmärke. Olge teie roll päikesepaneelide omaniku, elektritarbija või võrguvõrku investorina.

Tulevikus võite teoreetiliselt kasutada kõiki teile kuuluvaid varasid, märgistada ja kasutada neid žetoone osaliselt või muul viisil makse- või rahastamisvahendina.

4.3 Fondi omandamise märgid

Kõiki neid eraldi žetoone saab seejärel kasutada raha hankimiseks mitmel viisil: alates esialgsetest mündipakkumistest (ICO), turvamärgi pakkumiste (STO) ja esialgsete vahetuspakkumiste (IEO) kaudu kuni esialgsete DEX-pakkumisteni (IDO).

Algset mündipakkumist (ICO) kasutati varem peamiselt Blockchaini projektide jaoks raha kogumiseks Internetist . Eelkõige oli Ethereum žetoonide loomise ja müümise peamine plokiahel. Märkimisväärne arv kuritarvitamise juhtumeid tekkis ICO trendi alguses, ka seetõttu, et ICOd toimusid väljaspool riiklike seaduste ja määruste kaitset. Selle tulemusena **Julgeolek**

Token Offering (STO) loodi teenima sama eesmärki kui ICO, kuid nüüd peetakse tokenit väärtpaberiks, millel on standardprotokollid, hääleõigused ja palju muud, mis on, kuigi mitte täielikult, mitme riigi väärtpaberi- ja börsiseaduste ja määrustega kooskõlas. STO pole seni avalikus ruumis eriti edukaks osutunud. Samuti loodi uute, rohkem reguleeritud, kuid siiski "avatud" alternatiividena, nagu **esialgne vahetuspakkumine** (IEO) ja **esialgne DEX-pakkumine** (IDO). Siin on tsentraliseeritud või detsentraliseeritud vahetus, nagu Binance või Uniswap alustavatel ettevõtetel on võimalus saada ühisrahastust oma vahendusplatvormi kaudu, mis tavaliselt kontrollib KYC ja AML-i.

Kogukonna detsentraalse väärtuste Interneti kujundamise suund näib jätkuvat ideaalide, ideede, tehniliste võimaluste, vigade, imeliste õnnetuste ja visaduse keerises.

5 Blockchaini kasutusalad ja rakendused

Selles peatükis on toodud kolm näidet Blockchaini kasutamisest ja rakendustest. Enne seda tutvustatakse, kuidas organisatsioonid saavad strateegiliselt mõelda oma ärimudeli asjakohastele elementidele ja võimalustele, mida Blockchain pakub. Peatükk lõpeb konkreetsete punktidega, millele ettevõte Blockchaini rakendamisel tähelepanu pöörab.

5.1 Ärimudelid

Blockchain pakub tavaliselt väärtust ärimudelites ja äriökosüsteemides, kus luuakse/saab luua ja jagada partnerite vahel digitaalseid andmeid ja tehnoloogiat. See kui Blockchain on digitaaltehnoloogia, mis sobib nende digitaalsete andmepõhiste ärimudelitega ja võimaldab partneritel teha koostööd seal, kus nad varem ei saanud. Need partnerid saavad nüüd usaldada "süsteemi", kus nad enne Blockchaini ei usaldanud teineteist algusest peale koostööd tegema. Selles mõttes on Blockchain eelkõige võimalus kasvatada ja digitaliseerida ökosüsteeme, mis kasutavad **digitaalseid andmepõhiseid ärimudeleid** .

Mis puudutab ärimudeleid, siis **detsentraliseeritud ärimudeli lõuend**[6][7] on asjakohane, aga ka detsentraliseerimine on avalike lubadeta plokiahela kohanduste jaoks kesksel kohal. Sellel konkreetsel lõuendil on žetoonide omanikel keskne positsioon, kuna neil on mitu rolli, näiteks kasutaja, valideerija, töötaja ja/või omanik. Seda tüüpi "uus" mõtlemine annab aimu potentsiaalsetest uutest võimalustest, mida avalik lubadeta Blockchain toob, kuna osapooltel, kes üksteist ei tunne, on alternatiivina seadistada ja kasutada suhteliselt madalat tõkkesüsteemi, et jagada ja kontrollida andmeid koos, kui nad ise ei tea. üksteist.

Seejärel seab avalikkus halduse detsentraliseeritult, andmeid säilitatakse detsentraliseeritult ja suhtlus eri osapoolte vahel toimub peer-to-peer. See on plokiahela kõige avatum vorm. Ettevõte võib vabalt Blockchaini ehitusplokke ise kohandada. Tsentraliseeritud süsteemi korral teeb otsuseid keskorganisatsioon.

Detsentraliseeritud ärimudeli puhul jagatakse müük sageli nende vahel, kes panustavad võrgustikku kõige rohkem ning platvormi kasutamise kulud on väga madalad – näiteks sotsiaalblogimise Blockchain platvormi Steemit puhul.

