Tartu Ülikool

Maailma keelte ja kultuuride kolledž

Rene Torop

„BITCOIN, BLOCKCHAIN UND KRYPTOASSETS: EINE UMFASSENDE EINFÜHRUNG“ VALITUD PEATÜKKIDE TÕLGE JA TÕLKE ANALÜÜS

Magistriprojekt

Juhendaja: Terje Loogus

Kaasjuhendaja: Anne Arold

Tartu

2019

SISUKORD

SISSEJUHATUS

Magistriprojekt eesmärk oli tõlkida Alexander Berentseni ja Fabian Schäri teose „Bitcoin, Blockchain und Kryptoassets" valitud peatükid eesti keelde ning analüüsida tõlkimisel tekkinud probleeme ja nende lahenduskäike.

Tõlgitud teose puhul on tegemist Fabian Schäri väitekirjaga, mis avaldati 2017. aastal. Teoses on kokku kaheksa peatükki, mis jaotuvad 333 leheküljele. Peatükid 1 ja 6 kirjutati mõlema autori poolt koos ning ülejäänute autoriks on vaid Fabian Schär, kes on ettevõtlusnõustaja digipanganduse valdkonnas ning samuti Baseli Ülikooli dotsent plokiahela valdkonnas. Teose eesmärk on anda põhjalik ülevaade plokiahela tehnoloogiast ning sellel põhinevast krüptovääringust bitcoin.

Teemavalik põhineb asjaolul, et plokiahela näol on tegemist võrdlemiselt uue revolutsioonilis-disruptiivse tehnoloogiaga, mis võib muuta tulevikus pea kõikide valdkondade toimimist. Revolutsioonilisus seisneb selles, et plokiahelal töötavad teenused on läbipaistvad, avalikkusele avatud ning samuti väga turvalised. Disruptiivsus peegeldub asjaolus, et traditsiooniline väljakujunenud teenusepakkuja roll võib plokiahela tehnoloogia rakendumisel hoopiski kaduda. Sellest lähtuvalt tekkis huvi, kuidas midagi sellist on üldse võimalik teostada. Lisaks üldisele huvile valdkonna vastu oli veel mõjuvaks teemavaliku ajendiks isiklik huvi krüptovääringutega tegelema hakata, mis paraku aga ei realiseerunud.

Magistriprojekti raames tõlkisin tervenisti teise peatüki, mis annab piisava ülevaate plokiahelast ja bitcoinist ning mis on samuti veel mõistetav inimesele, kes ei oma erialalisi teadmisi arvutiteaduse valdkonnast. Samuti tõlkisin alapeatüki 5.3, mis käsitleb bitcoinide nn kaevandamist ehk juurdetekitamist, mis omakorda tekitas arvutimaailmas palju pahameelt.

Tõlkeprojekti eesmärk oli keskenduda valdkonna terminitele ning tõlkimisele eesti keelde. Terminite tõlkimise analüüs moodustab projekti teoreetilise poole põhituuma. Selleks lähtusin Peter Newmarki tõlketeooriast.

Magistriprojekt koosneb neljast peatükist: sihttekstist, teema tähtsusest/ajakohasusest, tõlkimise lähtekohtadest, mis omakorda jaguneb kaheks alapeatükiks ning terminite analüüsist.

1. SIHTTEKST

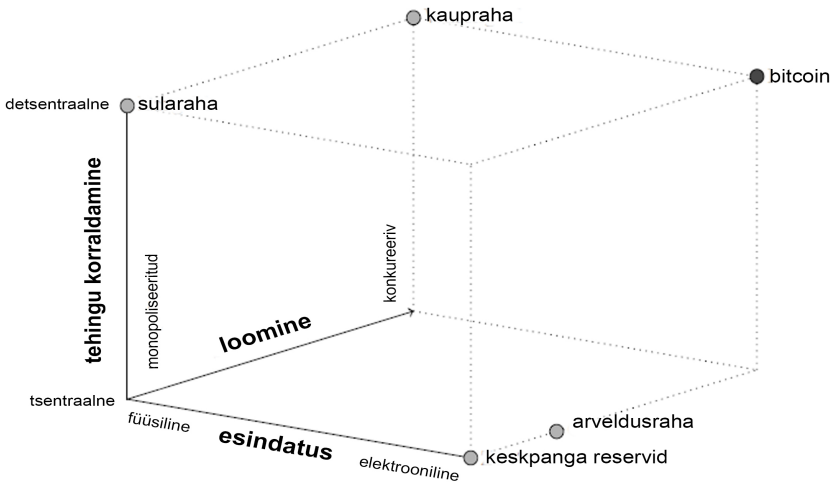
2 Bitcoini ülevaade

Selles peatükis alustame bitcoini analüüsiga. Seletame termineid, piiritleme bitcoini süsteemi klassikalisest finantssüsteemist ja selgitame, millised tagajärjed on keskasutuse puudumisel. Arutame, kuidas täidetakse peatükis 1.5.3 toodud kolme tehingutingimust ning loome aluse raamatu teise, palju tehnilisema osa jaoks. Hiljem keskendume bitcoini süsteemi päritolule, arengule ja poliitilistele omadustele ning analüüsime valmisolekut maksta bitcoinide eest. See peatükk sobib hästi lühikese kokkuvõtte kui ka põhjaliku ülevaatena, mis tõstab esile bitcoini süsteemi uuenduslikku olemust.

2.1 Bitcoini esmane liigitus

Bitcoin on laiahaardeline kontseptsioon, mis võimaldab erinevaid tehnoloogilisi komponente sidudes väärtusühikuid konkurentsi põhimõttel luua, virtuaalselt monitoorida ja detsentraalselt kaubelda. Süsteem avab seeläbi uue kontrollmehhanismide kombinatsiooni ja suudab luua rahaühikuid, mis erinevad oluliselt kaup-, sula- ja arveldusrahast (vt joonis 7).

Sellise kombinatsiooni teeb eriliseks see, et ühendatakse virtuaalraha eelised ostmisel-müümisel ja sõltumatust süsteemist tingitud tehingute detsentraliseeritus.



Joonis 7. Rahaühikute kontrollstruktuuride maatriks

Mõiste „bitcoin“ on mitmetähenduslik. Seda kasutatakse üldise süsteemi kui ka mõnede selle alamkomponentide kirjeldamiseks. Sinna alla kuuluvad bitcoini võrgustik, bitcoini (kommunikatsiooni-)protokoll ja bitcoini (raha-)ühikud. Täpsemalt suhtlevad bitcoini võrgustiku osalejad bitcoini protokolli standardvormis, kus nad ostavad-müüvad bitcoini ühikuid.

Bitcoin termini mitmetähenduslikkus tekitab aeg-ajalt segadust ja takistab seega süsteemist arusaamist. Seetõttu pöörame tähelepanu terminoloogia täpsele piiritlemisele. Kasutades terminit *bitcoin* ilma täiendita, mõeldakse bitcoini süsteemi või bitcoini tehnoloogiat. Kui räägime ühest samanimelisest alakomponendist, siis kasutame alati täiendeid *võrgustik, protokoll* ja *ühik.*

2.2 Bitcoini süsteem

Unikaalsete [13] kontrollmehhanismide kombinatsiooni (joonis 7) võimaldamiseks ühendab bitcoini tehnoloogia erinevad alamkomponendid üheks innovaatiliseks terviksüsteemiks. Joonis 8 näitlikustab süsteemi ülesehitust ja komponente.

[13] vt märkus 2.1

Joonis 8. Ülevaade bitcoini tehnoloogiast (teh.=tehingu)

Bitcoini ühik. Bitcoini ühikud (ka bitcoinid) on virtuaalsed rahaühikud süsteemis. Neid ei ole füüsiliselt olemas ja neid ei saa saata failidena. Bitcoini ühikud on pigem nagu registrisissekanded, mida omistatakse kindlale isikule.[14]

Bitcoini võrgustik. Bitcoini võrgustik on täiesti detsentraliseeritud. See hõlmab kõiki osalejaid ja nende sidemeid ning on peamine sidevahend teabe vahetamiseks ja konsensuse saavutamiseks.

Bitcoini protokoll. Bitcoini protokoll määrab, kuidas side peab bitcoini võrgustikus toimuma. Eelkõige sisaldab see mis tahes liiki sõnumite vormindamise standardseid juhiseid.

Asümmeetriline krüptograafia. Asümmeetrilist krüptograafiat kasutatakse tõendamiseks ja kontrollimiseks. See võimaldab bitcoini võrgustiku kõikidel kasutajatel kontrollida mistahes tehinguteate legitiimsust.

Blockchain. *Blockchain* (edaspidi plokiahel) koosneb avalikust registrist. Iga inimene saab seda registrit vaadata, koopiat alla laadida ja seda muuta. Otsustavaks teguriks on ainult selline versioon registrist, kus (1) on ainult tõestatud legitiimsed tehingud ja (2) mida peetakse konsensuslikult kõige ajakohasemaks versiooniks. Viimane tingimus tehakse kindlaks *konsensusprotokolli* kaudu. Selleks kasutab bitcoini plokiahel printsiipi, mis sai tuntuks *Proof-of-Work* (töökinnitus) nime all.

2.3 Eristumine olemasolevatest süsteemidest

Registri kasutamine ei ole omane ainult bitcoini tehnoloogiale. Nagu lõigus 1.5.2 seletatud, põhineb enamik virtuaalseid rahaühikuid registritel. Näiteks ei kujuta arveldusraha endast midagi muud, kui registril põhinevat nõuet päris (sula-

[14]Täpsemalt, kindlate bitcoini ühikute tulevane edastamine on seotud tingimusega, mida saab täita ainult konkreetne isik või teatud rühm inimesi.

)rahaühikutele, mis esitatakse elektroonselt.[15] Sel juhul juhib registrit keskasutus, mis tagab sisuliselt tehinguvõimekuse, -legitiimsuse ja -konsensuse.

Tehinguvõimekus tagab omaniku võimekuse algatada oma vahenditel põhinevat tehingut. Pangandussüsteemis teostatakse seda infrastruktuuri kasutamise võimaluse kaudu. Kommertspangad rajavad filiaalivõrgustiku, aktsepteerivad kirjalikke maksekorraldusi ja hõlbustavad klientidega algatatud suhtlust terminalide, koduarvutite ja muude elektrooniliste kanalite kaudu. Kui keskasutus kaob, kaob ka vastav infrastruktuur. Seetõttu peab bitcoini süsteemis olema muu võimalus, mis võimaldaks osalejatel tehinguid siiski algatada.

Võrgustiku liikmete kommunikatsiooniga kaasneb ka *tehingulegitiimsuse* kontroll. Keskasutus on kohustatud tuvastama tehingu algataja ja tagama, et tegu on vastava väärtusühiku tegeliku omanikuga. Identifitseerimine toimub tavaliselt allkirjade ja PIN-koodide kontrolli või dokumentide või biomeetriliste tuvastamisprotseduuride abil. Kõik need kontrollmehhanismid põhinevad asjaolul, et keskasutus teeb esmalt kindlaks juurdepääsu kriteeriumid ja vajaduse korral neid võrdleb. Selle asutuse puudumisel peab tehingulegitiimsuse kontroll ka teisiti toimuma.

Tsentraliseeritud süsteemide ainuõigusliku raamatupidamisõiguse automaatseks tulemuseks on üks selge register. Kui registri ainsaks raamatupidajaks on keskasutus, siis eksisteerib ainult üks registriversioon. Seoses sellega on tsentraalsetes süsteemides tagatud *tehingukonsensus.* Teisest küljest, kui ainuõigus ei realiseeruks, tekiksid registrist erinevad, põhimõtteliselt võrdsed, versioonid ja tekiks küsimus, kuidas saab jõuda konsensusele, milline neist registriversioonidest on kehtiv.

Bitcoini tegelik innovaatilisus seisneb seega teadlikus keskasutuse loobumises. Teisalt võib see ära hoida süsteemseid sõltuvusi. Bitcoini omanikud võivad neid sõltumatult ja piiramatult käsutada, ilma et nad peaksid toetuma kindlale kolmandale instantsile. Teisest küljest teeb keskasutuse puudumine ka palju keerulisemaks *tehinguvõimekuse* tagamise, *tehingulegitiimsuse* kontrolli ja *tehingukonsensuse* saavutamise. Kui puudub vastav asutus, kes neid tingimusi kontrollib, peab kolme tehingutingimuse täitmine olema tagatud alternatiivsete vahenditega. Neid põhimõtteid kirjeldatakse järgmises lõigus.

[15] Sula- ja arveldusraha ei ole samaväärsed. Kuigi sularaha kuulub kullakatteta raha kategooriasse, hõlmab usaldusraha ainult lubadust välja maksta kullakatteta rahaühikuid.

Märkus 2.1

Eristumine Yap-süsteemist

Märkuses 1.10 leheküljel 38 esitlesime Yapi saarte rahasüsteemi. Näitasime, et väärtusühikud eemaldatakse veskikividest, ehk virtualiseeritakse, nii et süsteemi saab hallata kaudse registri alusel.

Seoses kontrollistruktuuridega on Yap-süsteem samas kategoorias nagu bitcoin. Veskikivide väärtusühikud on virtuaalsed, luuakse konkurentsitingimustes ja tehinguid käsitletakse detsentraliseeritult.

Suur erinevus kahe süsteemi vahel on see, et bitcoini saab rakendada keskkonnas, kus usaldusväärsus ei ole otsustav. Seevastu toimib Yap-süsteem vaid osalejate lähedaste suhete ja väärkäitumise korral sotsiaalse tõrjutuse ohu tõttu. Bitcoin on seega palju paremini skaleeritav ja vabalt ligipääsetav.

Bitcoin loob läbipaistvuse ning muudab kõik tehingud ja registri seisundi matemaatiliselt kontrollitavaks – iga süsteemi osaleja jaoks. Bitcoin töötab seetõttu ilma igasuguste usaldussuheteta ja eristub (vaatamata mõningatele sarnasustele) Yap-süsteemist selgelt.

2.4 Kokkuvõte töö põhimõttest

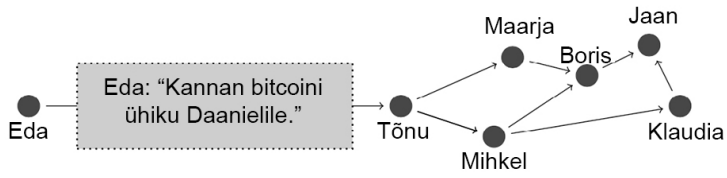
Käesolevas lõigus võetakse kokku bitcoini töö põhimõte, mis põhineb kolmel tehingutingimusel ning kuidas neid detsentraliseeritusest hoolimata saavutada.

2.4.1 Tehinguvõimekus

Süsteemi aluseks on bitcoini võrgustik. See tagab teabe vahetamise ja põhineb peer-to-peer-tehnoloogial. *Peer-to-peer* tähendab, et kõik võrgustiku liikmed on ilma eranditeta võrdsed ja suhtlemine liikmete vahel võib toimuda. Puuduvad keskne struktuur või erivolitustega liikmed.

Tehinguid ja muid konsensuse leidmise teateid saab saata bitcoini võrgustiku kaudu. Näiteks kui Eda saadab Daanielile bitcoini ühiku, loob ta tehinguteate, mis

sisaldab vastavat maksekorraldust. Teade on kirjutatud vastavalt bitcoini protokolli standarditele ja edastatakse ühele võrgustiku liikmele.



Joonis 9. Tehingu algatamine

Joonisel 9 toodud näites jõuab tehinguteade Tõnule, kes teeb teatest koopia ja edastab selle kõigile otsestele kontaktidele, nimelt Maarjale ja Mihklile. Maarja ja Mihkel teevad sama. Edastamist jätkatakse seni, kuni uusi võrgustiku liikmeid enam ei leita.

Kuigi maksekorralduses on saajaks Daaniel, ei pea saatma tehingusõnumit otse Daanielile. See, kas ja millal Daaniel sellest sõnumist teada saab, pole esialgu tähtis. Nagu hiljem näeme, ei pea Daaniel isegi (otseste) võrgustiku liikmete hulka kuuluma. Tähtis on ainult, et suur osa võrgustiku liikmetest on tehingust teadlikud.

Ühelt poolt toob bitcoini võrgustiku detsentraliseeritud ja dünaamiline topoloogia kaasa süsteemi märkimisväärse vastupidavuse. Üksikute liikmete äralangemisi saab kergesti kompenseerida ning suhtlemist võib jätkata alternatiivsete teede kaudu. Kui keegi soovib tehingut algatada, siis piisab sellest, kui edastada tehinguteade igale võrgustiku liikmele ja oodata selle edastamist. Kui edastamine ebaõnnestub, saab tehinguteadet teistele võrgustiku liikmetele uuesti saata. See põhimõte tagab tehinguvõimekuse igal ajal.

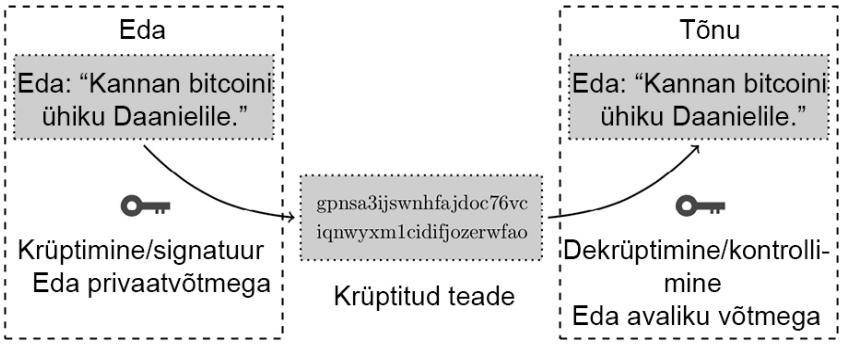
Teisest poolt peab suhtlemine bitcoini võrgustikus toimuma ilma turvaelementideta. Sissepääsu piirangud puuduvad ja liikmed võivad luua mistahes hulga pseudonüüme, mis muudab üksikute liikmete tõrjumise süsteemist võimatuks ja välistab reputatsiooni tekkimist. Sellest tulenevalt peavad liikmed iga sissetuleva teate puhul eeldama, et see on saatja huvides manipuleeritud ja nad peavad olema

võimelised kontrollima selle õigsust. Eriti tehingukorralduste, st registri kohandamist käivitavate teadete puhul, on läbivaatamine otsustava tähendusega.

2.4.2 Tehingulegitiimsus

Kui võrgustiku liige saab tehinguteate, peab ta tagama, et tehing algatati vastava väärtusühiku tegeliku omaniku poolt. Selleks kasutab bitcoin proovitud ja testitud krüptograafilisi protseduure, mida kasutatakse ka e-panganduse rakendustes ja veebipõhises kauplemises.