5.2 Ettevõtte plokiahela rakendused

Selles lõigus kirjeldatakse kolme juurutatud rakendust neljas erinevas tööstusharus ja võrreldakse neid, kasutades suhtelisi eeliseid, mida Blockchain nendes rakendustes pakkus. Neli rakendust on järgmised:

1. Valitsus ja avalikud hüved Lantmäteritelt.
2. Tootja BMW.
3. Singapore Airlinesi digitaalne rahakott.

[6]https://canvanizer.com/new/decentralized-business-model-canvas
[7]https://medium.com/mvp-workshop/decentralized-business-model-canvas-1-9daf6e4bc9fe

Üks kasulik ülevaade, mis aitab teil mõista, kus paljud Blockchaini sektorid Blockchaini rakendavad, on allpool toodud 67 ettevõtte plokiahela võrgustiku ja sektorite seas, kuhu need rakendused kuuluvad (Rauchs, Blandin, Bear, McKeon, 2019).

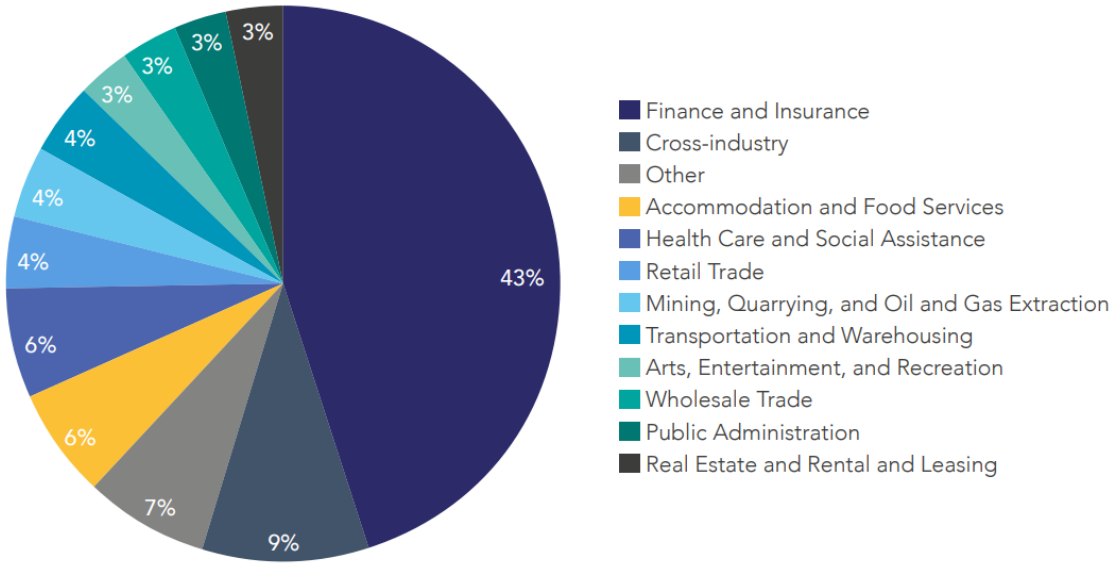


Figure 11: Ülevaade 67 reaalajas ettevõtte Blockchaini võrgust ja sektoritest, kuhu need kuuluvad (Allikas: Rauchs, Blandin, Bear, McKeon, 2019).

Esimene näide on **valitsuse ja avalike hüvede sektoris** . Rootsi **Lantmäteriedil** on ülesandeks pidada katastrisüsteemi korrashoidu, anda geoandmeid ja teostada maa kinnistamist. Vaja on suuremat läbipaistvust ja projekti tõhusust, kuna erinevad partnerid töötavad koos, kasutades käsitsi protsesse, mis näivad ebaefektiivsed ja veaohtlikud.

Lantmäteriet katsetas selleks lahendust, et näha, kuidas sellised osapooled nagu kinnisvara ostjad, müüjad, maaklerid, finantsteenused, juristid, pensionifondid ja Lantmäteriet saavad koostööd teha tõhusal veebiplatvormil, mis tagab päringu kohese läbipaistvuse digiseadmete kaudu. Projekt loodi järkjärgulise projektina (2015–2019) kontrollitud kasti olukorras koos usaldusväärsete partneritega, kuid ilma ambitsioonika lühiajalise detsentraliseerimiseta. Selgelt keskenduti madalal rippuvate viljade korjamisele maaomandite registris, luues samal ajal aluse tulevastele teenustele.

Projekti käigus kerkisid esile juriidilised probleemid, millest tuli üle saada. Ühe jaoks pidi Lantmäteriet mõtlema, kuidas käsitleda üksikisikute õigust oma andmeid kontrollida (EL-i isikuandmete kaitse üldmäärus – GDPR), sealhulgas soovi ja võimaluse korral neid kaitsta ja kustutada. Nagu ka selle kohta, kuidas saab digiallkirju EL-i piires õiguslikult siduvate allkirjadena kasutada (eIDAS-e juhend) või Blockchainil põhinevate digiallkirjastatud (e-)lepingute staatusest.