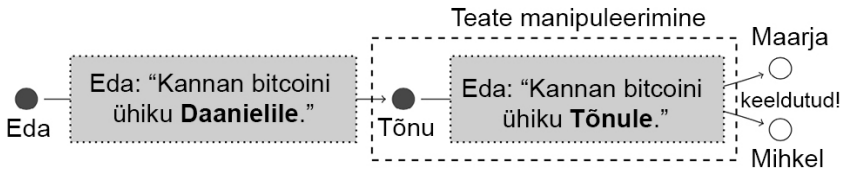
Väärtusühiku omanik on privaatvõtme, millega krüpteeritakse tehinguteade enne saatmist, ainuomanik. Seejärel saab teadet uuesti dešifreerida sobiva avaliku võtme abil. Vastupidi privaatvõtmele on avalik võti teada. Seega saab iga isik selle dešifreerida. Sellega seoses ei käsitle see protsess tehinguteate saladust, vaid pigem selle päritolu kontrollimist. Dešifreerimine õnnestub ainult siis, kui teade tõesti krüpteeriti vastava privaatvõtmega. Seeläbi saab kindlaks teha, kas sõnumi algatajal oli juurdepääs privaatvõtmele. Kuna Eda on ainus isik, kes oma privaatvõtit teab, on võimalik kontrollida, kas Eda on ka tegelikult tehinguteate autoriks.



Joonis 10. Tehinguteate krüptimine ja dekrüptimine

Joonis 10 illustreerib protsessi näite abil. Selle asemel, et saata sõnum Tõnule tavalises tekstis, krüpteerib Eda sõnumi enne selle saatmist. Ta kasutab oma privaatvõtit, kuid hoiab seda alati salajasena. Tõnu saab krüptitud sõnumi ja proovib seda lahendada Eda avaliku võtmega. Kui see õnnestub, teab Tõnu, et teade on varem krüptitud Eda privaatvõtmega.

Tehingu esialgne kontrollimine ei ole piisav. Tehinguteade suunatakse ebaturvalise võrgu kaudu ja seepärast peab iga saaja seda uuesti kontrollima, enne kui ta saab pidada tehingut legitiimseks. Kui Tõnu edastab tehinguteate Maarjale ja Mihklile, siis peavad kaks adressaati ise veenduma edastatud teate legitiimsuses. Eelkõige peavad nad kontrollima, kas maksekorraldus pärineb tegelikult Edalt ja kas teate terviklikkus on täidetud. Kui seda uut kontrolli ei toimuks, oleks Tõnul võimalus teadet muuta (analoogselt joonisele 11) ja Eda nime alt edastatud maksekorraldust manipuleeritud kujul edasi saata.



Joonis 11. Tehinguteate manipuleerimise katse

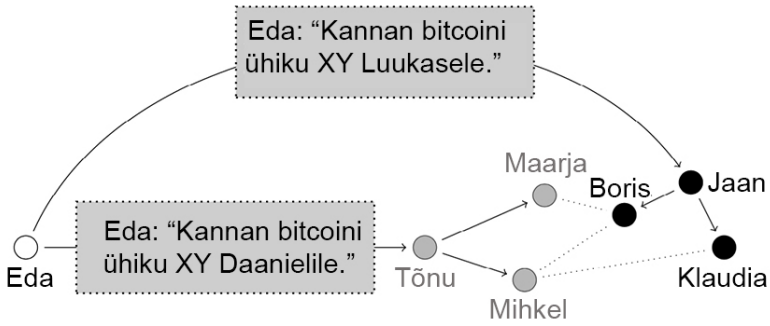
Sellise manipuleerimise vältimiseks aktsepteerivad Maarja ja Mihkel ainult originaalset krüptitud teadet. Omalt poolt kasutavad nad Eda avalikku võtit ja kontrollivad seega sõnumi legitiimsust. Kuna Tõnul ei ole võimalust krüpteerida manipuleeritud maksekorraldust ilma Eda privaatvõtmeta, on Maarjal ja Mihklil kergesti võimalik tuvastada manipuleerimiskatseid nagu joonisel 11 kujutatud. Dešifreerimine ebaõnnestub ja manipuleeritud tehinguteade lükatakse kohe tagasi.

Kui tehingu sõnum on aga legitiimne, läheb see kontrolli teostava võrgustiku liikme individuaalsesse tehingukogumisse. Seal viibib see omamoodi järjekorras, kust seda võib kanda avalikku registrisse.

2.4.3 Tehingukonsensus

Detsentraliseerituse tõttu tekib paratamatult olukord, kus võrgustiku liikmete erinevad järjekorrad erinevad või sisaldavad isegi vastuolulisi tehinguid. Näiteks eeldame, et üks inimene algatab üheaegselt kaks maksekorraldust, edastades samad bitcoini ühikud erinevatele võrgustiku liikmetele. Tsentraalses süsteemis on sellise konflikti puhul valiidne ainult see tehing, mis jõuab keskasutusse esimesena. Kuid bitcoini süsteem loobub selgesõnaliselt keskasutusest. Sellega seoses on olemas võimalus, et

osa võrgustikust saab esmalt teada ainult esimesest tehingust, samal ajal kui teine osa saab esmalt teada teisest tehingust. Mõlemad tehingud on põhimõtteliselt legitiimsed, kuna neid käivitas seaduslik omanik ja nad viitavad olemasolevale väärtusühikule. Kuid kuna kaks maksekorraldust viitavad samale väärtusühingule, on need vastuolus.



Joonis 12. Vastuoluliste tehingute laienemine

Joonis 12 näitab sellise olukorra konkreetset näidet. Eda saadab tehinguteate samaaegselt Tõnule ja Jaanile. Teates Tõnule märgib ta, et soovib üle kanda konkreetse bitcoini ühiku Daanielile. Teates Jaanile viitab ta samale bitcoini ühikule, kuid asendab saaja Luukasega. Mõlemad teated on krüptitud Eda privaatvõtmega ja on seega legitiimsed. Teated salvestatakse erinevate võrgustiku liikmete individuaalsetesse järjekordadesse ja nad saadetakse edasi. Tõnu, Maarja ja Mihkel on arvamusel, et Eda soovib bitcoini ühikut Daanielile üle kanda. Boris, Jaan ja Klaudia aga märkisid tehingu saajaks Luukase ja see sisestati ka nende järjekorda. Et vältida olukorda, kus Eda saab mitu korda kasutada sama bitcoini ühikut (Double Spend) ja saavutada konsensus, tohib ainult üks kahest tehingust avalikku registrisse jõuda.

Võrgustiku kui terviku jaoks ei ole oluline, milline kahest konkureerivast tehingust registrisse jõuab. Tähtis on ainult see, et on olemas protsess, mis võimaldab saavutada konsensust ja selgitab, millist tehingut loetakse kehtivaks.

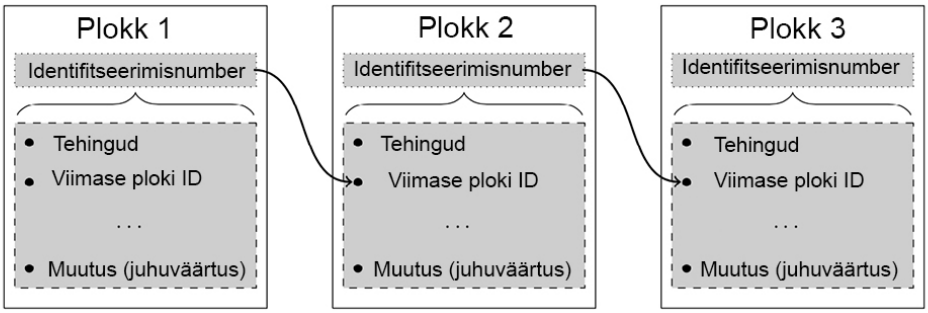
Sel eesmärgil loovad võrgustiku liikmed nn plokid. Plokid on infopaketid, mis sisaldavad vähemalt ühte tehingut. Selliste plokkide loomiseks on vajalik arvutusvõimsus. Iga võrgustiku liige võib vabalt otsustada, kas ja kui palju riistvara ressurssi ta soovib selleks kasutada. Võrgustiku liikmed, kes otsustavad eraldada arvutusvõimsust ja osalevad aktiivselt selles protsessis, tuntakse ka bitcoini kaevandajana. Protsess ise kannab nime bitcoini kaevandamine.

Kaevandaja saab ploki loomiseks kasutada mis tahes tehingut oma järjekorrast. Kuid tehingud peavad olema legitiimsed ja ei tohi konkureerida teise tehinguga plokis. Kui kaevandaja ignoreerib neid kahte tingimust, lükkab ülejäänud võrgustik tema ploki tagasi.

Lisaks tehingutele peab plokk sisaldama teavet *status quo* kohta, st viidet registriolekule, millega plokk on seotud. Seda tehakse teisele plokile viidates, luues kronoloogilise plokiahela (seega nimi blockchain). Joonis 13 näitab sellise ahela struktuuri.

Plokile viitamiseks kasutatakse unikaalset ploki identifitseerimisnumbrit.[16] See sõltub ploki täpsest sisust. Tehingu või ploki muu komponendi muutmine tooks paratamatult kaasa identifitseerimisnumbri muutmise.

Kui ploki sisu ja selle identifitseerimisnumber muutuvad, põhjustab see vastuolu ahela struktuuris, nii et kõik järgnevad plokid, mis viitavad otseselt või kaudselt vastavale plokile, tuleb uuesti koostada. Näiteks kui keegi muudab plokis 1 tehtud tehingut, muutub selle ploki identifitseerimisnumber. Kuna ploki 2 sisendina kasutati ploki 1 vana identifitseerimisnumbrit, tuleb korrigeerida ka ploki 2 viidet. Ploki 2 sisu muutmisel saab see ka uue identifitseerimisnumbri, mis omakorda mõjutab ploki 3 sisu ja identifitseerimisnumbrit.



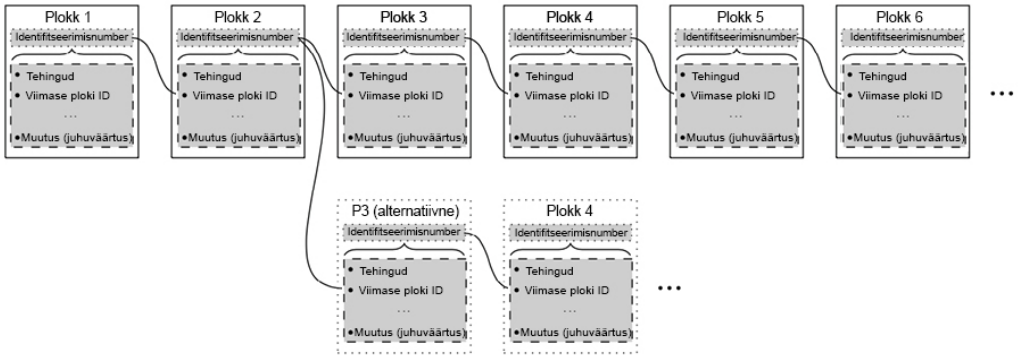
Joonis 13. Plokiahela näide

Konsensuse alusel peavad võrgustiku liikmed ajakohasemaks sellist registrit, kus ahela versioon (1.) sisaldab ainult legitiimseid tehinguid ja (2.) kujutab endast

[16] See on ploki päise räsiväärtus (vt peatükk 4.2). Tehakse lihtsustatud eeldus, et identifitseerimisnumber on ploki osa. Nagu peatükist 5 näeme, pole see täiesti õige. Identifitseerimisnumbrit saab igal ajahetkel ploki sisust arvutada.

pikimat teadaolevat ahelat süsteemis.[17] Sellest tulenevalt saab domineerivat ahelat muuta ainult siis, kui võrgustiku liige suudab taastada kõik plokid, mis on muutunud kehtetuks ja kasvatada alternatiivne ahel pikimaks ahelaks. See on võimalik ainult siis, kui võrgustiku liige kontrollib üle 50% kogu süsteemi arvutusvõimsusest.

Näiteks kui võrgustiku liige soovib joonisel 14 kujutatud ahela kolmandat plokki muuta, peab ta viitama ahela teisele plokile ja looma nii palju uusi plokke, et ta saaks lõpuks üle võtta domineeriva konsensusliku ahela. Kõik teised kaevandajad moodustavad samaaegselt domineeriva ahela ploki 6 põhjal uusi plokke. Ründav võrgustiku liige peab olema võimeline looma uusi plokke kiiremini kui ülejäänud võrgustik kokku. Mida kaugemal on plokk konsensuslikus ahelas, seda rohkem viitavad järgnevad plokid sellele, kas otseselt või kaudselt. See omakorda tähendab seda, et iga kinnituse korral, s.t iga järgneva ploki puhul, muutub ploki manipuleerimine raskemaks. Seeläbi on plokid ahela kaudu kindlalt kaitstud.



Joonis 14. Rünnak plokiahelale, alates plokist 3

Ühe ploki arvutamiseks kulub sekundi murdosa, ka tavalise arvutiga. Esmapilgul võib seda efektiivsust pidada eeliseks. Tegelikult muudaks selline kiire plokkide arvutamine konsensuse saavutamise võimatuks. Uusi plokke loodaks palju kiiremini kui neid saaks bitcoini võrgustiku kaudu edastada ja vahetada. Seega töötaks iga kaevandaja oma individuaalse ahelaga, mis muudaks konsensuse saavutamise võimatuks.

Vastumeetmena on plokkide vastuvõtmine kunstlikult piiratud, nii et võrgustik võtab uue ploki keskmiselt vastu ainult iga kümne minuti järel. Vastuvõtukriteerium põhineb plokkide identifitseerimisnumbritel. Konkreetselt peab uue ploki

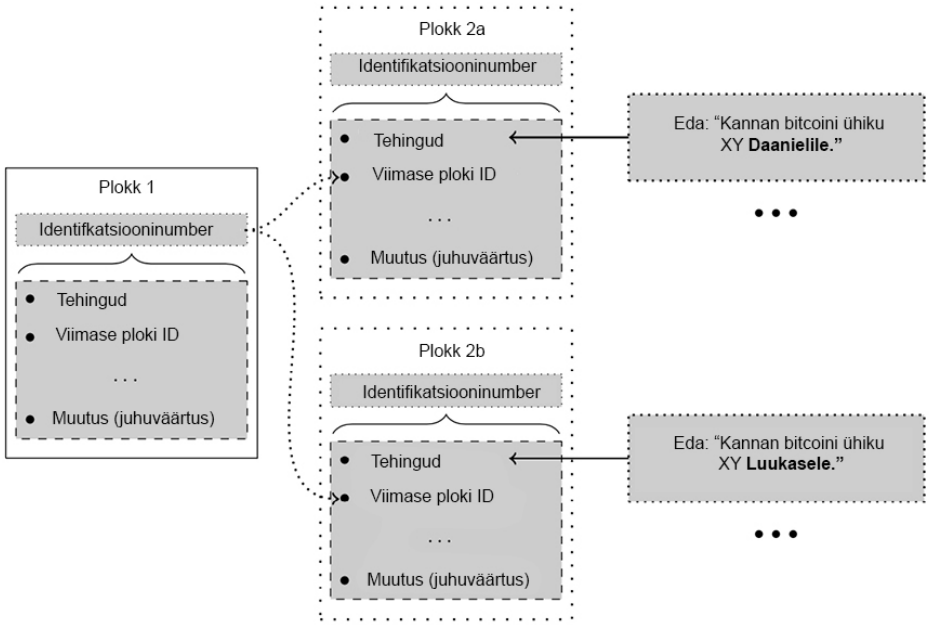
[17] Hiljem näeme, et konsensuse protokoll ka tegelikult eelistab seda ahelat, mille loomiseks oli vajalik suurim arvutusvõimsus.

identifitseerimisnumber olema allpool ettenähtud piirmäära. Alles siis võetakse plokk vastu. Piirmäära korrigeeritakse iga 2016 plokki järel nii (ligikaudu 14 päeva), et saavutatakse kümne minutiline samm, hoolimata üldisest arvutusvõimsuse tasemest.

Identifitseerimisnumbri genereerimiseks kasutatava funktsiooni eripära tõttu ei ole võimalik ennustada, millised sisendid toovad soovitud sihtväärtuse. Võrgustiku liikmed on seega sunnitud proovima erinevaid ploki väärtusi, kuni nad juhuslikult leiavad kombinatsiooni, mille tulemuseks on piisavalt väikese identifitseerimisnumbriga plokk. Selleks, et kaevandaja saaks luua erinevaid identifitseerimisnumbreid, ilma et oleks vaja tehinguid või viidet muuta, lubab plokk *juhuväärtusi* (*nonce*), mida kaevandaja saab proovida ja seekaudu luua palju erinevaid identifitseerimisnumbreid.

Seda katse-eksitus meetodi tuntakse nime all *proof-of-work* (eesti keeles töökinnitus). Kehtivat identifitseerimisnumbrit sisaldav plokk tõendab, et ploki loomiseks kulutati keskmiselt teatud kogus arvutusvõimsust.

Eriti oluline on kulude asümmeetria lahenduse saavutamise ja selle kontrollimise vahel. Sobiva ploki leidmine on väga aeganõudev. Uusi plokke tuleb luua seni, kuni ühel plokil juhtub olema identifitseerimisnumber, mis jääb allpool piirmäära. Keskmiselt kulub kümme minutit kuni üks kaevandaja ühe sellise ploki võrgustiku jaoks leiab. Lahenduse kontrollimine on teisest küljest lihtne, sest väidetavat lahendust sisaldavat plokki saavad kontrollida kõik võrgustiku liikmed paralleelselt ja sekundi murdosade jooksul. Teades, et kõik osapooled kontrollivad plokki, siis kaasavad võrgustiku liikmed plokki ainult legitiimsed tehingud. Sellest kõrvale kalduv toimimine tuvastataks kiiresti, mille tagajärjel ülejäänud võrgustik ei aktsepteeri plokki isegi siis, kui tal on kehtiv identifitseerimisnumber.



Joonis 15. Erinevad tehingud plokikandidaatidega

Pöördudes tagasi joonises 12 toodud näite juurde, peaks selguma, kuidas konsensus saavutatakse. Jaan, Boris ja Klaudia lisavad tehingu Luukase kasuks oma ploki kandidaatide hulka. Tõnu, Maarja ja Mihkel teevad sama, aga Daanieli kasuks. Sõltuvalt sellest, milline kaevandaja suudab esimesena luua ploki, mille identifitseerimisnumber on allpool sel momendil kehtivat piirmäära, jääb üks tehing kehtima ja teine kõrvaldatakse. Sarnaselt joonisele 15 võib ahel areneda mitmes suunas, sõltuvalt sellest, milline kaevandaja loob järgmise ploki.

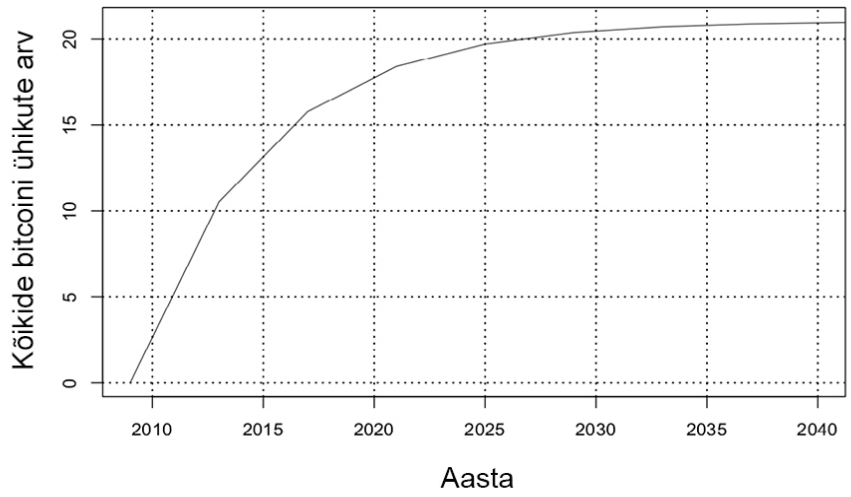
Arvutusvõimsus, mida kaevandajad pakuvad, toob kaasa kulusid. Riistvara tuleb hankida ja hooldada. Lisaks tekivad elektrikulud. Need kulud jäävad kaevandajate enda kanda. Registri haldamine ja valideerimine tuleb aga kogu võrgustikule kasuks. Seega on see protsess üldsuse hüvanguks, mille pakkumine on kasulik kõigile võrgustiku liikmetele. Ilma hüvitist saamata ei oleks keegi motiveeritud oma arvutusvõimsust pakkuma.

Bitcoini süsteem lahendab selle motivatsiooni küsimuse, kompenseerides teatud summa kogu kasust. Igale plokil võib lisada täpselt ühe nn *coinbase'*i tehingu. See tehing genereerib uued bitcoini ühikud selle kaevandaja kasuks, kes ploki lõi. Kui kaevandajal õnnestub luua uus plokk, millel on kehtiv identifitseerimisnumber, siis lisatakse plokk koos *coinbase* tehinguga ahelale.

Kui Boris suudaks luua kehtiva identifitseerimisnumbriga ploki, sisaldaks see plokk Eda ja Luukase vahelist tehingut ja coinbase tehingut Borise kasuks. Kui aga Maarjal õnnestuks luua sobilik plokk, sisaldaks see plokk Eda ja Daanieli vahelist tehingut ja coinbase tehingut Maarja kasuks. Näitena on joonisel 16 kujutatud Maarja ja Borise tehingut.

Nagu ka kõik muud tehingud, aktsepteeritakse coinbase tehingut üldiselt siis, kui see ilmub ahela pikimas versioonis. See annab kaevandajatele indu alati viidata kõige pikema ahela viimasele plokile ja jätkata tööd konsensusliku registriga. Kui kaevandaja otsustab viidata plokile, mis ei vasta konsensuse ahela viimasele plokile, võtab ta teadlikult suurema rahalise riski.

Lisaks motivatsiooni probleemi lahendamisele tagab kaevandamismehhanism bitcoini ühikute loomise. Iga uue plokiga luuakse süsteemi teatud koguses uusi bitcoini ühikuid, millega tasustatakse kaevandajaid. Esimesed neli aastat oli see tasu 50 bitcoini ühikut ploki kohta. Tasu vähendatakse poole võrra iga 210 000 ploki järel (ligikaudu iga nelja aasta tagant) ja hõlmab praegu 12,5 bitcoini ühikut. Bitcoini ühikute kogus on piiratud sellise perioodilise kasvu vähenemise läbi, mis tähendab seda, et mitte kunagi ei saa olema rohkem kui 21 miljonit bitcoini ühikut. Joonisel 17 on kujutatud ringlevate bitcoini ühikute asümptootilist kasvu, mis ligikaudu 2040. aastaks läheneb nullkasvule. Viimased bitcoini ühikud luuakse arvatavasti aastal 2140.[18]



Joonis 17. Uute bitcoinide loomisajakava

[18]Tehingutasud, mis makstakse kaevandjatele, moodustavad makstava hüvitise teise osa. Kui kõik 21 miljonit bitcoini ühikut on loodud, toetub süsteem ainult tehingutasudele.

2.5 Tekkimine, arendamine ja haldamine

Selles peatükis vaadeldakse bitcoini süsteemi päritolu ja selle ebatavalist arengut. Esitatakse bitcoini süsteemi eelkäijad ja näidatakse krüptovaluuta haldus-poliitilisi iseärasusi ja seoseid.

2.5.1 Soov virtuaalraha järele

Esimene samm bitcoin poole toimus 1982. aastal *DigiCash* leiutamisega David Chaum'i poolt. Chaum väitis, et elektroonilised maksevahendid piiraksid oluliselt privaatsust ja jälgitavad rahavood tekitaksid tundlikke andmeid. See probleem motiveeris teda arendama virtuaalset rahaühikut, mis jäljendas sularaha anonüümsust. *DigiCash* põhineb monopoliseeritud rahaloomel ja tehingute tsentraliseeritud töötlemisel, kuid rakendatud krüptograafilise protsessi kommutatiivsus[19] võimaldab süsteemi, milles keskpank rahaühikud pimesi heaks kiidab ning seetõttu puudub teave tsirkulatsioonis olevate rahaühikute seerianumbrite ehk loodud rahaühikute hulga kohta. Selle tulemusena ei saa seerianumbreid ühelegi isikule omistada ja rahaühikuid saab kasutada anonüümselt. Tehingulegitiimsuse kontroll toimub ainult keskpanga heakskiidu kaudu. Tehingukonsensus saavutatakse keskse negatiivse registri kaudu. Kui rahaühikut kasutatakse, tuleb selle seerianumber esitada keskpangale. Kui seerianumber ei ole veel keskpanga registris, siis võib eeldada, et heakskiidetud rahaühikut kasutatakse esimest korda ning on seega kehtiv. Kui sama rahaühikut kasutatakse mitmendat korda, siis oleks vastav seerianumber juba keskpanga negatiivses registris ja seda võidaks pidada *Double Spend* (topeltkulutamise) katseks, mida võidakse blokeerida.

Püüdlus anonüümse virtuaalse rahaühiku järgi suurenes veelgi pärast Tim May Krüptoanarhismi manifesti. Manifest loeti ette esmakordselt Crypto '88 konverentsil, kuid avaldati hiljem kirjalikult. See ennustab sotsiaalseid muutusi, mis on tingitud krüptograafia tehnilistest võimalustest ja võimaldab uut majanduslikku suhtlemist, mis ei alluks kõikvõimsa riigi piirangutele ja repressioonidele. Eelkõige nõuab see virtuaalseid rahaühikuid ja siduvaid lepinguid, mis toimivad anonüümses (või pseudonüümses) keskkonnas.

[19]Erinevate krüpteerimisetappide järjekorda saab vastavalt vajadusele ümber pöörata.

Nähtavalt mõjutatud Krüptoanarhismi manifestist, avaldas informaatik Wei Dai 1998. aastal lühiessee virtuaalse rahaühiku pseudonüümi *b money* kohta. B money süsteemis kasutatakse avalikke võtmeid pseudonüümina, millega saab tehinguid teha. Tehingulegitiimsuse tagab seotud isiku allkiri koos privaatvõtmega. Kõik osalejad (või juhuslik osa) säilitavad eraldi registreid kõigi pseudonüümide praeguste kontojäägi kohta. Puudub konkreetne ettepanek tehingukonsensuse saavutamiseks. B money esitati kui mõttelist eksperimenti, mis eeldab sünkroonset sidekanalit, mida ei saa halvata. Rahaloomeprotsess toimub konkurentsitingimustes matemaatilisi mõistatusi lahendades, mida saab lahendada vaid suure arvutusvõimsuse kaudu, kuid on lihtne kontrollida. Seega on lahendus tõenduseks, et keskmiselt kulutati teatud maht arvutusvõimsust. Sõltuvalt ülesande raskusastme parameetrist võib rahaloomele seada ükskõik milliseid piirkulusid.[20]

Kunstliku kulu idee tuleneb Adam Backi, Cynthia Dworki ja Moni Naori publikatsioonidest ning töötati algselt välja selleks, et võidelda teenustetõkestamise rünnete (DoS) ja rämpsposti vastu. See moodustab ka aluse töökinnitusel põhinevale konsensuseprotokollile, mida kasutatakse bitcoini süsteemis tehingukonsensuse saavutamiseks.

2005. aastal tutvustas Hal Finney korduvkasutatavate tõendite ideed, mis ühendas Wei Dai ja Adam Backi ideed. Hal Finney oli hiljem üheks esimeseks bitcoini kasutajaks ja esimese tõelise bitcoini tehingu adressaadiks.

Samuti aastal 2005 avaldas Nick Szabo blogipostituse Bit Goldi kohta. Artiklis kirjeldatakse *proof-of-work* (töökinnituse) algoritmi kombinatsiooni rahaühikute loomiseks konkurentsitingimustes. Samal ajal kasutatakse arvutusvõimsust avaliku registri tagamiseks, mis muutub refleksiivse viitamise kaudu plokkidest koosnevaks ahelaks. Kuigi Szabo blogipostitust ei mainita Satoshi Nakamoto bitcoini väljaandes, võib eeldada, et Bit Gold on oluliselt mõjutanud bitcoini tehnoloogia arengut.

[20] Wei Dai märgib, et üldiste parameetrite osas kokku leppimine tekitab süsteemis tõsiseid probleeme.

2.5.2 Satoshi Nakamoto

Bitcoin avalikustati 31. oktoobril 2008 autori(te) poolt, kes kasutas(id) pseudonüümi *Satoshi Nakamoto*[21]. Avaldamine toimus krüptograafia postiloendis teadusliku artikli vormis, kusjuures tänaseni ei ole teada, kes end selle pseudonüümi taga varjab.

Kui välja arvata autori isik, on artiklis (ja etalonrakenduses) avalikustatud kõik bitcoin tehnoloogia üksikasjad.[22] Süsteemi esimene looja ei oma süsteemis mingeid erilisi eelisõigusi ning on pärast avalikustamist ja hiljem ka kolmandate isikute arendustöö tulemusel muutunud tehnoloogia seisukohast irrelevantseks. Kuid see ei tohiks mingil juhul vähendada looja saavutust. Siinkohal tuleb märkida, et UCLA (California Ülikool Los Angeleses) professor Bhagwan Chowdhry esitas anonüümse autori Nobeli majanduspreemia nominendiks.[23]

Meedia huvi tundmatu isiku vastu on ka vastavalt kõrge. Internetis on palju oletusi selle kohta, kes võib olla Satoshi. Märkus 2.2 on käsitleb mõningaid hüpoteese.

Märkus 2.2

Kes on Satoshi? - Spekulatsioon

2014. aasta märtsis põhjustas Newsweeki ajakirjanik Leah McGrath Goodman elevust, kui ta teatas laiaulatuslikus ülevaates Satoshi Nakamoto identiteedi eeldatavast tuvastamisest. Ilmselgelt ebapiisavalt uuritud ja hiljem võltsiks tõestatud artiklis väideti, et bitcoini looja oli 64-aastane Jaapani päritolu ameeriklane. Nagu aga selgus, ei olnud mehel nimega Dorian Satoshi Nakamoto kogemusi *peer-to-peer* võrgustike või krüptograafiliste süsteemidega. Kümme päeva pärast Newsweeki artikli väljaandmist avaldas Nakamoto kirjaliku pöördumise, milles ta eitas kõiki seoseid bitcoiniga.

Tegelikult saab bitcoini väljamõtleja olla pärit väga kitsast inimeste rühmast, kuna see eeldab väga spetsiifilist teadmiste ja oskuste pagasit. Paljuräägitud kandidaat

[21] Maskuliinse pseudonüümi tõttu kasutame edaspidi ainsuse vormi. Seda ei tohiks mingil juhul pidada spekulatsiooniks. Rõhutame, et Satoshi Nakamoto pseudonüümi taga peituvate inimeste sugu ega arv ei ole teada.

[22] Githubi hoidik versioonide ja täieliku lähtekoodiga: https://github.com/ bitcoin/bitcoin

[23] Kuna auhindu anonüümsetele üksikisikutele või rühmadele ei anta, võib nominatsioonile järgneda preemia ainult siis, kui Satoshi identiteeti ümbritsev müsteerium on eelnevalt lahendatud.

on Nick Szabo. Arvutiteadlane ja jurist on muu hulgas ka Bit Goldi looja. Lisaks paljudele muudele tõenditele ilmnes ka tekstianalüüsist, et Satoshi Nakamoto kirjutamisstiil on väga sarnane Nick Szabo kirjutamisstiilile. Nick Szabo eitab otsest osalemist bitcoini projektis. Olenemata sellest, kas ta on Satoshi Nakamoto, on tema uurimustöö oluliselt panustanud bitcoini arendamisse.

Uuemad tõendid 2015. aasta lõpust viitavad 44-aastasele austraallasele Craig Steven Wright'ile. Mitmed blogipostitused 2008. ja 2009. aastast seostavad Craigi bitcoini arendamisega; sealhulgas nõudis, et emailid temale krüpteeritaks avaliku PGP[a] võtmega, mida saab seostada Satoshi Nakamotoga. Viited Craig Wrightile on väga vastuolulised ja osati isegi ümber lükatud. Ta ise esialgu ei kommenteerinud, kuid muutis oma seisukohta 2016. aasta mais ja väitis, et on bitcoini looja. Korduvalt leiti, et oletatavad tõendid on võltsid ja Satoshi identiteet on tänaseni lahendamata.

---

[a]PGP (Pretty Good Privacy) on avatud lähtekoodiga krüpteerimisprotokoll, mis põhineb era ja avalike võtmete koostöötamisel.

2.5.3 Bitcoini tehnoloogia poliitika ja haldamine

Kogu bitcoini süsteem, sealhulgas kõik alamkomponendid, on detsentraliseeritud ja täielikult avalikustatud. Puudub keskasutus, ettevõte või isik, kes vastutaks, kes süsteemi töökorras hoiaks või selle edasist arengut määraks. Pigem on bitcoin autonoomne konstruktsioon, mida hoitakse elus kõigi liikmete kaudu. Sõltumatus igasugusest võimalikust asutusest vastab teadlikule disainivalikule ja on võimalik seletus, miks väljamõtleja soovis jääda anonüümseks. Tsentraalselt korraldatud virtuaalsed rahaühikud on regulatiivse sekkumise tõttu sageli ebaõnnestunud. Ilma konkreetse asjaomase asutuseta ei saa sellised sekkumised süsteemi peatada.

Teisest küljest tekitab juhtkonna puudumine palju küsimusi ja takistab süsteemi kaosesse langemist Eelkõige tekivad järgmised kaks küsimust:

1. Mis juhtub, kui avalikustatud tehnoloogia kopeeritakse ja keegi loob oma "bitcoini" ühikud?

2. Kes määrab bitcoini süsteemi edasise arengu ja kuidas saab reageerida puudustele ja kohandada tehnoloogiat?

1. Koopiad – nn altcoinid

Avalikustatud tehnoloogia tähendab, et bitcoini süsteemi saab piiranguteta kopeerida. Igal inimesel on võimalus võtta üle Satoshi lähtekood, seda kohandada ja avaldada süsteemi alternatiivne versioon.

See aga ei tähenda, et lähtekoodi kopeerimise abil saab luua täiendavaid bitcoini ühikuid. Kloonid on uued, selgelt eraldatud alternatiivsed süsteemid, mis põhinevad eraldi registritel. Näiteks võiksime luua *Book Coin*i; bitcoini-tüüpi krüptoväärin just selle raamatu lugejatele. Selliseid koopiaid nimetatakse ka *altcoin*ideks (alternatiivsed mündid). *Book Coin*i võiks olla bitcoini tehnoloogia täpne koopia või muudetud parameetritega.

Uue altcoini loomiseks ei pea uue krüptovääringu looja midagi muud tegema, kui bitcoini lähtekoodi kohandada ja uuesti koostada Kui see takistus on liiga suur, võib kasutada ühte teenuspakkujat paljude seast, kes aitaks parameetrite seadmisega ja käivitamisega lepingupõhiliselt.[24]

Märkus 2.3

Altcoinid ja jalgpall – analoogia

Selle põhimõtte selgitamiseks teeme võrdluse spordiga. Nagu bitcoini tehnoloogia, on ka jalgpalli reeglid vabalt saadaval ja neid saab põhimõtteliselt tahte järgi muuta. Levinumad reeglikohandused hobijalgpallimängudes hõlmavad mänguplatsi ja väravate suurust, mängijate arvu ja suluseisus rakendamata jätmist. Põhimõtteliselt pole kujutlusvõimel piire.

Keegi ei keela lastel mänguväljakul nimetada oma mängu “Meistrite Liigaks” ja mängida vastavalt muudetud reeglitele. Kuid keegi ei mõtle mänguväljaku "Meistrite Liiga" kõrvutamist UEFA miljardi dollari äriga Teatud jalgpalliliigi legitiimsuse ja populaarsuse tagavad teised mängijad, fännid ja sponsorid.

Bitcoin käitub sarnaselt. Igaüks saab luua uusi kloone ja alternatiivseid münte. Reegleid saab üle võtta täpselt või osaliselt. Majanduslikust vaatevinklist on need

[24] Ühe teenusepakkuja näide: https://www.walletbuilders.com

alternatiivid asjakohased ainult siis, kui teiste osalejate jaoks tekib teatud väärtus ja maksevalmidus.

Nüüd on selliseid altcoine juba sadu. Mõnel neist on laiendatud funktsionaalsus või olulised parameetrite erinevused; aga paljud on lihtsalt erineva nimega koopiad bitcoinist. Vaatamata olemasolevate altcoinide suurele hulgale on bitcoin selge number üks krüptoväärtus. Süsteemil on tohutu eelis praeguste võrgustikuefektide tõttu, mille tulemusel on bitcoinil turuväärtus palju kordi suurem kui kõigil muudel krüptovääringutel kokku.[25]

2. Bitcoini süsteemi haldamine ja areng

Bitcoini süsteemi motivatsioonistruktuurid on kavandatud nii, et kehtivaid eeskirju järgides kasvab ka tulu. Vitalik Buterin selgitab seda nähtust Bitcoini Magazine'i esimeses väljaandes. Ta väidab, et bitcoin on esimene arvutivõrgustik, kus pettust ei takista mitte omandiõiguse piirangud, vaid ka asjaolu, et keegi ei saa ühepoolse, normist kõrvalekalduva tegutsemisega oma positsiooni parandada. Standardsed eeskirjad vastavad seega Nashi tasakaalule.

Siiski peab olema teadlik, et bitcoini puhul on tegemist tarkvaraga ja tarkvara on põhimõtteliselt võimalik muuta. Eeskirjade muutmine toimub alati siis, kui piisavalt suur osa võrgustikust lepib ühtlustamise osas kokku ja saab ühiselt kasu *status quo*'st kõrvale kaldumisest.

Bitcoini süsteemi detsentraliseeritud juhtimine vastab kõige keerukamale mitmekihilisele demokraatlikule protsessile. Lõplik analüüs ei ole võimalik ja selle katse ei mahuks selle raamatu kaante vahele ära. Sellest hoolimata tutvustame järgmistes peatükkides teemat lühidalt ja tõstame esile mõningad kõige olulisemad tegurid.

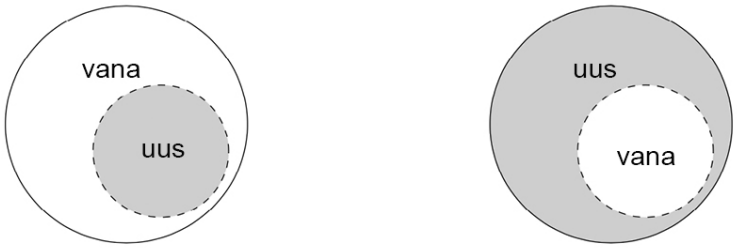
Põhimõtteliselt tuleb rõhutada, et süsteemi dünaamika on otsustava tähtsusega. Staatilist süsteemi ei saa definitsioonist lähtudes kohandada ning seega ei võimalda tegutseda vastavalt muutuvatele keskkonnatingimustele. Näiteks kui turvarisk tuleb ilmsiks, siis saab seda sulgeda, kui tehnoloogia on muudetav. Kuid on ka üksikasjalikemaid põhjuseid, mis muudavad bitcoini süsteemi kohandumisvõimet

[25] Teenus http://coinmarketcap.com säilitab ajakohastatud nimekirja 100 populaarsemast krüptovaluutast, sealhulgas hinna ja turuväärtusega.

ihaldusväärseks. Nende hulka kuuluvad funktsioonide ulatuse laiendamine, pikaajalise stabiilsuse tagamine või uute tehnoloogiate kaasamine.