Maaomandite müük oli ambitsioonikas selle poolest, et erinevad osapooled lõid uue protsessi ja mängu uue tehnoloogilise lahendusega. Blockchaini lahendused hõlmasid nii privaatseid, suletud, loaga Blockchaini süsteeme kui ka hajutatud avalikku võrku. Privaatne Blockchain kuulub valitsusele, seda juhib piiratud arv usaldusväärsete vahendajate sõlme ja see on Rootsi avaliku valitsuse järelevalve all. See süsteem teeb koostööd ChromaWay ja sidusrühmade

privaatvõrguga. See kasutab nutikaid lepinguid, praktilist Bütsantsi tõrketaluvust ja töötõenduse konsensusmehhanisme, väljas ja sisse lülitatud digitaalset identiteeti mobiiltelefonirakenduse kaudu ja ilma žetoonideta.

Arvestades varasemaid GDPR-i probleeme, jääb toiming Lantmäterietile registreerituks ja seda ei kanta üle avalikku plokiahelasse. Lepingud allkirjastatakse käsitsi ja paigutatakse räside kaudu Blockchaini. Algsed lepingud on serveris teiste osapooltega, sellel infol on varukoopiad. Telia pakub mobiilirakenduse ID-lahendust, mis võimaldab inimestel registreeruda ilma oma Rootsi riigiteenistuse numbrit avaldamata. Need registreeringud salvestatakse Bitcoini plokiahelas räsi kaudu ja kinnitatakse. Digitaalseid isikuandmeid saab üksikisiku soovil eemaldada ja see ei ole seadusega ette nähtud avalikuks teabeks.

Peamised eelised olid nii Blockchaini tehnoloogia kasutamise turvalisus kui ka töökindlus. Viimase osas nihkus maaomandi registreerimise tähtaeg 4-6 kuult mõne päeva peale. Samuti nähti ette 100 miljoni euro aastas kokkuhoid tänu väiksematele vigadele ja hooldusele (Kairos Future, 2017). See vähendab ebaselgete omadustega lepingute, pettuste andmete või vara varastamise võimaluste riske. Läbipaistvaks muutus ka auditijälg nii kliendile, audiitorile kui seadusandjale. Samuti tugevdas ökosüsteem omavahelisi protsesse ja andmevahetust ilma keskse teenuse ja ärimudeli liigse pöördeta. Ja lõpuks, kuid mitte vähem tähtsana, avalik juurdepääsetavus suurendas usaldust protsessi ja osapoolte vastu. Pärast testimist võiks süsteemi laiendada, et hõlmata selliseid osapooli nagu kindlustusandjad, notarid ja muud kohalikud ametiasutused.

Projekt valmis 2019. aastal, näidates, et platvormi arhitektuur osutus võimalikuks, kuid Lantmäteriedi innovatsioonijuhi Mats Snälli sõnul ei integreeritud seda kunagi kinnistusregistri tootmissüsteemi, kuna seadusandluse muudatus oleks vaja enne, kui süsteemi saaks tulevikus laiendada. (Baraniuk, 2020). Tõenäoliselt viitab see väljakutsele avaldada kasutaja identiteediandmeid avalikus plokiahelas.

Teised uuringud viitavad ka "põhilise muutuse juhtimisstruktuuris, näiteks Lantmäterieti rollis", mis võis olla konkreetselt kinnisvaraökosüsteemide jaoks aluseks projekti edasise arengu külmutamiseks (Schnuer, 2020). .

Vahepeal kasutab Lantmäteriet oma õppetunde Bockchainiga katsetamiseks. Näiteks ühine valitsusülesanne DIGG-ga, mille eesmärk on leida „mudel või kontseptuaalne lahendus, kuidas luua usaldust tehisintellekti ja muu uue tehnoloogia, näiteks Blockchaini tehnoloogiaga automatiseerimise vastu”. (AI Rootsi, Lantmäteriet, 2020).

Teine Blockchaini rakenduse näide puudutab **tootmissektori BMW-d. Autotööstuse ärimudelid peavad tegelema** 4. tööstusrevolutsiooni tehnoloogiatega, nagu elektrifitseerimine ja autonoomsed süsteemid üha kasvavates keskkonnateadlikes tingimustes.

BMW mõista, kuidas saab kasutada autode digitaalset identiteeti, et see võimaldaks kasutada teisi 4. tööstusrevolutsiooni tehnoloogiaid ja kontseptsioone. Eelkõige auto ja kasutaja pideva Interneti-ühenduse olemasolu privaatsus/turvalisus, samuti vajadus neid andmeid turvaliselt säilitada. See turvaline andmevahetus seadmete vahel, mis tagab turvalise digitaalse identiteedi , on see, mille Blockchain potentsiaalselt lauale toob, pakkudes seega BMW-le sissepääsu autode jagamismajanduse turule.

BMW on testinud mitmeid autojagamisrakendusi, nagu Share Now, kus saab kaasata mõlema auto kui kasutaja digitaalset identiteeti. Need autotööstuse kombineeritud digitaalsed

identiteedid võivad registreerida näiteks bensiinitanki või auto parkimiskoha. Seda tüüpi teavet saab seejärel kasutada ärimudelites, kus autotootjad koos vahendajatega või ilma pakuvad isikupärastatud teenuseid, nagu kahjukindlustus, autonoomsed autosõidud või parandavad oma autokogemust üldiselt.