Selliste muudatuste sisendid ja ettepanekud tehakse detsentraliseeritult erinevate kanalite kaudu ja põhimõtteliselt võib igaüks neid esitada. Nende rakendamist arutatakse tavaliselt avalikult. Eelistatud aruteluplatvormid on foorumid ja postiloendid. Abstraktse idee rakendamiseks on kõige olulisem *Bitcoin Improvement Proposal* (BIP) (Bitcoini parandamise ettepaneku) protsess. BIPid tuleb koostada ettenähtud formaadis, sisaldama nende asjakohasust ja tehnilist kirjeldust.

Kui ettepanek on vastuoluline, nii et vastuvõtmine või tagasilükkamine ei ole konsensuslik, võib toimuda hääletamine. Sellistel hääletustel osalevad ainult kaevandajad. Hääletamine toimub arvutusvõimsuse eraldamise kaudu. Kui kaevandaja loob edukalt kehtiva ploki, on tal lubatud hääletada.[26] Ettepanek võetakse vastu, kui see saavutab eelnevalt kindlaksmääratud intervalli (näiteks viimase 1000 ploki) jooksul ettenähtud jah-häälte protsendi. Tavaliselt on vastuvõtmiseks vaja 55%, 75% või 95% häälteenamust.



(a) Nõrk kahvel (b) Raske kahvel

Joonis 18. Tarkvara kokkusobivus hargnemise puhul

Detsentraliseeritud süsteemis ei saa kedagi sundida hääletamistulemust austama või rakendama. Ilma hääletamistulemuste austamise vajaduseta tähendab iga lahkarvamus süsteemi jaoks lõhestumise ohtu ja võimaldab tekkida niinimetatud *kahvlitel* (inglise keeles *fork*); see tähendab eraldamise punkte, kus üks osa võrgustikust rakendab muudatusi, samas kui teine osa seda ei tee. Kahvlid

[26]Hääled integreeritakse coinbase tehingu (tehing, millega tasustatakse kaevandajat) sisendisse. Kuna tasu taasluuakse ja seega ei vaja tehing sisendit, võib eelmise tehingu viite asemel lisada suvalise stringi.

põhjustavad konkureerivaid registreid, mis vastavalt nende eeskirjadele võivad olla paralleelselt pikimad registriversioonid.

Selleks, et hinnata selliste erimeelsuste tõsidust ja konsensuse taastamise võimalusi, tuleb eristada *pehme* ja *raske kahvli* (*soft fork* ja *hard fork*) vahel (vt joonis 18). Pehme kahvli korral kitsendab uus tarkvara tulevaste plokkide heakskiitmise reegleid, nii et uued eeskirjad kujutaksid endiste eeskirjade alamhulka. Selle tulemusena loetakse uue tarkvara alusel loodud registriversioone kehtivaks ka vana tarkvara all, kuid (enamasti) ei kehti vastupidine olukord. Raske kahvel karmistab eeskirju. Heakskiitmise kriteeriumeid laiendatakse nii, et vanad eeskirjad on uute eeskirjade alamhulk. Selle tagajärjel loetakse (tavaliselt) vana tarkvara poolt kehtetuks uue tarkvara alusel loodud registrid. Vastupidiselt loeb uus tarkvara kehtivaks vana tarkvara alusel loodud registrid.

Kokkuvõttes võib öelda, et pehmed kahvlid sobivad kokku uute tarkvaraversioonidega ja rasked kahvlid vanemate tarkvaraversioonidega. Sarnaselt tabelis 3 esitatuga kaob pehme kahvel, kui uus tarkvara muutub dominantseks, see tähendab, et enamik võrgustiku arvutusvõimsusest järgib just seda.[27] Seevastu saab tugevat kahvlit kaotada ainult vana tarkvara domineerimisega. Kui uus tarkvara kinnistub, jäävad püsima registri kaks erinevat versiooni: üks vanade ja üks uute eeskirjade järgi.

Märkus 2.4

Raske kahvel tarkvara ajakohastamisel

19. veebruaril 2013 avaldati võrdluskliendi *Bitcoin Qt* (nüüd *Bitcoin Core*) versioon 0.8.0.[a] Muu hulgas parandas värskendus eelmise versiooni vea, mis harvadel juhtudel põhjustas kehtivate plokkide kõrvaleheitmist. Seega pikendati uue versiooni vastuvõtuvahemikku.

Kuna kõik kaevandajad ei läinud kohe üle uuele tarkvaraversioonile, põhjustas see 11. märtsil raske kahvli. Loodi uus plokk, mida uus tarkvara pidas kehtivaks, kuid vana tarkvara lükkas selle samaaegselt tagasi. Uue versiooni ahel oli domineeriv, kuid vana

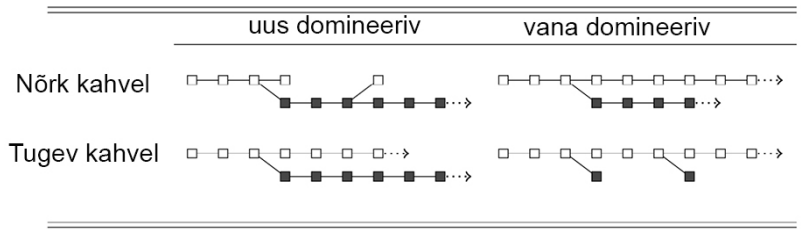
[27] Nõrk kahvel lahendatakse automaatselt niipea, kui uus tarkvara saab enamuse võrgustiku arvutusvõimsusest. Kui registrit laiendab vana tarkvaraga loodud plokk, võib see ajutiselt viia registri mitme versiooni juurde; uue tarkvara kõrgem arvutusvõimsus tagab siiski, et register kasvab vastavalt uutele reeglitele keskmiselt kiiremini. Kuna see register kehtib ka vanade reeglite kohaselt, lülitatakse kõik osalejad sellele versioonile kohe, kui see on pikim versioon.

versioon luges seda kehtetuks. Vastupidiselt oleks uus versioon vana domineerivat ahelat tunnustanud.

Pikemaajalise raske kahvli ärahoidmiseks läksid mõned suured kaevandajad tagasi versioonile 0.7.0, mille ahel sai seetõttu kasvada kiiremini kui konkureeriva versiooni 0.8.0 oma. Nagu tabelist 3 näha, välditi rasket kahvlit vana versiooni kunstliku domineerimisega ning lõpuks toimus kooskõlastatud üleminek tarkvara versioonile 0.8.0.

[a]Uuenduse märked on saadaval https://bitcoin.org/en/release/v0.8.0

Tarkvara kohandusi on seega palju lihtsam rakendada, kui neid saab rakendada pehme kahvli kaudu. Pehme kahvliga on isegi uuendamata võrgustikuressursid kohe uue tarkvaraga kasutamiseks saadaval, kuna toetatakse kogu uut heakskiiduvahemikku. Raske kahvli puhul tuleb aga igat ressurssi eraldi ajakohastada. Alles siis toetab ressurss laiendatud heakskiiduvahemikku.



Tabel 3. Registriversioonide areng nõrga ja tugeva kahvli korral sõltuvalt eraldatud arvutusvõimsusest. Valge = vana tarkvaraga loodud plokid. Must = uue tarkvaraga loodud plokid. Harunemine alates plokist 4.

Kõik eelnevalt käsitletud otsustusprotsessid bitcoini süsteemi edasiarendamise kohta tehakse arvutusvõimsuse eraldamise kaudu. Seda pakub võrgustikus ainult üks grupp: kaevandajad. Bitcoini süsteemi teised osalejad, nagu näiteks tarbijad, kauplejad või investorid täidavad olulisi rolle, kuid ei oma otsest mõju hääletamise ega kahvlite kaotamise tulemusele. Seega võiks väita, et poliitilises protsessis domineerib üks huvigrupp, ning see on palju kritiseeritud punkt. Eelkõige asjaolu, et

kaevandajatel võivad olla omad eesmärgid ja need ei pruugi tingimata kattuda kogu bitcoini süsteemi huvidega, võib põhjustada muret protsessi jätkusuutlikkuse üle.

Osaliselt on kriitika kindlasti õigustatud. Siiski oleks vale väita, et bitcoini süsteemi kontrollivad ainult kaevandajad. Muudel kasutajagruppidel on mitu võimalust, mis kaudselt mõjutavad edasist arenguprotsessi.

Esiteks on kõigil osalejatel võimalus teha ettepanekuid, osaleda aktiivselt poliitilises diskursuses ja mõjutada avalikku arvamust.

Teiseks on kaudne vetoõigus. Muudatuse rakendamine teiste huvigruppide tahte vastu võib põhjustada süsteemset ebakindlust ja ebastabiilset suhet. See omakorda avaldab negatiivset mõju bitcoini ühiku aktsepteerimisele ja turuhinnale, mis võrdub kaevandajate tegeliku tulu vähenemisega.

Kolmandaks, paljud muudatused põhjustavad raske kahvli. Kui pehmed kahvlid on tulevikku ühilduvad, mis tähendab, et isegi saadavalolevad võrgustiku ressursid on kohe saadaval uue tarkvaraga kasutamiseks, nõuab raske kahvel iga ressurssi individuaalset ajakohastamist. Alles seejärel toetavad kaupmehed, kasutajad, võrgustiku sõlmed ja kõik muud ressursid uut heakskiiduvahemikku ning kaaluvad nende alusel tehingute ja plokkide kehtivust. Tänu sellele asjaolule on raske kahvli rakendamine väga keeruline, isegi siis kui see põhineb laialdasel heakskiidul. Kuid kui selline raske kahvel on pealesunnitud, seisneb kaevandajatele oht hallata sellist registrit, kus puuduvad kasutajad, kauplejad või muude ressursid.

Nende kolme võimaluse loend ei ole mingil juhul ammendav. Selle asemel peaks see rõhutama otsuste tegemise keerukust ja näitama, et selles protsessis on kaasatud oluliselt rohkem huvigruppe kui esmapilgult näha võib.

Märkus 2.5

Keskasutused

Bitcoinil ei ole süsteemi detsentraliseeritud iseloomu tõttu ametlikke esindajaid. Süsteem muutub selle fakti tõttu tugevamaks, sest puuduvad kesksed ründepunktid. Kuid detsentraliseeritus raskendab erinevate süsteemiosaliste koordineerimist.

Detsentraliseerituse ebasoodsate asjaolude vastu võitlemiseks on bitcoini süsteemi esindamiseks või isegi juhtimiseks loodud mitu organisatsiooni. Sellised organisatsioonid on väga vastuolulised kahel põhjusel. Esiteks, arvamused soovitud arengu suuna osas sageli eristuvad. See tõstatab küsimuse, kust saab selline organisatsioon oma legitiimsuse ja millises ulatuses oleks sellel võimalik esindada

väga heterogeenset kasutajabaasi. Teiseks on tsentraliseeritud organisatsioonide kokkukutsumine absoluutselt vastuolus bitcoini range detsentraliseerituse põhimõttega. Paljud kasutajad kardavad võimu koondumist ja on vastu sellele, et meedias kujutatakse selliseid organisatsioone bitcoini süsteemi esindajatena. Tegelikult on nende organisatsioonide võim aga väga piiratud. Bitcoini ökosüsteemi mitmed osalejad, sealhulgas kaevandajad, tarbijad, kauplejad ja teenuspakkujad, arendajad, vahetusbörsid ja paljud teised, kes toetavad bitcoini ühikute positiivset nõudlust, peavad heaks kiitma väikesi muudatusi süsteemis. Kui osa ökosüsteemist otsustab läbi viia muudatust ilma kõikide osalejate toetuseta, võib see muutus põhjustada (raske) kahvli ja uue krüptovaluuta.[a]

Järgnevalt käsitletakse mõningaid tuntumaid organisatsioone. Siinkohal tuleks taaskord selgesõnaliselt välja öelda, et ükski neist organisatsioonidest ei ole ametlik bitcoini süsteemi esindaja.

Bitcoin Foundation. Organisatsioon loodi 27. septembril 2012, eesmärgiga edendada bitcoini levitamist, saada süsteemi huvides poliitiliselt aktiivseks ja pakkuda ressursse koolitamiseks. Organisatsioon rahastab end liikmemaksude ja annetuste kaudu ning oli teatud perioodi vältel tööandjaks arendajatele ja lobistidele[b]. Mitmed valed otsused ja majanduslikult ebaõnnestunud konverents viisid organisatsiooni maksejõuetuse lävele. Probleemide ulatus ilmnes 2015. aasta aprillis, kui Olivier Janssens, veidi pärast nõukogu liikmeks valimist paljastas hetkeolukorra avalikkusele. Suur osa tööjõust lasti lahti ja organisatsiooni struktureeriti. Kahjustatud maine ja rahaliste raskuste tõttu on organisatsioonil ainult väike tähtsus.

Blockchain Alliance. Organisatsioon loodi 2015. aastal mõnede bitcoini ökosüsteemi suurimate ettevõtete poolt. Organisatsioon loodi platvormina aktiivseks suhtlemiseks reguleerivate asutustega, et välja töötada ühiseid lahendusi kuritegevuse vastu võitlemiseks. Koostöö eesmärk on võidelda arusaamatuste ja eelarvamuste vastu.

---

[a]Vt näiteks Etherumi tugevat kahvlit ja esialgsete konsensuse eeskirjade taaselustamist Etherum Classic näol.

[b]Sealhulgas libertaarse Cato Institute'i jurist Brian Harper.

2.6 Bitcoini hetkeväärtus

Bitcoin ühikud on vabalt kaubeldavad ja neid saab kasutada kaupade ja teenuste ostmiseks ja müümiseks. Bitcoini ühikuid võtavad vastu arvukad poed, restoranid, baarid, teenusepakkujad ja veebipoed. Lisaks saab bitcoini ühikuid kauplemisplatvormidel teiste vääringute vastu vahetada.

Bitcoini ühiku tegeliku majandusliku hetkeväärtuse määrab turg, s.t pakkumine ja nõudlus, mis peegeldab seega turuosaliste tunnustust ja maksevalmidust.

2.6.1 Bitcoin on *fiat*-raha

Bitcoin ühikud kuuluvad *fiat*-raha kategooriasse, kuna neil puudub fundamentaalne väärtus või maksefunktsioon (vt paragrahvi 1.4).[28] Turuhinna kujunemine põhineb ainult kollektiivsel ootusel, et omandatud bitcoini ühikuid saab teatud hetkeväärtuse eest müüa.

Märkus 2.6

Fundamentaalselt väärtusetu!

Erinevad allikad väidavad ikka ja jälle, et bitcoini ühikutel on fundamentaalne väärtus. Väidetakse, et avaliku registri muutumatus võimaldab alternatiivseid rakendusi. Iga tehingu korral võib registrisse salvestuda väike koguse suvalisi andmeid. Need on kaitstud võrgustiku arvutusvõimsusega ja salvestatakse registris muutmata kujul. Sealt ka küsitav järeldus, et bitcoini ühikut võib vaadelda ressursina, millel on teatud fundamentaalne väärtus.

Ressursi argument ignoreerib olulist punkti. Bitcoini tehnoloogia on täielikult avalikustatud ja seetõttu võib seda vabalt kopeerida (vt peatükki 2.5.3). Põhimõtteliselt võib mõnda muud avalikku registrit kasutada samal viisil. Mis eristab bitcoini registrit kõikidest teistest registritest on kaevandamisprotsessi jaoks eraldatud

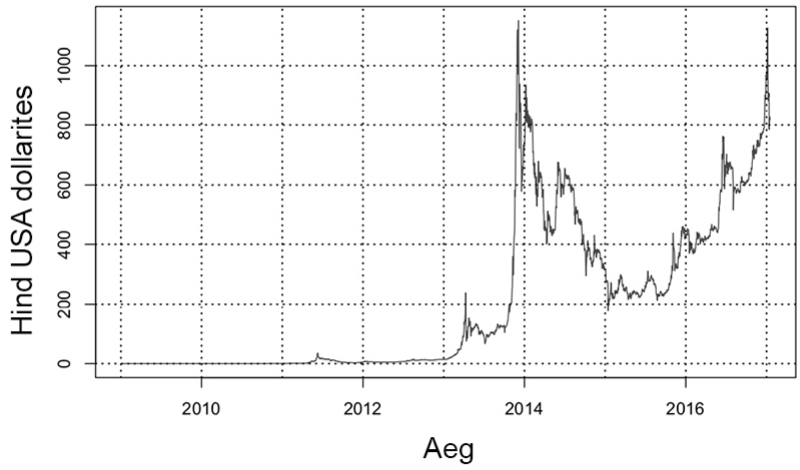
[28] Kullakatteta raha on enamasti välja andnud riigiasutus ning seadusega selle kasutamist toetatakse või sunnitakse. Sellest tulenevalt on mõningaid kullakatteta raha määratlusi, mis nõuavad kullakatteta raha kategooria vajalikuks kriteeriumiks riigiasutusest põlvnemist. Põhimõtteliselt on rahaühiku päritolu tähtsusetu. Finantsteooria vaatepunktist lähtuvalt on kullakatteta rahaühikud iseloomustatud ainult põhiväärtuse ja sellega kaasnevate maksmise lubaduste puudumise kaudu. Järelikult tuleb ka bitcoini ühikud liigitada kullakatteta raha hulka. Rohkemate argumentide käsitlemine bitcoini ühiku liigitamise kohta on toodud lisas 2.6.

suurem arvutusvõimsus. Selle tulemusena suureneb registri turvalisus, kuna rünnakud vajavad ka rohkem arvutusvõimsust.

Lähemal vaatlusel peaks siiski olema selge, et eraldatud arvutusvõimsuse hulk on hinna tagajärg, mitte vastupidi. Kui bitcoini ühiku hind langeb, on ka tulu kaevandajatele väiksem. Arvutusvõimsuse eraldamine mõne teise tegevuse jaoks muutuks atraktiivsemaks, mis jätaks bitcoini võrgustiku ilma paljude kaevandajate arvutusvõimsusest. Seega sõltub "ressurss", mis peaks väidetava põhiväärtuse kindlustama, otseselt hinnast või nõudlusest ning võib täielikult kaduda.

Erinevalt enamikust teistest arveldusvaluutadest, riik ei väljasta ega ei toeta bitcoini ühikuid. Neid ei saa kasutada maksuvõlgade[29] tasumiseks. Omavääringutel, mis kuuluvad samuti arveldusraha kategooriasse, on selline riigipoolne garantii olemas. Lisaks ei ole bitcoini ühikud seaduslikud maksevahendid. Puuduvad eeskirjad, mis kohustavad isikut aktsepteerima bitcoini ühikuid ning tunnustavad bitcoini ühikuid kui sobiliku vahendina võla tasumiseks. Seega ei saavuta bitcoini ühikud seaduslikkust riigi või muu asutuse kaudu, vaid üksnes läbi usalduse tehnoloogiasse.

Seega ei ole üllatav, et bitcoini ühikute algne turuhind oli null ja hinna kujunemist iseloomustas üldiselt suur volatiilsus. Joonisel 19 on näidatud bitcoini ühiku turbulentne hinna areng dollarites alates bitcoini süsteemi loomisest.



Joonis 19. Bitcoinide hinna areng USA dollarites.

[29] Ääremärkus: seaduseelnõu NH HB552, mis oleks võimaldanud New Hampshire osariigis (USA) maksukohustuslastel tasuda maksuvõlga bitcoini ühikutega, esitati 8. jaanuaril 2015 ja lükati tagasi 2016. aasta jaanuari lõpus.

2.6.2 Hinna arengu olulised sündmused

2009

Esimesed bitcoini tehingud sooritati ainult testimiseks. Bitcoini ühikud olid kui elektrooniline mänguraha, millel ei olnud tegelikku majanduslikku väärtust ja mida sageli edastati uutele kasutajatele tasuta.

Aasta jooksul kasvas kasutajate baas ja sellega ka tehingute arv. 2009. aasta keskpaigaks toimus päevas umbes 200 tehingut, ja kuigi bitcoini ühikul ei olnud põhiväärtust ega seotud makselubadust, võimaldas selle piiratud kogus ja vaimustus bitcoini tehnoloogia vastu tekkida omamoodi väärtusel.[30]

Esimene hindamine tehti 5. oktoobril 2009. See arvutati bitcoini loomiseks kulunud keskmise elektrienergia kulu põhjal, mille tulemusena kujunes ühe bitcoini ühiku hinnaks 0,000764 dollarit.

2010

6. veebruaril 2010 loodi *Bitcoin Market,* esimene kauplemisplatvorm, mis võimaldas vahetada bitcoin ühikuid omavääringu vastu. Esimene tehing kauplemisplatvormil toimus 17. märtsil 2010. Platvorm koos foorumite ja IRC (Internet Relay Chat) kanaliga oli turuhinna määramisel otsustava tähtsusega.

Esimene dokumenteeritud kaupade ost bitcoini ühikutega toimus 22. mail 2010. Bitcoini kasutaja laszlo teatas internetifoorumis, et on valmis tasuma kahe Domino pitsa eest 10 000 Bitcoini ühikut.[31] Sel hetkel ei olnud otsene ostmine võimalik, kuna müüja ei soovinud bitcoini ühikuid vastu võtta. Neli päeva pärast kuulutamist leidis laszlo ühe kasutaja, kes oli nõus aitama. Kasutaja jercos maksis oma krediitkaardiga 25 dollarise arve ja sai bitcoini ühikud vastutasuks.

Laszlo pitsad on nüüd saavutanud kultuse ning on oluliseks võrdluspunktiks bitcoini ühikutega tasumise ajaloos. Tehinguga määrati ühe bitcoini ühiku väärtuseks ajaloolised 0.025 dollarit ning pandi alus edasisteks ostudeks krüptovaluutaga.[32]

---

[30] Camera, Casari ja Bigoni (2013) kasutavad kontrollitud eksperimenti, et näidata, kuidas väärtusetud ühikud võivad saada soovitud vahetusobjektiks.

[31] *laszlo* võis seda tehingut hiljem kahetseda. Raamatu väljaandmise ajal oli bitcoini ühikute ligikaudne väärtus 8,2 miljonit dollarit.

[32] Pitsa pakkumise ajal oli hind *Bitcoini Market*il peaaegu kaks korda kõrgem. Erinevad hinnad kinnitavad väga killustunud turgu, millel on väga madal vahetus- ja kauplemismaht.

2010. aasta juulis toimus suur hinnatõus 0.08 dollarini ühe bitcoini ühiku kohta. Samal ajal alustas tegevust tuntud Jaapani Bitcoini vahetusplatvorm *MtGox*. *MtGox* oli algselt mõeldud (interneti) fantaasia kogumiskaardimängu [33] vahetusprogrammi jaoks, kujunes aga siis ühe teise fantaasiamängu veebisaidiks ning 2010. aasta juulis muudeti see lihtsalt bitcoini ühikutega kauplemiseks.[34] Platvormil oli peatselt suur tähtsus ja võimaldas enam-vähem tüüpilist turuhinna kujunemist.

Hind tõusis veelgi ning 7. novembril 2010 oli see lühikest aega 0,5 dollarit, kuid see langes kiiresti 0,2-0,3 dollari tasemele.

2011

Sellele järgnes veel üks märkimisväärne hinnatõus, nii et 2011. aasta 10. veebruaril mööduti dollarist. Hinnatõusu varjutas darknet platvormi *Silk Road* käivitamine, millel oli märkimisväärne mõju bitcoini ühiku varase hinna arengule. Veebisait avaldati internetis 2011. aasta veebruaris ning see võimaldas anonüümset kauplemist mis tahes kaupade ja teenustega, sõltumata igasugustest seaduslikest piirangutest. *Silk Road* kujunes ebaseaduslike ainete ja kahtlaste teenuste *eBay*'ks. Toimus elav kauplemine, kus maksevahendina kasutati eranditult bitcoini.

2011. aasta 10. juunil jõudis bitcoini ühik ajutisele tipptasemele veidi alla 32 dollari, mis ajutiselt peatus *MtGoxi* platvormi häkkimisega 2011. aasta juunis. Ründajatel õnnestus saada kontroll *MtGox* kasutajakontode üle ja teha sihilikult madala hinnaga müügitellimusi. See avaldas märkimisväärset negatiivset mõju usaldusele ja põhjustas järgnevate kuude suhtelise hinnalanguse. Seda sündmust hakati kutsuma *2011. aasta suureks mulliks.*

Samal ajal käivitas Wikileaks bitcoini annetamise funktsiooni, mis võimaldas mõttekaaslastel toetada teenust bitcoini ühikutega. See sündmus on hinnaarengule väga tähtis, kuna see suutis illustreerida bitcoini ühiku otsustavat eelist. 2010. aasta lõpus peatas veebimaksesüsteem Paypal äritegevuse Wikileaksiga, mis raskendas rahaliste vahendite kogumist. Bitcoini tehinguid ei saa blokeerida. See avas Wikileaksile sõltumatu sissetulekuallika. Samas võimaldas bitcoin Wikileaksi pooldajatel annetusi teha.

---

[33] MtGox tähistab Magic: The Gathering Online-exchange.

[34] Veebisaidi arhiivis aadressil https://web.archive.org/web/http://mtgox.com/ saab mõista MtGoxi veidrat arengut mitmete hetktõmmiste põhjal.

2012

9. mail avaldas FBI raporti, mis viitas krüptovaluuta ohtudele, kuid samal ajal väites, et bitcoini ühikud on kurjategijate jaoks lihtsalt veelüks võimalus ning bitcoin eeldatavasti ei asenda olemasolevaid võimalusi. Aruandes selgitati ka seda, et bitcoini tehingud ei ole anonüümsed ja paljudel juhtudel on algataja tuvastamine võimalik. Sellele järgnes laialdane kajastamine meedias.

Aasta jooksul tõusis märkimisväärselt bitcoini ühikute vastuvõtukohtade arv. Suurim makseteenuse pakkuja *Bitpay* teatas 11. septembril 2012, et teeb nüüd koostööd üle 1000 ettevõttega kogu maailmas, sealhulgas paljud restoranid, aga ka mõned ebatavalisemad ettevõtted, nagu hambaarstid ja matusefirmad. 15. novembril lisandus suur rahvusvaheline mängija, blogi hostimise teenus *wordpress*.

Saksa keelt kõnelevas maailmas kujunes bitcoini keskpunktiks Graefekiez piirkond Berliinis. See, mis algas kaks aastat varem üheainsa restoraniga, muudeti alates 2012. aasta novembrist bitcoini ostupromenaadiks, kus oli arvukalt bitcoini vastuvõtukohti.

28. novembril sai see teoks: valmis 210 000. plokk ja seega tasustati ploki loomist esimest korda 25 ühikuga tavalise 50 bitcoini ühiku asemel.[35] Nn *Block Reward Halving* päev oli hinnatõusu perioodi alguseks. Pidevalt kostab hääli, kes näevad seda sündmust järsu hinnatõusu põhjusena. Majanduslikust seisukohast on see hüpotees siiski väga küsitav, kuna kasvumäära poole võrra vähendamine oli prognoositav. Seetõttu tuleks hinnamõjusid eelnevalt hinnata.

2013

2013 oli aasta, mil bitcoin sai äärmise hinnakõikumiste tõttu meedia suure tähelepanu. Bitcoini ühiku turuhind tõusis aasta algul järjekindlalt, möödudes märtsi alguses eelmisest kõrgemast tasemest, milleks oli 35 dollarit.[36]

Märtsi keskpaigas põhjustas tarkvaraviga, mis tekitas registris ajutise kahvli, lühiajalise (päevasisese) üle 20% hinnalanguse (vt märkus 2.4).

Negatiivsed hinnamõjud olid lühiajalised. Poliitilise olukorra tõttu Küprosel[37] ja sellest tulenevalt nõudlusest riigile kättesaamatute alternatiivsete investeeringute

---

[35] Täpsemat infot selle bloki kohta võib leida https://blockchain.info/block- height/210000

[36] Sõltuvalt sellest, millist hinda kasutada pidepunktina, purustati senine tippväärtus juba 28. veebruaril.

järele, tõusis hind 9. aprillil kõrgemale kui 200 dollarit. Kui olukord Küprosel veidi rahunes, vähenes bitcoini hind kiiresti.

Mai alguses tekkisid kuulujutud, et San Diegos on paigaldatud esimene bitcoini töötav sularahaautomaat. Uudisekanali ABC 10 aruande kohaselt lubas masin krüptovaluutat dollari suhtes osta ja müüa. Nagu hiljem selgus, esitleti sularahaautomaati vaid pressikonverentsil. Esimene statsionaarne ja avalikult kättesaadav bitcoini sularahaautomaat käivitati 28. oktoobril Vancouveris. Käivitamine oli äärmiselt edukas – esimesel päeval saavutati viiekohaline käive (Kanada) dollarites.

2. oktoobril suleti *Silk Road* FBI poolt ja saidi väidetav administraator Ross Ulbricht vahistati San Francisco avalikus raamatukogus. Sellest ajast alates ilmuvad saidi reinkarnatsioonid üha uuesti. Bitcoini hind langes lühiajaliselt umbes 20% võrra, kuid tõusis ühe päeva jooksul samale tasemele tagasi ja hakkas uuesti tõusma.

Veidi rohkem kui üks kuu hiljem toimus USA senati kuulamine pealkirjaga "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies". Kutsutud olid mitmesugused eksperdid ja arutati erinevate ametkondade seisukohalt elektrooniliste rahaühikute võimalike riskide kui ka võimaluste üle. Kuulamisele järgnenud päevadel tõusis bitcoini hind dramaatiliselt ja jõudis 29. novembril lõpuks 1216 dollarini.[38] Kuulamise üldist positiivset kulgu ja esimesi samme õiguskindluse tagamiseks peetakse põhilisteks hinna suurenemise põhjuseks.

Teine põhjus, mida sageli loetakse tohutu hinnatõusu põhjuseks, on Hiina investorite suur nõudlus. Seda teooriat toetab eelkõige järgnenud hinnalanguse moment, mis kattus Hiina keskpanga regulatiivse sekkumisega 5. detsembril. Eraisikuid tõkestati rohkem, börside tegevust piirati ja finantsvahendajad jäeti bitcoini ühikutega kauplemisest täiesti välja.

Teisest küljest usuvad mõned analüütikud, et rekordilist hinda ei põhjustanud mitte *Silk Road*i sulgemisest tingitud suurem õiguskindlus ja Senati kuulamine, ega ka Hiina suur nõudlus. On märke selle kohta, et hind oli tingitud peamiselt suurima kauplemisplatvormi *MtGox* petturlikest manipulatsioonidest.

Vaatamata märkimisväärsele langusele aasta lõpus, lõpetas 2013. aasta bitcoini hind võrreldes aasta algusega ligikaudu 5400% kõrgemal.

---

[37] Küprose võlakriis tõi kaasa konfiskeeriva erimaksu, mille kehtestasid EL ja IMF, millega konfiskeeriti osa pankades hoiustatud eravarast.

[38] Hind tol päeval oli peaaegu võrdne kulla untsi hinnaga.

2014

9. jaanuaril 2014 teatas interneti jaemüüja *Overstock*, et võtab bitcoini ühikuid makseviisina vastu, olles sellega esimeseks suurettevõtteks mitmete hulgas. Sellele järgnesid teadaanded satelliittelevisiooni operaatorilt *Dish* (mai), interneti reisibüroolt *Expedia* (juuni), arvuti riistvaratootjalt *Dell* (juuli), meediahiiult *Time Inc.* ja tarkvaratootjalt *Microsoft* (mõlemad detsembris, kuid Microsoft taganes 2016. aasta alguses).

Siiski on ebaselge, mil määral selline aktsepteerimine on mõjutanud bitcoini ühiku hinda. Ühest küljest suurendavad vastuvõtukohad väärtuse õiguspärasust ja meedias kajastamist, seeläbi mõjutades üldist nõudlust positiivselt. Teisest küljest võivad ostud bitcoini ühikutega avaldada negatiivset mõju hinnale, kuna suur kogus bitcoini ühikuid realiseeritakse ostmisega. Kõik suured ettevõtted on sõlminud lepingud *Coinbas*i või *BitPay*ga, mis konverteerivad bitcoini ühikud kohe pärast laekumist vastava riigi vääringusse või need pannakse müüki. Realiseerimise tulemusena paisatakse vastav bitcoini ühik avatud turule, mistõttu pakkumine suureneb ja hind langeb.

Vahepeal on olnud korduvalt probleeme bitcoini ühikute väljamaksega *MtGox*i kauplemisplatvormil. Veebruari alguses peatati lõpuks väljamaksed.[39] Meetme õigustuseks toodi nn *Transaction Malleability* – probleem, mis võib põhjustada tehingute identifitseerimisraskusi ning võib sõltuvalt sisemisest raamatupidamisest põhjustada märkimisväärseid raskusi. Kui *MtGox* kaks nädalat hiljem tegevuse lõpetas ja seejärel hiljem pankrotti läks, siis kaotasid paljud inimesed enamus oma bitcoini ühikutest. Börsil on kadunud kokku poole miljardi dollari väärtuses bitcoini ühikuid. Järgnevatel kuudel on ilmnenud arvukalt vihjeid, et bitcoini ühikute kadumisel ei olnud midagi pistmist oletatava põhjusega.

Lisaks platvormile usaldatud ligikaudu 850 000 bitcoini ühiku kaotusele oli sündmustel ulatuslik negatiivne mõju kogu bitcoini süsteemi mainele, mida ülejäänud suured bitcoini ettevõtted ei saanud hoolimata ühisest pressiteatest kompenseerida. Paljud inimesed seostasid bitcoini ainult *MtGox*iga. Bitcoini ühik kaotas 2014. aastal umbes 60% oma väärtusest.

[39] Maksejõuetuse tõttu pole pressiteadet ametlikul saidil enam näha. Alternatiivsed sekundaarsed allikad on siiski olemas.

2015

4. jaanuaril jõudsid halvad uudised vahetusbörside kohta järgmisse vooru. *Bitstamp*i platvorm häkiti ja varastati 5,1 miljoni dollari väärtuses bitcoine. Järgnes 10% hinnalangus 270 dollarini, mis jätkus ka pärast lühikest taastumist, mille tulemusena oli jaanuari keskel bitcoini ühiku hind 200 dollarit.

Pärast nõrka aasta algust kõikus Bitcoini ühik esimese kolme kvartali jooksul hinnavahemikus 200-300 dollarit. Üldiselt iseloomustasid seda aastat suured riskikapitaliinvesteeringud. Näiteks tuleks välja tuua bitcoin ettevõte *21 Inc*, mis sai märtsis ligikaudu 116 miljonit dollarit riskikapitali. Ainult 2015. aasta jaanuarist kuni oktoobrini ulatusid avalikkusele teada riskikapitaliinvesteeringud bitcoini ja plokiahela ettevõtetesse peaaegu poole miljardi dollarini. Teisest küljest avaldas New Yorgi kehtestatud BitLicense'i määruse lõplik versioon suure tõenäosusega juuni algusest alates pärssivat mõju edasistele investeeringutele kui ka bitcoini ühiku turuhinnale.

Oktoobris algas hindade järsk tõus, mille tulemusel tõusis bitcoini ühiku turuhind üle 400 dollari. Muuhulgas võis selle kasvu tingida rangem kapitalikontroll Hiinas ja Euroopa Kohtu 22. oktoobri otsus vabastada käibemaksukohustusest Kuid Satoshi Nakamoto identiteedi uutest kuulujuttudest tulenev suurenenud meedia tähelepanu võis samuti vähemalt osaliselt tõusu põhjustada (vt märkus 2.2).

Novembris toimunud IS-i terrorirünnakud Pariisis põhjustasid mitmeid meediakajastused mis ühendasid bitcoini terrorirühmituste rahastamisega. Tegelikku riski hinnati Ühendkuningriigi rahandusministeeriumi aruandes väikeseks. Hinnale ei olnud märgatavat mõju.

Bitcoini ühiku hind aasta lõpuks oli 430 dollarit.

Märkus 2.7

Suurenev huvi plokiahela tehnoloogia vastu

Paljud suured ettevõtted käivitasid 2015. aastal oma bitcoin tehnoloogia uurimisprojektid, sealhulgas UBS, IBM ja Nasdaq. Enamasti välditi mõistet bitcoin ja kasutati alternatiivseid plokiahelaid nagu Ethereum, mis töötab bitcoini plokiahelast eraldi.

Projektid on peamiselt seotud väärtpaberite kulutõhusa kauplemise ja kiire töötlemisega, isejõustuvate lepingutega (Smart Contract/nutileping), samuti võimalike rakendustega seadmete võrgustikku ühendamisel väga kiidetud asjade interneti kaudu.

Kuidas huvi plokiahela tehnoloogia vastu on mõjutanud bitcoini ühiku hinda, saab vaid spekuleerida. Ühelt poolt suurendavad need rakendused huvi tehnoloogia vastu. Teiselt poolt kahjustavad alternatiivsed plokiahelad bitcoini plokiahela domineerivat positsiooni.

2016

Aasta algas Bitcoini hinna väiksema langemisega, mis asendus ühtlase tõusuga. Märtsis ja aprillis põhjustas segadust vahetusbörsi *shapeshift.io* häkkimine. Teenust saboteeris töötaja (serveri infrastruktuuri juht) ja seejärel varastati sealt mitu korda. Kokku varastati peaaegu 200 000 dollari väärtuses erinevat krüptovaluutat. *Shapeshift.io* ärimudeli tõttu ei põhjustatud kahju klientide varale. Nende sündmuste ajal jäi bitcoini hinna areng suhteliselt stabiilseks ja aeglane kasvutendents jätkus.