Selle konkreetse näite puhul katsetas BMW aga lihtsamat projekti, keskendudes ainult auto ID-le ja selle salvestatud andmetele, seega ei keskendunud kasutajale. Mõte seisneb selles, et võimalikud kasutatud BMW ostjad oleksid huvitatud usaldusväärsetest andmetest auto läbisõidu, avariiajaloo, hooldusajaloo ja muu info kohta. Potentsiaalne müüja võib neid andmeid jagada potentsiaalse müüja või tema kindlustusandjaga, BMW võib kasutada teavet oma ärimudeli täiustamiseks, näiteks kasutada seda oma klientide paremaks teenindamiseks.

Selle lahenduse loomiseks töötas BMW Startup garaaž Blockchaini idufirmadega, antud juhul VeChainiga. Samuti kasutab BMW tulemusi auto ID väljatöötamiseks, mis on esimene samm sõiduki identiteedi (VID) suunas, mida Mobility Open Blockchain Initiative (MOBI) liikmed saavad koos kasutada. MOBI on Blockchaini konsortsium, mis töötab koos välja Blockchaini standardeid.

Koostöös VeChainiga sündis rakendus **VerifyCar** . VeChain on detsentraliseeritud autonoomne organisatsioon, millel on keskne juhtorgan, mis kasutab oma avalikul VeChaini plokiahelal volituste tõestamise konsensuse meetodit ja erinevaid märke.

VID-l on sellel plokiahelal unikaalne ID. Rakendus kogub perioodiliselt andmeid (autosiseste SIM-kaartide ja masinatevahelise side kaudu), mida kontrollitakse VeChain Blockchainis: VeChain salvestab ainult viite andmetele, andmed jäävad sõidukisse endasse. Jäädvustatud autoandmed sisaldavad nii staatilist teavet, nagu auto tüüp ja tootmiskuupäev, kui ka dünaamilist teavet, nagu läbitud kilomeetrite arv. Kui autoomanik soovib andmeid teise osapoolega jagada, kasutab ta rakendust VerifyCar, et näidata andmeid, sealhulgas plokiahela viiteid, et näidata, et need on sõidukisse salvestatud tegelikud andmed.

Selle BMW kavatsus puudub kontroll VeChaini juhtimise ega koodi üle. Alates 2022. aastast pole rakendust toodetud .

Selle lahenduse katsetamisel astub BMW kontrollitud esimese sammu detsentraliseeritud Blockchaini tehnoloogia järkjärgulise integreerimise suunas. Samuti, kui VerifyCari saab kasutada autode jaoks, siis miks mitte omada VID-i moodi digitaalset isikutunnistust, et autoosad ei oleks võltsitud, millisest kohast ostetud toorainet tootmisliinilt leida või teatud tootmise tootmis- või transporditingimustest aru saada. masinad, mille olete tellinud? Selle mõtteviisi kohaselt katsetab BMW Blockchainiga ka **läbipaistva tarneahela kasuks** .

Näiteks 2019. aastal **laiendati PartChaini** pilootprojekti esitulede ostmiseks Amazon Web Servicesi, Microsoft Azure'i ja Hyperledger Fabric Blockchaini abil (Ledger Insights (2020, 31. märts)) teistele tarnijatele. See võimaldas BWM-il jälgida oma komponente ja pikaajaline kriitilise tähtsusega tooraine „kaevandusest sulatustehaseni". (BMW Pressclub Global, 2020). Lisaks sellele, et tagada „lihtsam sertifitseerimine ja lühemad tolliprotseduurid" (BMW, 2019).

näide **on Singapore Airlinesi digitaalne rahakott KrisPay** . Singapore Airlines soovis plokiahela abil oma klientide lojaalsust veelgi suurendada. Selle tulemusel tugevdati 2018. aastal oma püsikliendiprogrammi KrisFlyer KrisPay digitaalse Blockchaini rahakotiga.

KrisPayga saavad kliendid vahetada oma KrisFlyeri lennumiile KrisPay miilide ehk krüptovaluuta žetoonide vastu. Neid KrisPay märke saab salvestada ja kulutada erinevate kaupmeeste juures, nagu pangad, bensiinijaamad ja kauplused. Samuti saab klient salvestada ja vahetada muid hüvesid, näiteks kasutades DBS-i (Development Bank of Singapore Limited) krediitkaarti, või teenida, osta või kulutada Singapore Airlinesi miile, näiteks lennu uuendamiseks. KrisPay märgi rahalise väärtuse dikteerib Singapore Airlines. Seega lahendus, mida KrisPay siin pakub, on anda klientidele lihtne viis oma preemiate lunastamiseks, et hoida ära kilomeetrite raiskamist, kui salvestate need žetoonid kaupmehevõrku. Teatud viisil saavad kliendid fiati tagatud valuutadele digitaalset lisa/alternatiivi.