Mai lõpus toimus plahvatuslik tõus, mis ulatus 70%. Sellele järgnes korrektsioon, kuni juunikuu keskpaigaks oli hinnaks 600-700 dollarit. Tõsise hinnatõusu potentsiaalsete käivitajana sel momendil võimalikuks peetud ja hiljem toimunud briti ELi referendumist (*Brexit*) tingitud turu ebakindlust ning samuti juuli alguses toimunud *Bitcoin Reward Halving Eventi*.

18. juunil, vahetult enne Brexiti referendumit, saavutas Bitcoin 780 dollariga kõrgeima hinna peale kahte aastat.

Augusti alguses rünnati edukalt Hong Kongis baseeruvat suurt vahetusbörsi *Bitfinex* ning varastati 60 miljoni dollari väärtuses bitcoine. Kui vargus sai teatavaks, oli bitcoini hind juba languses. Võib eeldada, et uudised häkkimisest mõjutasid hinda veel rohkem negatiivselt ja välistasid võimaliku hinnakorrektuuri. Hind langes kohati tunduvalt alla 600 dollari.

Kui esimene suur paanika möödus ja sai selgeks, et suudeti vältida *Bitfinex*i maksejõuetust, algas pidev tõusutrend. Hinnatõusud võisid olla põhjustatud ebakindlusega seoses USA presidendivalimiste ja Hiina aktiivsuse suurenemisega. Teiseks potentsiaalseks hinnatõusu põhjuseks võisid olla kullapiirangud Indias, mis vastavalt aruannetele suurendasid huvi bitcoini vastu.

2017

Aasta alguses jätkus tugev hinnatõus. Hind tõusis ajutiselt üle 1100 dollari, kuid seejärel toimus järsk korrektsioon. Hinnalangus toimus paralleelselt Hiina keskpanga pressiteatega, milles teatati, et bitcoini vahetusbörsidele rakenduvad tulevikus rangemad eeskirjad. Hiina keskpank väljastas Hiina peamistele vahetusbörsidele *BTCC, OKCoin* ja *Huobi* kohtukutsed.

Selle raamatu trükkimise ajal (15. jaanuar 2017) oli bitcoini ühiku hind ligikaudu 820 dollarit.

5.3 Bitcoini kaevandamine: stiimulid ja näited

Selles peatükis vaadeldakse arvutusvõimsuse eraldamist ja uuritakse konsensusprotokolli teatud osade individuaalset stiimuli vastavust/algatuse kooskõla. Keskmes on küsimus, kuidas kaevandajad käituvad ja millised on võimalused kasumi maksimeerimiseks. Lisaks näidatakse mitmesuguseid rünnakute stsenaariume.

5.3.1 Arvutusvõimsuse eraldamise majanduslikud kaalutlused

Eraldatud arvutusvõimsuse hulk sõltub selle kulude struktuurist ja eeldatava tasu reaalsest majanduslikust ekvivalendist.

Kulusid mõjutavad peamiselt olemasoleva riistvara tõhusus ja hoolduskulud nagu hooldus, elektrienergia või jahutus. Sellest tuleneb teatud arvu räsiväärtuste arvutamise hind: niinimetatud piirkulud.

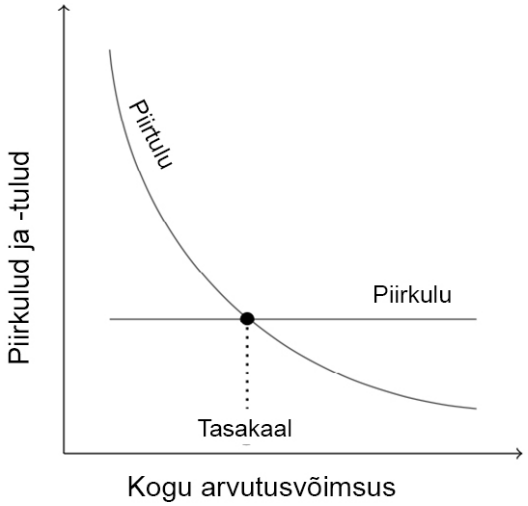
Tasu makstakse bitcoini ühikutes. Seega on reaalne majanduslik ekvivalent otseselt sõltuv bitcoini hinnast. Kui hind tõuseb, suureneb ka tegelik majanduslik tulu. Kui hind langeb, väheneb ka tulu. Lisaks sellele mõjutab teiste kaevandajate arvutusvõimsus saadavat tulu. Selle põhjuseks on asjaolu, et järgmise ploki loomise tõenäosus kaevandaja jaoks on täpselt sama, kui tema enda arvutusvõimsus võrgu üldise arvutusvõimsusega võrreldes.

Kaevandusturgu peetakse väga konkurentsivõimeliseks. Sisenemisbarjäärid on väikesed ja inimeste arv, kes eraldavad arvutivõimsust, on väga suur. Kasum on üldiselt võimalik ainult siis, kui piiratud rühm kaevandajaid saab töötada palju tõhusamalt kui ülejäänud võrgustik. Kui nõuded on homogeensed,[40] jõuab turule täiendavat arvutusvõimsust seniks, kuni oodatav piirtulu ehk täiendava arvutusvõimsuse ühiku tulu vastab selle üksuse piirkulule.

Lihtsuse huvides eeldame, et iga ühiku piirkulu on sama. Mastaabiefektist tingitud piirkulude vähendamine oleks mõeldav, kuid need ei muuda turu põhilist dünaamikat.

[40] Kaevandusturu matemaatiline modelleerimine heterogeensustingimustes on leitav Schär (2015).

Vähenenud piirtulu tuleneb turul valitseva konkurentsi muutumisest.[41] Mida suurem on võrgustiku kogu arvutusvõimsus, seda väiksem on tõenäosus, et ühe arvutusvõimsuse ühikuga luuakse kehtiv plokk. Selle tulemusena väheneb ühe ühiku eeldatav tulu kogu arvutusvõimsuse suurenemisega. Vähenevad piirtulud, piirkulude ja -tulude tasakaal lõikumisel on toodud joonisel 63.



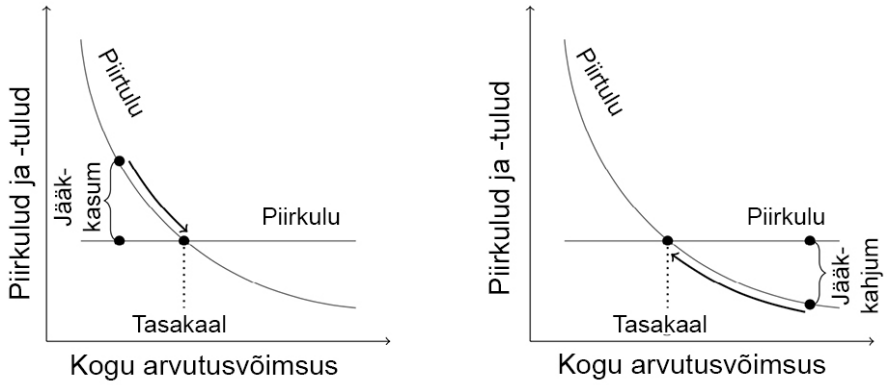
Joonis 63. Arvutusvõimsuse tasakaal

Püsikulud, nagu riistvara hankekulud, mängivad olulist osa turule sisenemise kaalutlustes; kuid kui riistvara on olemas, võib neid kulusid arvutusvõimsuse eraldamise osas eirata. Tähtis on ainult piirtulu ja piirkulude suhe.

Kui võrgustikus ei ole piisavalt arvutusvõimsust, s.t kui arvutusvõimsus on väiksem, kui tasakaal lubada võiks, saab iga arvutusvõimsuse ühikuga teenida tulu. Kuna võrgusõlmed [42] konkureerivad üksteisega ja kõik soovivad saavutada võimalikult suurt tootlust, eraldatakse täiendavat arvutusvõimsust seni, kuni järgneva arvutusvõimsuse ühiku maksumus ületab selle ühiku eeldatavat tulu. Sarnaselt joonisele 64a ühtlustub võrgustik seega tasakaalu punkti juures.

[41] Erinevalt peatükis 1.5.1 esitatud väitele ei tulene piirtulude vähenemine inflatsiooniliste mõjude tõttu. Bitcoini ühikute arvu kasv on seotud ploki loomisele kuluvale kümnele minutile ja seda saab arvutusvõimsuse suurendatud eraldamisega ainult vähe mõjutada.

[42] Eelnevalt kasutati terminit *võrgustiku liikmed.*



(a)muutus liialt madala arvutusvõimsuse eraldamisel

(b)muutus liialt kõrge arvutusvõimsuse eraldamisel

Joonis 64. Võrgustiku kogu arvutusvõimsuse reguleerimine

Arvutusvõimsuse ülepakkumise puhul esineb väga sarnane dünaamika – ehkki vastupidises suunas. Iga eraldatud arvutusühiku maksumus ületab oodatava piirtulu. Seetõttu on igal kaevandajal põhjust vähendada oma arvutusvõimsust, kuni arvutusvõimsus ei anna enam kahjumit. See on tasakaalu puhul nii, mis viib joonisel 64b kujutatud dünaamikale.

Märkus 5.3

Tõhusam kaevandamise raudvara

Kaevandusriistvara efektiivsus on aastate jooksul dramaatiliselt kasvanud. Esialgu oli kaevandamine võimalik ainult arvuti protsessoriga (CPU). Kuna graafikakaart (GPU) on räsiväärtuste arvutamiseks palju parem ja on sageli väga kõrge arvutusvõimsusega, kirjutati peatselt programme, mis lubasid räsiväärtuste arvutamist graafikakaardiga. Niinimetatud *Field Programmable Gate Arrays* (FPGA, väljaga programmeeritavad ventiilmaatriksid) võimaldasid ahelate konfigureerimist ning suurendasid tõhusust veelgi. Alates 2013. aastast on kasutusel peamiselt *Application Specific Integrated Circuits* (ASIC, rakendusspetsiifilised integraallülitused). Need on masinad, mis on spetsiaalselt välja töötatud SHA256 räsiväärtuste arvutamiseks, mille elektrooniline lülitus on riistvarasüsteemi tihedalt integreeritud. Seepärast saab riistvara kasutada ainult ühe funktsiooni täitmiseks, mille jaoks ta on ka optimeeritud.

Kuid pidev riistvara tõhususe kasv ei vii asjaoluni, et võrgustikku on soodsam ülal hoida, pigem eraldatakse süsteemi arvutusvõimsust seni, kuni on saavutatud esialgne kulupunkt. Suurem raskusaste kompenseerib suuremat koguarvutamisvõimsust.

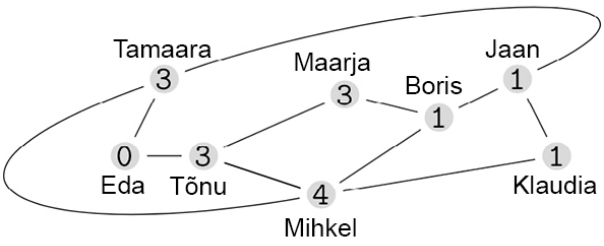
Selle eskaleerumise põhjuseks on kaeveturgude olemus. Konkurentsivõimelises tasakaalus peab teatud ajavahemikus arvutusvõimsuse eest kulutama alati samaväärse rahalise väärtuse, mida on võimalik teenida emissioonitulu ja tehingutasudega. Mis tahes kasumivõimalused meelitavad ligi kaevandajaid ehk rohkem arvutusvõimsust ning seeläbi muudavad kasumi saamise võimatuks. Vastav dünaamika on kujutatud joonisel 64.

5.3.2 Arvutusvõimsuse eraldamise näide

Järgmises näites käsitleme arvutusvõimsuse eraldamist järgnevalt. Me lähtume sellest, et osalejad pakuvad kokku 16 arvutusvõimsuse ühikut ja see väärtus vastab tasakaalukogusele.

Sõlmede arvutusvõimsus on esitatud joonisel 65 vastavas mullis. Tõenäosus, et sõlm võib luua järgmise ploki vastab täpselt samale arvule, mis on jagatud 16 arvutamisvõimsuse ühikuga.

Eda töötab täissõlmes, kuid on otsustanud arvutusvõimsuse eraldamise vastu. Seega on tõenäosus leida kehtiv plokk 0, kuid ta osaleb võrgustikus tavaliselt. Lisaks on ta endiselt võimeline kontrollima kõigi tehingute ja ahela legitiimsust. Kõik teised sõlmed osalevad aktiivselt uute plokikandidaatide loomisel. Mihklil on neli arvutusvõimsuse ühikut ja seega 25% võimalus luua järgmine kehtiv plokk. Ülejäänud 12 arvutusvõimsuse on jaotatud ülejäänud võrgustiku liikmete vahel.



Joonis 65. Arvutusvõimsuse eraldamine kaevandamisel

5.3.3 Ühiskaevandused

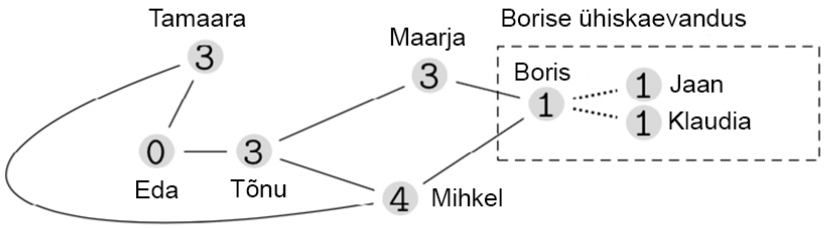
Kui kaevandaja valduses on ainult suhteliselt väike osa võrgustiku koguarvutamisvõimsusest, peab ta taluma pikki perioode ilma tasuta. Kuigi ta saab kasumlikkuse arvutuses arvestada eeldatavate väljamaksetega, ei tea ta kunagi ette, kas ja millal eeldatavad väljamaksed tegelikult toimuvad. Tasu on enam-vähem loterii ja arvutusvõimsus on piletite arv, mille kaevandaja saab. Mida kõrgem on arvutusvõimsus, seda suurem on eduvõimalus – kuid mingit garantiid pole.

Tõenäosuse süsteemil on kaks olulist mõju. Esiteks vähendatakse kaevandajate planeerimise turvalisust. Kuigi kaevandajad saavad küll kulusid plaanida ja arvutada oodatavat tulu, on väljamaksete aeg ainuüksi juhuslikkuse küsimus. Teiseks võib tegelik väljamakse oluliselt erineda eeldatud väljamaksest. See on sageli juhtum, kui arvutusvõimsust eraldatakse suhteliselt lühikese aja vältel. Mõlemad probleemid on tingitud väljamakse volatiilsusest.

Et vältida väljamaksete volatiilsuse probleemi ja oma sissetulekut ühtlustuda, on kaevandajatel võimalus ühineda nn *ühiskaevandustesse*. Vastavad sõlmed koondavad oma arvutusvõimsuse ja toimivad ühe kaevandajana. Kõrgem arvutusvõimsus viib regulaarsemate väljamakseteni, mida saab jagada proportsionaalselt kõigi kaevanduse liikmetega. Seega eeldatav väljamakse jääb samaks,[43] kuid tasumäärade volatiilsus langeb märkimisväärselt, kuna tulud saabuvad regulaarselt ja muutuvad paremini planeeritavaks.

Joonisel 65 toodud näites tegutsevad Boris, Jaan ja Klaudia eraldi kaevandustes. Igaüks neist kontrollib 1/16 kogu võrgustiku arvutusvõimsusest, kui tasu ploki kohta on 12,5 bitcoini ühikut, siis eeldavad kõik kaevandajad 12.5/16 bitcoini ühiku suurust tasu iga 10 minuti järel. Probleem seisneb selles, et kolm kaevandajat ei saa 15 korral 16-st tasu. Erinevate tulemuste võimalikud tasud on 15 x 0 ja 1 x 12,5 bitcoini ühikut, mille tulemuseks on palga kõrge standardhälve 3,125.

[43]Tegelikkuses nõuavad ühiskaevanduste operaatorid protsenditasu. Sellisel juhul väheneb kaevanduse liikmete eeldatav väljamakse. Kuid suurema planeerimise turvalisuse tõttu on paljud inimesed selleks valmis.



Joonis 66. Borise ühiskaevandus

Joonisel 66 moodustavad nad meeskonna. Seetõttu langeb standardhälve 1,68 peale, kuna meeskonna liikmed saavad nüüd kolmel korra kümnest proportsionaalset tasu 12.5/3 bitcoini ühikut. Selline ühinemine ei mõjuta eeldatavat tasu. Seda saab tõestada väga lihtsa näidisvõrrandiga, mis võrdleb eeldatavat tasu üksinda ja meeskonnas kaevandades.

$$12{,}5 \cdot \frac{1}{16} = 12{,}5 \cdot \frac{3}{16} \cdot \frac{1}{3}$$

Loomulikult pole võrrand lihtsalt meie eeskujuks. Kui kaevandaja arvutusvõimsus h, võrgustiku kogu arvutusvõimsus H ja praegune tasu ploki eest R on võrdsed, siis ei mõjuta *ühiskaevanduse* P agregeeritud arvutusvõimsus individuaalset eeldatavat tasu.[44]

$$R \cdot \frac{h}{H} = R \cdot \frac{P}{H} \cdot \frac{h}{P}$$

Tegelikult on perioodid, kus tasu ei saada, isegi pikemad, et paljud soolokaevandajad peaksid ootama kuid või isegi aastaid, et iseseisvalt luua üks kehtiv plokk ja saada selle eest tasu. Sellepärast on bitcoini võrgustikus *ühiskaevandused* ülimalt tähtsad, nii et praktikas tegelevad soolokaevandamisega ainult isikud, kes juba omavad väga suurt arvutusvõimsust.

Ühiskaevandused on ka üks teguritest, mis viivad bitcoini süsteemi hiiliva tsentraliseerimiseni. Kui suur osa võrgustiku arvutusvõimsusest on koondatud vaid

[44] Tugineb eeldusel, et tasakaalumuutuse dünaamikast tulenev P muutus ei mõjuta kogu arvutusvõimsust H.

mõnele üksikisikule, on raamatupidamine de facto tsentraliseeritud. See muudab bitcoini võrgustiku haavatavamaks. Lisaks ei kasuta kaevandusega ühendatud kaevandajad sageli täisõlme (vt ka peatükk 3.2.3). Need on ühendatud *ühiskaevanduse* operaatoriga poolkeskse alamvõrgu kaudu ja saavad kogu kaevandamiseks vajaliku teabe selle kanali kaudu. Tihti nimetatakse selliseid kaevandajaid ka *hasheriteks*, et näitlikustada, et nad arvutavad ainult räsiväärtusi teise poole jaoks ja ise ei loo ploki kandidaate ega otsusta nende plokkide sisu üle.

Joonisel 66 toodud näites puudutab see Jaani ja Klaudiat. Oma otsusega liituda Borise *ühiskaevandusega* loobuvad nad ka oma terviklikust sõlmest ja edaspidi arvutavad räsiväärtusi Borise jaoks. Võrgustik kaotab korraga kaks terviklikku sõlme ja on selle ühinemise kaudu veel ühe suure kaevandaja (kaevanduse operaatori) võrra rikkam, kes kontrollib ligi 20% arvutusvõimsusest.