KrisPay funktsioone on lihtne kasutada oma mobiilseadmes oleva rakenduse ja vahetute müügipunktitehingute kaudu. Täiendava kasutatavuse parandamiseks saab KrisFlyeri miile perekonna või volitatud kandidaatide piires üle kanda.

Blockchaini rahakotte ja krüptovaluutasid kombineerides kasutab KrisPay Blockchaini tugevusi, nagu turvalisus kõigi kasutajate jaoks, kuna tehingute registreerimine on võltsimiskindel. Kaupmeeste tehingud kiidetakse kohe heaks ja tehakse arusaadavaks, ilma aeglasemat kulukamat vahendajat kasutamata. See toetab viipemaksete vastavust kaupmeeste (ja nende finantsasutuste) vahel ning annab neile ajakohase klienditeabe.

KrisPay töötati välja koos KPMG Digital Village'i ja Microsoftiga. KrisPay on Singapore Airlinesile kuuluv eraettevõte, mis töötab Microsoft Azure'i (algselt Ethereumi protokollil põhineva) kombinatsioonil Azure'i rakenduse ja andmebaasi funktsioonidega. Erinevad partnerid haldavad ja kontrollivad Blockchaini andmebaasi nii, et igaühel oleks kliendi-/tehinguteave samal ajal saadaval.

Microsoft teatas, et lõpetab oma Azure Blockchaini 2021. aastal ja toetab klientide üleminekut Quorum Blockchain Service'ile, mis on Ethereumi protokolli teine variant (Microsoft, 2021).

KrisPay märgid ja rahakott ühendati 2020. aastal uues rakenduses Kris+. See rakendus kasutab kliendiandmeid ka selleks, et Singapore Airlines saaks oma kliente paremini teenindada ja pakkuda isikupärastatud pakkumisi isegi mobiiltelefoni geograafilise asukoha alusel.

KrisPay rahakotti saab potentsiaalselt kasutada piletite ostmiseks, teie digitaalse identiteedi tõendamiseks või täiendava üldise märgina, mida saab kasutada fiat-valuutade või muude lojaalsuspunktide vastu vahetamiseks.

Kokkuvõtteks võib öelda **, et kõik need rakendused** on juhitavad täpselt määratletud Blockchaini juhtumid, mida rakendatakse hoolikalt osana suuremast visioonist keskkonnas, mida algatajad usaldavad ja kontrollivad. Juhtumid näitavad selgust elementide osas, mida nad näevad võimalusena või võimaluse puudumisena, ja kasutavad järkjärgulist muutuste protsessi, mille käigus nad suurendavad jõupingutusi ettevaatlikest esimestest sammudest täieliku rakendamiseni.

Nende keskkond koosneb stabiilsetest protsessidest, tuntud ärimudelist ja usaldusväärsetest partneritest, et katsetada tehnoloogia rohkem proovitud aspekte ja selle detsentraliseeritud ärimõjusid.

Täieliku detsentraliseeritud ärimudeli rakenduse näitamiseks ei olnud ruumi. Kui soovite näidet, lugege kindlasti Augur Predication turu näidet peatükis 16.5. (Lin Lim, Janse, 2021).

5.3 Millal on plokiahela rakendamisel mõtet?

Eelnevatest näidetest on selge, et Blockchaini edukaks rakendamiseks peavad olema teatud tingimused.

On mitmeid kriteeriume, mille põhjal saate otsustada, kas Blockchain on teie ettevõtte jaoks mõttekas juhtum. Nende kriteeriumide eesmärk on kõrvaldada andmete või andmeliiklusega seotud hõõrdumised või luua võimalusi andmete ja andmeliiklusega osapoolte vahel. Rusikareeglina võib kriteeriumid kokku võtta järgmiselt:

1. **Digitaalne innovatsioon** on osa strateegiast.
2. **Andmeid jagavad** erinevad osapooled .
3. Need andmed ja nendega seotud tehingud puudutavad **rahalist väärtust** .
4. Andmed on **konfidentsiaalsed** .
5. Erinevad osapooled muudavad andmeid.
6. Andmed tuleb kontrollida.
7. Arvestama peab **selge ja piisava investeeringutasuvuse** .
8. Kontrollimine on **keeruline, kulukas ja/või aeganõudvam** .
9. Lahendus Blockchaini valimiseks on probleemi lahendamiseks **lihtsaim lahendus** .
10. Lahendus mõjutab olemasolevat organisatsioonilist struktuuri.
11. Lahendus mõjutab olemasolevat töövoogu.
12. Lahendus mõjutab olemasolevat ökosüsteemi.
13. Tehniline lahendus on lähedane või integreeritav olemasolevate süsteemidega.
14. Lahendus on andmemahukas, kuid skaleeritav. Mõelge erinevustele 1k, 10k, 100k, 1 miljon või> 10 miljonit tehingut tunnis.

Kui näete võimalust Blockchaini nende kriteeriumide alusel rakendada, saate jätkata vajalike kasutajautiliitide ja nende utiliitide moodustavate ehitusplokkide mõistmist. Näiteks "maksemärgi" ehitusplokk mõjutab maksetehingute lihtsust, kiirust ja läbipaistvust. Teised ehitusplokkide näited on rahakotid, nutikad lepingud, dApp-id, žetoonide tüübid, oraaklid jne.

Praegu on Blockchaini mõju ettevõtetes keskendunud peamiselt efektiivsusele, vahendusele ja registreerimisele. Ja mõju on suurim seal, kus koostööd tegevad osapooled avavad ja loovad uusi andmeid. Tulevikus aga eeldatakse, et keerulised Blockchaini juurutused, mis juhivad ökosüsteemide detsentraliseerimist ja integreerimist, näevad Blockchaini suurimaid eeliseid.

Plokiahela projekti kasutamise hindamiseks saate kasutada järgmist lihtsustatud otsustuspuud:

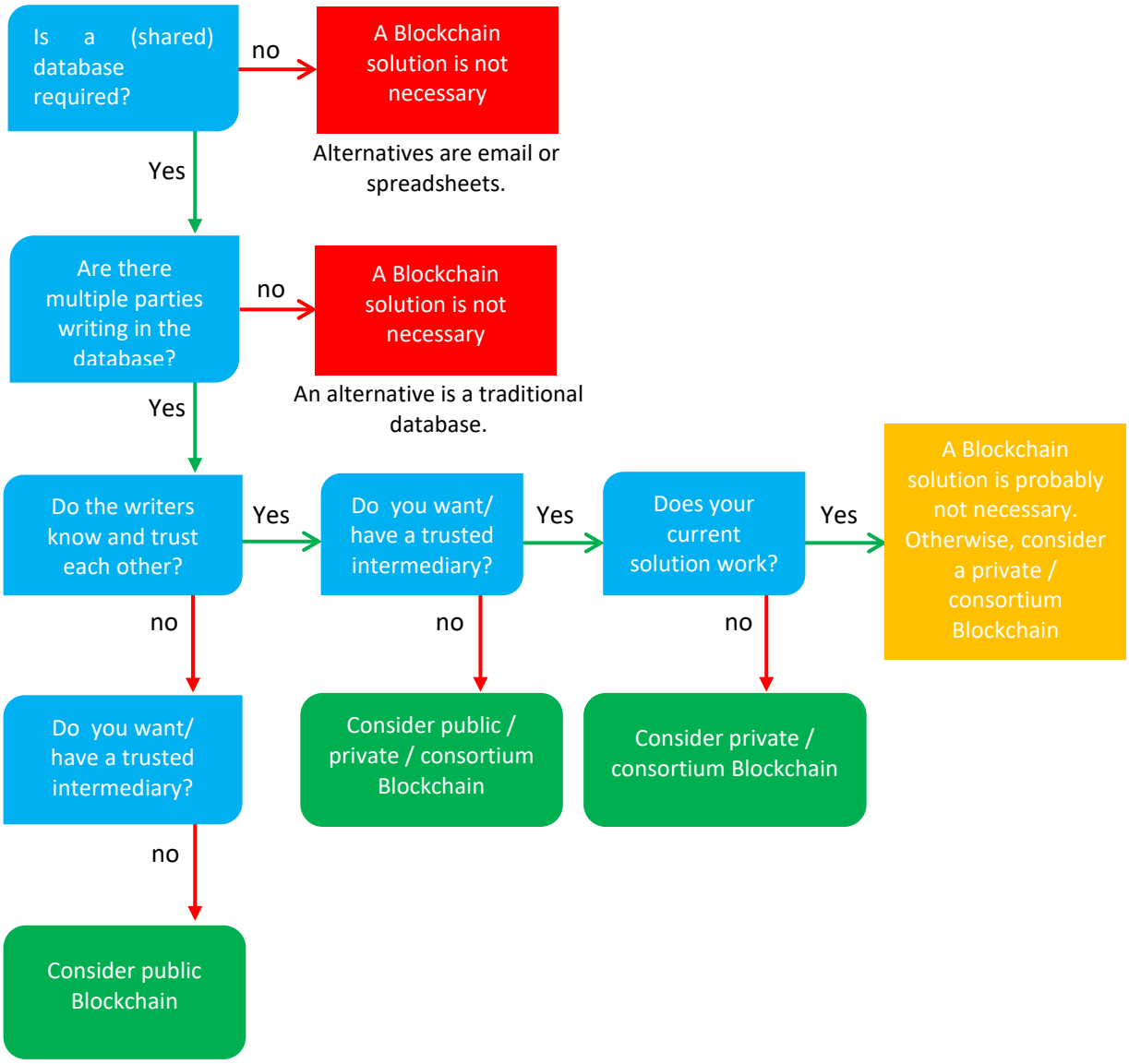


Figure 12: Lihtsustatud otsustuspuu, kas kasutada plokiahelat või mitte (Allikas: Lin Lim, C., Janse, A., Blockchain Basics, 2021).

6 Viited ja allikad edasiseks lugemiseks

Ackermann, J. & Meier, M. (2018). *Blockchain 3.0: plokiahelasüsteemide järgmine põlvkond.*

Täiustatud seminar Blockchain Technologies, 2018. aasta suveperiood, Munchi tehnikaülikool .