2. TEEMA TÄHTSUS/AJAKOHASUS

Tänapäeva infoajastul kolib üha rohkem teenuseid internetti: E-kaubandus, E-pangandus, E-turundus jpt. See tähendab, et areng IKT-valdkonnas (info- ja kommunikatsioonitehnoloogia) on olnud väga kiire. Võib öelda, et pea terve elu on internetti kolinud või kolimas. See on üldiselt tervitatav nähtus, sest see avardab tohutult inimeste võimalusi igapäevastel toimingutel, muutes igapäevast asjaajamist efektiivsemaks, mugavamaks ja lihtsamaks. IKT kiire areng on päädinud tehnoloogiaga, mille potentsiaali ja mõjukust võrdlevad mõned internetiga. Selleks on „plokiahel“ (inglise keeles *blockchain*) ja „bitcoin“.

Mis on plokiahel ja bitcoin?

Lihtsalt öeldes kujutab plokiahel endast andmebaasi ning bitcoin plokiahelal põhinevat makseviisi. Kuid mis teeb plokiahelal põhineva andmebaasi nii eriliseks ja innovaatiliseks? Selle mõistmiseks vaatleme plokiahelat ja bitcoini koos. Märksõnad mõlema tehnoloogia paremaks mõistmiseks on **hajutatus**, **läbipaistvus** ja **muutmatus** (Veerpalu & Demchuk, 2017).

1) Hajutatus

Hajutatus tähendab, et andmebaas ehk register eksisteerib mitmes kohas ning on seejuures sünkroonne. Andmebaas ei ole otseselt kellegi oma, seda ei kontrolli mitte ükski organisatsioon või asutus. See on isereguleeriv ja avalik ning toimib tänu arvutikasutajatele, kes tegutsevad P2P-võrgustikus (*peer-to-peer* ehk partnervõrk) ehk inimeselt-inimesele printsiibil (*ibid.*).

2) Läbipaistvus

Kuna andmebaas on avalik ja detsentraliseeritud, siis tähendab see seda, et kõigil on andmebaasile juurdepääs. Pärast 2008. aasta ülemaailmset majanduskriisi kritiseeriti finantsmaailma üldiselt läbipaistmatuses. Keskpankade ja muude finantsasutuste usaldusväärsus langes palju. Plokiahela tehnoloogia põhinebki aga teistel põhimõtetel kui traditsioonilised finantsasutused. Üks põhilisi printsiipe on just vahendaja

eemaldamine kogu protsessist. Usaldama ei pea mitte teenuse haldajat, keda tihti ei saagi usaldada, vaid teenuse alusprotokolle ja detsentraliseeritud haldamist (*ibid.*).

3) Muutmatus

Muutmatus tähendab, et kui tehing on kord plokiahelasse lisatud, siis teda sealt enam ära kustutada või muud moodi muuta ei saa, sest kõik kasutajad saaksid sellest teada. Lisaks ei ole andmebaas tsentraalne, vaid hajutatud, mis teeb selle häkkimise võimatuks. Need faktid lisavad plokiahelale enneolematu turvalisuse (*ibid.*).

Seega võimaldab plokiahela tehnoloogia andmebaasi detsentraliseeritud ehk **hajutatud** haldamist, mis välistab mõne üksiku asutuse kontrolli andmebaasi üle. Kuna andmebaas on avalik ja kõigile ligipääsetav, siis lisandub **läbipaistvuse komponent**, mis varasemalt puudus. Kui teatud arv legitiimseid tehinguid on toimunud, siis lisatakse nad kõik kokku ühte plokki ning see lisatakse avalikku andmebaasi. Tehingute kontrollimise ja andmebaasi haldamisega tegelevaid kasutajaid nimetatakse kaevuriteks või kaevandajateks. Kaevur või kaevandaja võib olla igaüks, kes on nõus oma arvuti ressurssi selleks eraldama. Selle protsessi läbi luuakse ka uusi bitcoine, millega tasustatakse kaevureid. Plokid on omavahel tihedalt seotud, sealt ka nimi *plokiahel.* Tulemuseks on selline **muutmatu** andmebaas, mida reaalselt ei ole võimalik häkkida või kuidagi teist moodi manipuleerida. Just selles seisnebki plokiahelal põhineva bitcoini innovaatilisus.

Olgugi et plokiahela tehnoloogia esmane eesmärk oli pakkuda alternatiivi pankadele ja traditsioonilistele makseviisidele, proovitakse seda integreerida järjest rohkem valdkondadesse peale rahanduse. Plokiahela tehnoloogia on veel võrdlemisi uus, seega on veel vara öelda, kuidas see uus tehnoloogia teatuid valdkondi täpselt muuta saab. Üheks valdkonnaks peetakse kinnisvara. Terve kinnisturaamatu võib plokiahelasse laadida, mis võimaldaks kiirema ligipääsu kinnisturegistritele ja hõlbustaks mistahes kinnisvaratehinguid, muutes neid lihtsamaks, kiiremaks ja odavamaks. Valdkondi, kus asjaajamine muutuks lihtsamaks, kiiremaks ja turvalisemaks on veel teisigi, kuid praeguse seisuga midagi konkreetset välja tuua ei ole võimalik. Areng liigub sinnapoole, et kõiki toiminguid, mis vajavad lepingu sõlmimist, on tulevikus võimalik teostada plokiahela abil.

3. TÕLKIMISE LÄHTEKOHAD

3.1 Lähteteksti tüübi määratlemine ja tõlketeooria

Enne tõlkima asumist on tähtis määrata lähteteksti tüüp. Lähtun siinkohal Katharina Reissi (Reiss, 2004: 163) liigitusest, mis jagab tekstid põhifunktsiooni järgi informatiivseks, ekspressiivseks ja operatiivseks. Informatiivse teksti põhieesmärk on edasi anda teavet, ekspressiivse teksti ülesanne on anda edasi teksti autorile omast väljenduslaadi, sõnakasutust, stiili, sageli edastades sõnumit kunstilisel ja esteetilisel viisil, operatiivse teksti eesmärk on veenmine keelekasutuse kaudu. Reiss lisab, et tekstid ei esinda ainult ühte funktsiooni, vaid funktsioonid pigem kombineeruvad ja ühtivad teksti eri kohtades. Näiteks on ajaleheartiklite ülesanne anda edasi teavet, aga samas ka mõjutada lugejat teatud määral.

Sarnaselt Reissile liigitab Peter Newmark (1988: 39–42) tekstitüübid ekspressiivseks, informatiivseks ja vokatiivseks. Ekspressiivse teksti funktsioonina näeb Newmark teksti autori mõtete väljendamist, hoolimata sellest, milliseid reaktsioone nad lugejates tekitavad. Sellised tekstid on ilukirjandus (lüüriline luule, lühijutud, romaan ja näidend), autoriteetsed seisukohavõtud (poliitilised kõned, dokumendid jne.) ja isikliku sisuga kirjutised (autobiograafia, essee, isiklik kirjavahetus). Ekspressiivse tekstitüübi vastandiks on informatiivne, mille põhifunktsioon on teabe edastamine. Informatiivse teksti tunnusjooned on: 1) formaalne, emotsioonitu ja tehniline stiil akadeemiliste tööde puhul; 2) neutraalne või mitteametlik stiil õpikute puhul, kus tehnilised terminid on määratletud; 3) mitteametlik soe stiil populaarteadusliku kirjanduse puhul, mida iseloomustavad lihtsad grammatilised struktuurid ning mitmekesine sõnavara, mis ühildub mõistete ja arvukate illustratsioonidega, ning standardsed metafoorid ja lihtne sõnavara; 4) väljendusrikas, huvitav ja mittetehniline stiil populaarkirjanduse puhul. Vokatiivse tekstitüübi funktsioon on kutsuda lugejaskonda tundma, tegutsema ja reageerima nii, nagu tekst seda ette näeb. Sellist funktsiooni on nimetatud ka konatiivseks (käitumuslik), instrumentaalseks, operatiivseks ja pragmaatiliseks funktsiooniks.

Sisuliselt lähtuvad nii Reiss kui ka Newmark Bühleri keelefunktsioonide mudelist. Tuginedes just eelmainitud tekstitüübi liigitustele on selle magistriprojekti raames tõlgitud tekst informatiivset laadi, sest selle funktsioon on anda põhjalik ülevaade plokiahela tehnoloogiast ja bitcoinist. Tõlgitud tekst vastab eelmises lõigus

kirjeldatud informatiivse teksti omadustele mitmeti: akadeemilise tekstina on selles läbiv formaalne ja tehniline stiil; samuti esineb paiguti populaarteadusliku kirjanduse tunnusjooni, sest autorid püüavad sisu võimalikult arusaadavalt edastada.

Akadeemilise ja populaarteadusliku stiili segunemine ja/või osaline kokkulangevus ei iseloomusta mitte üksnes tõlgitud Berentseni ja Schäri kirjutist, vaid on osa teadusmaailma trendist, mis on kestnud juba mõnikümmend aastat, nimelt pürgimine lihtsama ja arusaadavama väljenduse suunas. Seda on iseäranis märgata sotsiaalteadustes (sealhulgas käesoleval juhul majandusteaduses), milles traditsiooniliselt oli kombeks keerukas ja lugeja eelnevate teadmiste suhtes äärmiselt nõudlik väljendusviis, mis on aga viimastel kümnenditel asendumas lühema, lihtsama, vähem formaalse stiiliga, mida varem peeti võimalikuks üksnes populaarteaduslikes tekstides. (Clayton, 2015)

Mainitud trendi on mõistlik suhestada tõlketeooriast tuntud *skopose* mõistega. Lühidalt kokku võttes on *skopos*-teooria sisuks arvestada teksti eesmärki. See kehtib nii lähteteksti autori kui ka tõlkija kohta. Berentseni ja Schäri teose „Bitcoin, Blockchain und Kryptoassets" eesmärk on anda arusaadav ülevaade krüptovaluutaga seonduvast üliõpilastele, teistele akadeemilistele töötajatele, aga ka väljaspool akadeemilist maailma teemast huvitatutele, näiteks pankurid, rahandusametnikud või muud finantssektori töötajad, kes soovivad end teemaga kurssi viia. Sellist eesmärki arvestades on Berentsen ja Schär loonud teksti, mis põimib populaarteaduslikust kirjandusest tuntud stiili klassikalise akadeemilise range ja formaalse stiiliga.

Skopos-teooria on tähtis ka tõlkimise seisukohalt, pannes tõlkijat ja/või tõlketeoreetikut analüüsima muuhulgas järgmisi küsimusi: Mis on lähteteksti eesmärk ja kuidas seda määrata? Mis on sihtteksti eesmärk ja kuidas seda määrata? Kas lähteteksti ja sihtteksti eesmärgid on tingimata samad? (Vermeer 2004: 223)

Pöördudes tagasi konkreetse tõlkeprojekti juurde, siis lähteteksti eesmärk, nagu äsja välja toodud, on teemavaldkonna tutvustamine nii akadeemilisele kui ka mitte-akadeemilisele rahandusega seotud publikule. Arvestades teemavaldkonda (krüptovaluutad), on ka sihtteksti eesmärk eesti keeles tõlgituna selgelt sama – anda ülevaade krüptovaluutade olemusest ja rahateoreetilisest taustast akadeemilisele ja potentsiaalselt ka mitte-akadeemilisele publikule, näiteks rahandusega seotud töötajatele. Ehkki lähtetekst on saksakeelne ja kirjutatud saksakeelse „kultuuriruumi" jaoks, siis rahanduse ja eriti krüptorahaga seonduva puhul ei oma kultuuriruum praktiliselt mingit tähtsust. Kaasaegses rahvusvahelises majandusteaduses on

rahateooria universaalselt omaks võetud ja selles puudub kultuuriliselt tingitud tõlgendamisruum. Teatud mõttes võib paralleeli tõmmata matemaatika valdkonna tekstiga – näiteks tekst, mis kirjeldab ruutvõrrandi lahendamise valemit, on täiesti lahus nii lähte- kui sihtteksti keelte kultuurilisest kontekstist.

Seega kui lähtetekstis sisalduv saksakeelne informatsioon muuta eestikeelseks, ei ole ohtu, et tekiks tekstide vahel konflikt. Vermeeri mõistes on tegemist „tekstidevahelise sidususega“:

> To the extent that a translator judges the form and function of a source text to be basically adequate per se as regards the pretermined skopos in the target culture, we can speak of a degree of “intertextual coherence” between target and source text. (Vermeer 2004: 223)

Kokkuvõtvalt on antud tõlkeprojekti näol tegemist selgelt informatiivse tekstitüübiga. Informatiivsete tekstide tõlkimise korral on määravaks just sisu ja mõtte täpne edasiandmine.

3.2 Tõlkestrateegia

Tõlkimine on suuresti otsuste langetamise oskus, mis omandatakse praktilise töö käigus. Otsuseid tehakse tihti alateadlikult ja automaatselt, kõhutundele ja vaistule tuginedes. Sellele vaatamata saab neid otsuseid kategoriseerida tõlkestrateegiateks. Sõltuvalt erinevatest üldistusastmetest ja liigitustest on eri autorid pakkunud välja mitmeid tõlkestrateegiate määratlusi.

Antud tõlkeprojekti juurde asudes pakkus iseäranis huvi ühest küljest Newmarki (Newmark 1988) ja teisalt Pymi tüpoloogia (Pym 2018). Et aga Newmark eristab kokku 17 eri strateegiat, oli praktilistel kaalutlustel nii tõlkimise protsessi käigus kui ka hiljem analüüsides Newmarki liigitusega keeruline töötada.

Selguse ja praktilise kasutatavuse seisukohast tundus sobiv järgida Pymi (Pym 2018) strateegiaid. Võtan järgnevalt kokku selle põhielemendid:

- „autopiloot“ – tõlkija lähtub keeleoskusest ja teiste samalaadsete tekstide tundmisest, terminid saadakse sõnastikest ja teatmikest;
- kopeerimine – lähtekeele sõnade ja/või struktuuri ülevõtmine sihtkeelde;

- perspektiivi muutmine – näiteks formaalse/mitteformaalse isiku, passiivse/aktiivse lausestruktuuri vahetamine lähte- ja sihtteksti vahel;
- tiheduse muutmine – kui tõlkija teeb sihtkeele teksti vähem tihedaks (vähendades üldistusastet) või vastupidi suurendab sihtkeele teksti tihedust, võttes lähtekeele laialivalguva sisu kokku konkreetsemalt või üldistavamalt;
- lõikude järjekorra muutmine – kui tõlkija paigutab teatud tekstiosad teistsugusesse järjekorda;
- kompenseerimine – kui tõlkija kasutab sõna või fraasi tõlkimise asemel teisi meetodeid, et lähteteksti sisu sihtkeeles edasi anda, näiteks joonealuse märkuse, eessõna vms abil;
- kultuuriline vastavus (*cultural correspondence*) – kui tõlkija annab lähteteksti kultuuritaustaga seotud elemendid edasi sihtkeele kultuurile omaste elementide abil, selle asemel et otse tõlkida;
- teksti kohandamine (*text tailoring*) – kui tõlkija lisab või jätab välja sihttekstist teatud lähteteksti osad.

Tõlkimise ajal ja järel siiski selgus, et mitmed antud liigituses toodud strateegiad ei rakendu minu valitud informatiivsele tekstitüübile, vaid on kohased pigem teiste tekstitüüpide puhul (näiteks tihenduse muutmine, lõikude järjekorra vahetamine, kultuuriline vastavus). Sellest tulenevalt võtsin vaatluse alla ja otsustasin oma tõlketöö analüüsil kasutada hoopis klassikalise Vinay ja Darbelnet (2004: 85–90) klassifikatsiooni, mis liigitab tõlkestrateegiad otsesteks ja kaudseteks.

Ehkki töö resultaadis Pymi liigitus ei peegeldu, oli Pymi strateegiatel tõlketöö protsessi eel ja ajal minu jaoks oluline roll. Lähtetekstiga tutvudes ning tõlketegevuse eeltööna püüdsin süsteemselt läbi mõelda, kuidas Pymi kirjeldatud meetodid võiksid rakenduse leida. Praktilise tõlketöö käigus siiski avastasin, et tegelikkuses võtsin tarvitusele üksnes „autopiloodi“ ja kopeerimise võtteid; teisi liigituses toodud meetodeid ei tulnud tõlkimise jooksul rakendada. Samas andis Pymi teoreetilise baasiga tutvumine julgustust seetõttu, et teadsin, et vajadusel oleks olnud võimalus rakendada tehnikaid nagu näiteks tiheduse muutmine, kompenseerimine, teksti kohandamine.

Liikudes edasi Vinay ja Darbelnet (2004: 85–90) otseste ja kaudsete tõlkestrateegiate juurde, annan alljärgnevalt ülevaate mõlemast.

Otsesed tõlkestrateegiad.

- Laenamine/ülevõtt – lähtetekstist sõna või väljendi ületoomine sihtteksti muutmata kujul, märgitakse *kaldkirjas.* Laenamist kasutatakse siis, kui lähteteksti tehnilist terminist/protsessi ei eksisteeri sihtkeeles või kui sihttekstis soovitakse säilitada lähteteksti stiiliefekti. Tegelikult pole otseselt tegu tõlkestrateegiaga, sest midagi ei tõlgita.
- *Calque* ehk kalka – lähteteksti väljendi sõnasõnaline ületoomine sihtteksti. Sisuliselt on tegu neologismiga.
- Sõnasõnaline tõlge ehk metafraas – otsetõlge, mis vastab täpselt sihtteksti idiomaatikale. Sõnasõnalist tõlkestrateegiat saab rakendada siis, kui mõlemad kultuurid või keeled on sarnased.

Kaudsed tõlkestrateegiad.

- Transpositsioon – sõnaliigi muutmine sihttekstis, ilma et tähendus muutuks.
- Modulatsioon – lähteteksti perspektiivi muutus sihttekstis. Seda strateegiat kasutatakse siis, kui eelnimetatud strateegiatega kaasneb sihttekstis grammatiliselt ebakorrektne, mittesobiv, võõrandav ja veider väljend.
- Ekvivalent – sama nähtust antakse sihttekstis teise kujundiga edasi. Kui inglise keeles öeldakse “ouch!”, siis saksa keeles “aua!” ja eesti keeles “ai(a)!”.
- Adaptatsioon – sihttekstis luuakse lähtetekstile sarnane nähtus või situatsioon, seda võib nimetada ka kultuuri ekvivalentsiks.

Vinay ja Darbelnet kohaselt tuleks võimalusel eelistada otseseid tõlkestrateegiaid kaudsetele.