AI Rootsi, Lantmäteriet (2020, november). *Avaliku sektori AI usaldusmudeli loomine,*

Lugege aadressilt https://www.ai.se/en/node/85154

Antonopoulos, AM (2016). *Raha Internet: räägib* . Merkle Bloom Llc.

Augur. (nd). *Ülevaade* . Vaadatud 23. detsembril 2019 saidilt https://docs.ugur.net/#overview

Augur. (2018, 9. juuli). *Forecast Foundation OU privaatsuspoliitika* . Tutvutud 23. detsembril 2019 Augur.net veebisaidilt: https://www.ugur.net/privacy-policy/

Baraniuk, C. (2020, 11. veebruar). *Blockchain: revolutsioon, mis pole veel päris juhtunud* . Konsulteeritud saidilt https://www.bbc.com/news/business-51281233

Bitcoin Block Rewardi poolitamine . (2019). Konsulteeritud 23. detsembril 2019, alates

Bitcoinblockhalf.com veebisait: http://www.bitcoinblockhalf.com

BMW, (2019, 14. oktoober). Kuidas Blockchaini lahendused võivad autojuhti aidata. Uurige aadressilt https://www.bmw.com/en/innovation/blockchain-automotive.html

BMW Pressclub Global (2020, 31. märts). *BMW Group kasutab tarneahela läbipaistvuse suurendamiseks Blockchaini.* Uurige aadressilt https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency .

Buterin, V. (2013). *Ethereumi valge paber: järgmise põlvkonna nutikas leping ja detsentraliseeritud rakendusplatvorm* [White paper]. Konsulteeritud 27. detsembril 2019 Blockchainlabist: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, 6. mai). *DAO-d, DAC-id, DA-d ja palju muud: mittetäielik terminoloogiajuhend.*

Vaadatud 27. detsembril 2019 veebisaidil Ethereum.org: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

ChainTrade. (2017, 27. detsember *). 10 nutikate lepingute kasutamise eeliseid* . Konsulteeriti

27. detsember 2019, Mediumi veebisaidilt: https://medium.com/@ChainTrade/10-preferences-of-using-smart-contracts-bc29c508691a

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K. ja Reitzig, M. (2018). Bitcoin ja tõus

detsentraliseeritud autonoomsed organisatsioonid. Journal of Organization Design, 7(1).

https://doi.org/10.1186/s41469-018-0038-1

Kaorise tulevik. (2017) *Kinnistusregister plokiahelas – testbed* . Tutvumine saidil https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia, ChromaWay & Kairos Future. (2016). *The Kinnistusregister plokiahelas.* Tutvumine saidilt http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Ledger Insights (2020, 31. märts). *BMW laiendab osade jälgitavuse tagamiseks tarneahela plokiahelat.* Uurige aadressilt https://www.ledgerinsights.com/bmw-blockchain-supply-chain-parts-traceability/

Ledger Insights (2020, 15. oktoober), *Singapore Airlines laiendab oma plokiahelapõhist tasu digitaalset rahakotti* . Konsulteeritud aadressil https://www.ledgerinsights.com/singapore-airlines-extends-its-blockchain-based-reward-digital-wallet/

Lin Lim, C., Janse, A., *Blockchain Handbook* , september 2021, 10. peatükk. Väljaandja: De boekdrukker Amsterdam. NUR: 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain- baseboek-digitale-versie-2.pdf

Microsoft, 2021, 14. mai). *Nõutav toiming: migreerige oma Azure Blockchain Service'i andmed 10. septembriks 2021* . Lugege aadressil https://azure.microsoft.com/en-us/updates/action-required-migrate-your-azure-blockchain-service-data-by-10-september-2021/

Microsoft (2019, 2. mai), *Singapore Airlines muudab klientide lojaalsust Azure'i plokiahela abil* . Konsulteeriti 4

MOBI. (2019). *Sõiduki identifitseerimisstandard* . Tutvumine aadressil https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Nakamoto, S. (2008). *Bitcoin P2P e-sularaha paber.* Konsulteeritud 23. detsembril 2019, alates Metzdowd.com veebisait: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, 30. september). *Re: Lõhkusin rahakoti, saadab ei kinnita nüüd.* [Võrgus foorumi kommentaar]. Sõnum postitati aadressil https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, 1. november). *PayPali hiljutine elektrikatkestus soodustab bitcoinide kasutuselevõttu* . Vaadatud 23. detsembril 2019 Bravenewcoin.com veebisaidilt: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Rauchs M., Blandin, A., Bear, K., McKeon, S. (2019). 2. *globaalse ettevõtte plokiahela võrdlusuuring* . Tutvumine saidil https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf

Schnuer, C. (2020, 7. detsember). *Kinnisvaraturu muutmine plokiahela kaudu* . Konsulteeritud saidilt https://delano.lu/article/delano_changing-property-market-through-blockchain

Strategyzer. (nd) *Ärimudeli lõuend* . Konsulteeritud 23. detsembril 2019 saidil https://www.strategyzer.com/canvas/business-model-canvas

Sultan, K., Ruhi, U., & Lakhani, R. (2018). *Plokiahelate mõtestamine: omadused ja*

Rakendused. 11. IADISe rahvusvaheline konverents Infosüsteemid 2018, 49–57

Vigna, P. ja Casey, M. (2015). *Krüptoraha vanus: kuidas on bitcoin ja plokiahel*

väljakutse ülemaailmsele majanduskorrale . New York, NY: Picador/St. Martini ajakirjandus.

Young, S. (2018). *Põhiseaduslike õiguste jõustamine arvutiseadustiku kaudu.* Konsulteeritud alates

CUA Law Scholarship Repository veebisait: https://scholarship.law.edu/jlt/vol26/iss1/5/

I lisa – Terminite sõnastik

51% rünnak: rünnak plokiahela vastu, mis saavutatakse enam kui 51% kogu võrgu arvutusvõimsusest omandades.

Klient-server mudel: mudel, kus kliendid (kasutaja) on serveriga ühendatud. Server sisaldab klientide jaoks olulisi andmeid. Kliendid loovad neile andmetele juurdepääsu saamiseks ühenduse serveriga. See muudab kliendid serverist sõltuvaks.

Distributed Ledger Technology (DLT) : hajutatud pearaamatu tehnoloogia.

Kahekordne kulutamine : Bitcoini kaks korda kulutamine. Näiteks, et sul on 1 Bitcoin, aga sellega saadad inimesele A 1 Bitcoini ja isikule B 1 Bitcoini.

Täissõlm : sõlm, millel on plokiahela täielik koopia.

Miner : arvuti, mis pakub kehtiva ploki loomiseks arvutusvõimsust. Plokk on kehtiv ainult siis, kui see leiab kehtiva räsiväärtuseni viiva nonce'i.

Sõlm : seade, mis on ühendatud arvutivõrku.

P2P : vaadake peer-to-peer-i.

Peer-to-peer : arvutivõrk, kus arvutid on üksteisega võrdsed ja saavad üksteisele teenuseid pakkuda.

Töötõestus : konsensusmehhanism, mis nõuab, et kaevurid kasutaksid uue ploki jaoks õige räsiväärtuse leidmiseks arvutivõimsust. Õige räsiväärtuse leidmisel on neil lubatud plokk plokiahelasse lisada ja preemia saada.

Single Point of Failure (SPOF) : võrgu osa, mis peatab tõrke korral kogu võrgu töö.

SPOF : Vt Üks tõrkepunkt.

Usaldusväärne kolmas osapool (TTP) : usaldusväärne vahendaja.

TTP : vaadake usaldusväärset kolmandat osapoolt.

Valge raamat : dokument, mis kirjeldab, kuidas konkreetne probleem lahendatakse. Satoshi Nakamoto on Bitcoini valges raamatus kirjutanud, kuidas Bitcoin lahendab hajusvõrgus topeltkulutamise probleemi.

Blockchain 1.0 : Esimene plokiahelate põlvkond, mida on peamiselt kasutatud krüptovaluutade säilitamise ja ülekandmise hõlbustamiseks.

Blockchain 2.0 : plokiahelate teine põlvkond, mis on rohkem keskendunud nutikate lepingute, dAppide ja DAO-de lubamisele.

Blockchain 3.0 : kolmas põlvkond plokiahelaid, mis on lahendanud hulga probleeme, millega blockchain 2.0 peab veel tegelema. Selliste probleemide näideteks on mastaapsus, koostalitlusvõime, privaatsus, jätkusuutlikkus ja juhtimine.

Gaas : Ethereumi plokiahelas tehingu sooritamise tehingukulud.

Detsentraliseeritud rakendus (dApp): rakendus, mis kasutab plokiahela detsentraliseeritud andmesalvestust. Rakendust ei käivitata keskserveri, vaid sõlmede detsentraliseeritud võrgu kaudu. Nii nagu tavalisel rakendusel, on sellel sageli esiots ja kasutajaliides.

Detsentraliseeritud autonoomne organisatsioon (DAO): autonoomne üksus, mis tugineb ka üksikisikute palkamisele. Need isikud saavad täita teatud vajalikke ülesandeid, mida üksus ei saa. DAO käsutuses on selleks sisemine kapital, millega saab premeerida nende isikute teatud tegevusi. DAO eristab tsentraliseeritud organisatsioonist põhimõtteliselt see, et sellel ei ole tippjuhtkonda ega tegevjuhti. See on mittehierarhiline organisatsioon.

Nutikas leping : leping, mille tingimused on sätestatud koodis. Leping on isetäituv, kuna teeb tingimuste täitmisel ise vastavad vastavad toimingud. Leping peab siiski sisaldama piisavalt teavet igalt lepinguosaliselt, et jätta pooled ilma võimalusest leping lõpetada. Nutikaid lepinguid on kahte tüüpi: deterministlikud ja mittedeterministlikud.

Solidity : programmeerimiskeel, mis on spetsiaalselt välja töötatud Ethereumi jaoks nutikate lepingute kirjutamiseks.