4. TERMINITE ANALÜÜS

Tõlkimise protsess ei tekitanud stiili, lauseehituse ega tähenduste edasi andmise seisukohalt suuri väljakutseid, sest tegemist on akadeemilise, majandus- ja arvutiteadust siduva tekstiga. Nagu eelnevalt kirjeldasin, on tegu informatiivse tekstiga, milles on elemente nii rangelt akadeemilisest kui populaarteaduslikust stiilist. Põhiliseks väljakutseks olid hoopis võtmeterminid ise. Krüptovaldkonna algterminoloogia pärineb inglise keelest. Saksakeelse lähteteksti autorid on otsustanud jätta mõisted samuti otse ingliskeelseks, isegi kui need oleksid põhimõtteliselt saksa keelde tõlgitavad. Seega seisin silmitsi küsimusega, kuidas termineid tõlkida – kas jätta samuti ingliskeelseks, kasutada juba siiani eesti keeles käibivaid mõisteid (juhul kui neid on kirjanduses kasutatud) või luua ise uued. Analüüsis käsitletav terminite valik põhineb kolmel asjaolul: need on teksti sisu seisukohalt olulise tähtsusega; nende puhul on kasutatud erinevaid tõlkestrateegiaid, seega annavad hea läbilõike teooriaosas käsitletu rakendamisest; kolmandaks subjektiivne – need pakkusid mulle isiklikult huvi, inspireerisid mind analüüsima.

bitcoin või Bitcoin

Magistriprojekti keskse termini *bitcoin* kirjaviisi kohta on mitmeid arvamusi. Kas kirjutada *bitcoin* või *Bitcoin*, kas kirjutada kursiivis või mitte. Nii inglise kui ka eesti keeles kirjutatakse *Bitcoin* suure algustähega siis, kui viidatakse *Bitcoin*'i süsteemile, protokollile, tarkvarale või ökosüsteemile terviklikult, väikse tähega kirjutatakse *bitcoin* siis, kui viidatakse *bitcoin*'le kui valuutale, maksevahendile (Drawing the distinction between the uppercase "B" and lowercase "b" in Bitcoin, 2014 & Lätt, 2015) EKI keelenõuvakk sellist eristust ei tee ja soovitab kirjutada tsitaatsõnana *bitcoin* (EKI, keelenõuvakk). Uudiste artiklites ja teistes veebiväljaannetes kursiivi aga eriti ei kasutata ning ei kiputa vahet tegema ka suure algustähe kasutamisel. Ühtne kirjaviis puudub. Sauga (2018) käsitleb seda terminit tsitaatsõnana ning järgib seega EKI soovitatud kirjaviisi. Sarnaselt EKI-le pole Sauga diferentseerinud Bitcoini kui kogu süsteemi ja bitcoini kui maksevahendit vahel. Kuna Sauga raamatu eesmärk on *"*anda keskmisele internetikasutajast eestlasele põgus ülevaade krüptorahast, olla

lihtsaks teejuhiks ning aidata orienteeruda põnevas ja pealtnäha keerulises krüptoraha-maailmas.*"* (Sauga 2018: 9), siis ei ole selline eristamine vajalik.

Mäger (2018) on bitcoini kirjaviisi probleemile teistmoodi lähenenud. Erinevalt Asse Saugast, kes oli raamatut kirjutades autori rollis, oli Kadri Mäger tõlkija rollis. Autori ja tõlkija vabadused ja kohustused erinevad. Kui autor on oma sõnakasutuses ja väljendusviisis suhteliselt vaba, siis tõlkijale sellised vabadused ei laiene. Sarnaselt magistriprojekti raames tõlgitud tekstile oli ka Mägra tõlgitud tekstis Bitcoini ja bitcoini eristus tehtud. Kui mina otsustasin lihtsuse ja selguse huvides sellise eristuse välja jätta, siis Mäger jäi tõlkija rolli kindlaks ja järgis algteksti. Bitcoin kui kogu süsteem ongi *Bitcoin* ja bitcoin kui maksevahend on *bitimünt* (Mäger 2018: 35). Bitimünt on sõnasõnaline tõlge eesti keelde, mida kasutatakse üsnagi tihti. Kursiivis kirjaviisi aga rakendatud ei ole, tegemist on kalkaga ehk tõlkelaenuga.

Selguse mõttes otsustasin mina oma tõlkes kasutada ainult bitcoin, ilma suure või väikse algustähe erisuste ja kursiivita. Selline kirjapilt lubab ka lihtsamat, ülakomata käänamist. See ei pruugi olla just kõige täpsem ja korrektsem viis, aga selguse mõttes kindlasti kõige parem.

Põhjenduseks on otstarbekus ja lugemise mugavus – võtmemõistena tuleb bitcoin tekstis ette niivõrd tihti, et lugeja, kes sihtkeeles ehk siis eesti keeles tekstiga tutvub, võtab selle sõna omaks. Pidev kursiiv tekitaks minu hinnangul lugejas pigem segadust, sest tõmbab iga kord ülejäänud lausest visuaalselt eristudes ebavajalikult tähelepanu ja takistab lausete ja definitsioonide sisule keskendumist. Kui tõlgiksin terve raamatu ja see läheks avaldamisele, siis lisaksingi tööle eessõna, milles sellist valikut (isegi kui see läheb vastuollu õigekeelsusreeglitega) tutvustaksin ja põhjendaksin. Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia laenamine.

Blockchain

Eesti keeles on tunnustatud tõlkevaste *plokiahel.* Sarnaselt eesti keelele saaks selle termini sõnasõnaliselt saksa keelde tõlkida kui *Blockkette*, kuid saksa keeles üldiselt kiputakse ingliskeelseid termineid lihtsalt üle võtma, seda eriti IKT-valdkonnas. Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia kalka.

Nii Sauga (2018) kui ka Mäger (2018) on samuti kasutanud terminit *plokiahel.*

Transaktions-

Lähtetekstis ülitihti esinev sõna. Eesti keeles saaks samuti kasutada võõrsõna *transaktsioon,* millel on veidi rahandusega seotud konnotatsioon ja mis iseenesest sobiks bitcoini kui maksevahendiga hästi. Kuid selle sõnaga moodustatud liitsõnad tunduksid veidi võõrastavad. Lähtetekstis esineb just selle sõnaga palju liitsõnu, millest kolm moodustavad bitcoini töötamiseks vajalikud kriteeriumid: *Transaktionsfähigkeit, Transaktionslegitimität* ja *Transaktionskonsens.* Google´i otsingumootorit kasutades selgub, et kaks viimast terminit esinevad ainult seoses bitcoiniga. Kuna sõnaga *transaktsioon* on minu meelest kummaline liitsõnu moodustada, siis otsustasin kasutada sõna *tehing* ehk siis *tehinguvõimekus, tehingulegitiimsus* ja *tehingukonsensus.* Kahte viimast terminit guugeldades ei leia, esimese kohta on ainult kaks tulemust. Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia sõnasõnaline tõlge.

Sauga (2018) on bitcoinidega kauplemist nimetanud sõnaga ülekanne, mis on minu arvates umbmäärasem variant kui tehing. Eelmainitud *tehinguvõimekus, tehingulegitiimsus* ja *tehingukonsensus* on võetud kokku sõnaga *ülekannete usaldusväärsus* (Sauga 2018: 50), mille all autor mõtleb küll samasid põhimõtteid.
Mäger (2018) on ingliskeelse *transaction* tõlkinud kui *tehing*. Originaalteksti autor Julian Hosp on oma raamatus bitcoini tööks vajalikud kriteeriumid täpsemini välja toonud kui Asse Sauga. Terminite *tehingulegitiimsus* ja *-konsensus* asemel on Mägeri tõlkes kasutatud *tehingute õigsus* ja *konsensus*, mis minu hinnangul ei pruugi olla üheselt terminid, vaid olenevalt kontekstist võivad mõjuda ka pigem üldistavate kirjeldustena. Antud väide kõlab ehk vaieldavalt, sest iseenesest on termin mingi valdkonna üldmõiste sõnaline tähis ja võib küll koosneda ka mitmest sõnast, kuid julgen siinkohal sellisest arusaamast kõrvale kalduda.

Tehingute legitiimsus annab üldsõnaliselt edasi ühte paljudest võimalikest omadustest/kirjeldustest, mida saab nii tehingutele kui ka teistele objektidele omistada. Ei ole ju selge, et erialases kontekstis oleks eraldi võetuna *tehingute*

legitiimsuse näol üldse tegemist mingi kindla mõiste või terminiga. Pigem püütakse teatud nähtuse sisu võimalikult lihtsalt ja arusaadavalt lugejatele edasi anda.

Tehingulegitiimsus väljendab kindlat ja konkreetset mõistet. Samas on ka selge, et kui asendada meie tõlkes *tehingulegitiimsus* sõnadega *tehingute legitiimsus*, siis jääks samuti mõte samaks. Sellest tulenevalt väidangi, et kuigi mitmuses ja lahku kirjutatuna võib teatud kontekstis olla tegemist terminiga, siis see ei kehti universaalselt, sest on mõeldavaid kontekste, milles mitmuses ja lahku kirjutatuna ei teki resultaati, mida saaks vaadelda terminina.

Netzwerkteilnehmer

See oli samuti üks lähtetekstis väga tihti esinevatest terminitest. Esmapilgul selle termini tõlkimine raskusi ei tekita, võiks isegi arvata, et kindel termin on eesti keeles olemas. Esmalt tuleb kindlaks teha, kas terminid *võrk* ja *võrgustik* omavahel erinevad. EKSS defineerib *võrgustikku* kui ruuterite kaudu ühendatud võrkude kogumit ja *võrku* kui arvutivõrku, võrgustikku. Seega tähistavad mõlemad terminid umbkaudselt sama asja, mis tähendab, et mõlemad sobiksid tõlgitava termini konteksti. Sarnaselt EKSSile nimetab ka Duden terminid *Netzwerk* ja *Netz* sünonüümideks, kuid defineerib *Netzwerk*i ka nõnda: grupp inimesi, kes on omavahel ühendatud ühiste vaadete, huvide jms kaudu (Duden *sub* Netzwerk). Kahjuks on *võrgustiku* definitsioon eesti keeles nii napisõnaline, kuid saksa definitsioon aga soodustaks just selle termini kasutamist sellepärast, et *võrgustikud* teenivad kitsemaid huve kui *võrgud,* mis on olemuselt pigem üldisemad. Termini teise poole, *Teilnehmer,* võib tõlkida kui *osaleja, osaline*, mille tulemuseks oleks kas siis *võrgustikus osaleja* või *võrgustiku osaline*, mis tunduvad väga kunstlikud ja mittesobilikud. Paremini sobiksid kas *kasutaja* või *liige,* olgugi et nad ei ole nii täpsed kui kaks eelnevat terminit. *Võrgustiku kasutaja* oleks isik, kes lihtsalt kasutaks bitcoini võrgustikku millegi jaoks, *võrgustiku liige* oleks aga keegi, kes mingil määral ka võrgustikku panustaks, sest liikmesus seab teatud eeldused. Sestap otsustasin *Netzwerkteilnehmer* tõlkida kui *võrgustiku liige.* Kui aga eelistada termini *võrk* kasutamist, siis oleks *võrgukasutaja* hea variant, mis oleks samuti liitsõna nagu lähteteksti termingi, kuid mida seostatakse rohkem energia

valdkonnaga (Esterm *sub* võrgukasutaja). Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia adaptatsioon.

Mining pool

Järjekordne termin, mis on inglise keelest saksa keelde üle võetud muutmata kujul. *Mining pool* tähistab võrgustiku liikmete arvutusvõimsuse koondamist/ühendamist, et suurendada tõenäosust bitcoinide teenimiseks. Levinum eesti keelne vaste on *ühiskaevandamine,* mis tähistab antud tegevust täpselt. Alternatiivsed terminid oleksid *farm, kaevandamise kooperatiiv* ja *kaevanduskett*. Need aga ei tähista tegevuse olemust piisavalt täpselt ja efektiivselt, näiteks kasutatakse terminit *farm* tähistamaks ülisuuri bitcoini kaevandusi, kus on kasutusel sadu kuni tuhandeid kaevandamiseks vajaminevat raudvara (graafikakaart, harvem ka protsessor või bitcoini puhul ainult bitcoinide kaevandamiseks loodud seadeldised). Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia adaptatsioon.

Mining/miner

Termin *mining* tähistab tegevust, millele tugineb kogu bitcoini süsteem. Sellega tegelevad võrgustiku liikmed, kes pakuvad enda arvutusvõimsust *plokkide* loomiseks. *Plokid* on sissekanded registrisse, mis sisaldavad teavet vähemalt ühe tehingu kohta. Selliste plokkide loomine on rahaliselt kulukas, seega saab arvutusvõimsust eraldanud ja sobiva ploki loonud liige vastutasuks bitcoine, mida luuakse just plokkide loomise kaudu. Eesti keeles kutsutakse seda protsessi *kaevandamiseks* ja inimest, kes sellega tegeleb, *miner*iks e *kaevandajaks.* Kui saksa keeles oleks saanud *blockchain*i kohta öelda *Blockkette,* siis selle termini puhul oleks see ilmselt veelgi keerulisem, sest *Bergbau* ja *Abbau* ning *Bergmann*, *Bergarbeiter* ja *Kumpel* lihtsalt ei sobi, kuna otsene seos mäetööstusega on liialt suur. *Kaevandamine* ja *kaevandaja* eesti keeles ei ole küll ehk oluliselt neutraalsemad terminid kui saksa keele vasted, kuid lugeja keeletunnetust arvestades siiski sobivad antud konteksti. Siinkohal tundub, et saksa

lugeja eelistab selgelt uute valdkondade terminite jaoks ingliskeelseid mõisteid ja pigem välditakse olemasoleva saksakeelse terminoloogia kasutamist. Võimalik, et see on lihtsalt trend. Eesti keeles on olemas ka *kaevur* e mäetööline. Bitcoiniga seoses nimetatakse kaevuriteks just raudvara, millega kaevandajad bitcoine kaevandavad. Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia sõnasõnaline tõlge.

Nii Sauga kui ka Mäger on kaevandamiseprotsessi nimetanud *kaeveks*, mis algselt tuleneb aga Riigi Infosüsteemi Ametilt.

Soft fork ja *hard fork*

Terminid tähistavad plokiahela tarkvara uuendamise meetode, muudatusi plokiahelas. *Soft fork* on selline muudatus, mis kitsendab kriteeriumeid, s.t vana tarkvara kasutavad võrgustiku liikmed saavad verifitseerida plokke, mis loodi nii vana kui ka uue tarkvaraga, kuid uut tarkvara kasutavad võrgustiku liikmed ei saa verifitseerida plokke, mis loodi vana tarkvaraga. Sellise muudatuse õnnestumiseks on vajalik võrgustiku koguarvutusvõimsuses 51%-line toetus. *Hard fork* on aga vastupidine muudatus, mis laiendab kriteeriumeid, s.t uus tarkvara aktsepteerib vana tarkvaraga loodud plokke, kuid vana tarkvara ei aktsepteeri uue tarkvaraga loodud plokke. *Hard fork*'i abil sisse viidud muudatused on *soft fork*'ga võrreldes radikaalsemad, sest see võimaldab tekkida kahel eraldiseisval plokiahelal, mis poolitaks võrgustiku.

Mõlemat terminit kasutatakse just seoses krüptovaluutadega ning nendele terminitele hetkel eesti keeles häid ja ühtseid vasteid ei ole. Kõige levinum on sõnasõnaline tõlge ehk siis *raske kahvel* ja *pehme kahvel,* mis minu arvates aga ei sobi üldse, sest ei teki seos protsessi ja seda protsessi kirjeldava termini vahel. Sõnal *fork* on mõistagi ka teisi tähendusi (hargnemine, pooldumine). Kui terminid *hard fork* ja *soft fork* seostuvad krüptovaluutadega, siis *fork* ilma eesliiteta seostub tarkvaraga üldiselt. IT terministandardi sõnastik (ITS) annab *fork'*i vasteks *pooldumine,* Vallaste e-teatmik *harutamine ja* Esterm *hargnemine,* mis kirjeldavad antud protsessi täpsemalt, kui selle sõnasõnaline tõlge. Teised võimalused on ka veel *jagunemine, lahknemine* ja *lõhenemine.* Kõikide nende vastetega tähistatakse aga protsessi üldiselt, mitte aga selle astmelisust/suurusjärku, sama nagu inglise keeles. Inglise keeles on selle hargnemise mastaabi kirjelduseks kasutatud omadussõnu *hard* ja *soft* (eesti

keeles vastavalt *raske, kõva, tugev* ning *pehme*), mis eesti keeles ei sobiks. Sobilikum oleks rääkida *suurest* ja *väiksest hargnemisest,* mis kõlab IT-valdkonnas aga veidralt ja võõrastavalt. See võib olla üks põhjustest, miks kiputaksegi kasutama just inglise termineid, sest puudub sobiv eesti keelne vaste. Kaalusin kompromisslahendusena vähemalt pooleldi eestikeelset varianti, milles säilitada *fork*'i ja tõlkida *hard* ja *soft*. See aga ei kõlanud tõlget üle lugedes veenvalt. Seetõttu otsustasin siiski oma magistriprojektis kasutada termineid *raske kavhel* ja *nõrk kahvel*, mis viitavad teineteist vastanduvatele protsessidele. Eelnevast tulenevalt oli tõlkes kasutatud tõlkestrateegia sõnasõnaline tõlge.

Sauga küll mainib *fork*'e põgusalt lisamärkusena ning nimetab neid kahvliteks (2018: 130), kuid täpsemaid eristusi ei tehta.

Mäger on *hard fork*'i ja *soft fork*'i tõlkinud kui *pehme harunemine* ja *järsk harunemine* (Mäger 2018: 72–73), mille vastu midagi ette heita ei ole.

Nimede eestipäraseks mugandamine

Lähtetekstis kasutati bitcoini tööpõhimõtte paremaks selgitamiseks isikunimesid. Kasutatud nimed olid järgmised: Tamara, Edith, Tony, Michèle, Marcia, Brian, Jake ja Claudia. Otsustasin need nimed asendada eesti kultuuriruumis rohkem levinud nimedega nagu Mari ja Jüri jne, pöörates tähelepanu ainult sellele, et sugu klapiks. Algul esines kaheksast nimest ainult kolm, mis tõlkimist ei seganud, kuid veidi hiljem hakkas üha rohkem nimesid esinema, mis häiris tõlkeprotsessi, sest pidin pidevalt lähtetekstis tagasi minema ning üle vaatama, et isikutevahelised seosed tõlkes vastaksid lähteteksti omadega. See kulutas hulganisti aega ja segas tõlkimist. Oleks ma võõrapäraste nimede eestipärased vasted kuhugi üles kirjutanud, siis ei oleks sellist probleemi olnud, kuid seda ma ei teinud. Seega otsustasin muuta eestikeelses tekstis nimesid nii, et nende algustähed ja nimi üldiselt sarnaneksid lähteteksti nimede algustähtedega, aga ei kõlaks liiga võõralt. Tulemuseks oli:

Lähtetekst	Sihttekst
Tamara	Tamaara

Edith	Eda
Tony	Tõnu
Michèle	Mihkel
Marcia	Maarja
Brian	Boris
Jake	Jaan
Claudia	Klaara
Daniel	Daaniel

Järeldused

Kokkvõtvalt puudutan mõningaid olulisi tähelepanekuid, mida tegin antud tõlketöö eel, käigus ja järel.

Tõlketeooriatega tutvumine enne praktilise töö tegemist on kindlasti oluline, et määratleda teksti tüüp, eesmärk, kavandada rakendusele tulevaid strateegiaid. Samas oli kohati teoreetilisest kirjandusest ilma praktilise kogemuseta keeruline süvitsi aru saada. Liigitused tundusid kas kunstlikud või lihtsalt nii elementaarsed, et tekkis küsimus, milleks autorid peavad vajalikuks neid teoreetiliselt kirjeldada.

Näiteks tekstitüübi määratlemine ekspressiivseks, informatiivseks ja vokatiivseks on küll mõistetav ka ilma tõlkepraktikata, ent alles tõlkeprotsessi käigus sai selgeks, kui tähtis on tõepoolest teadvustada, mis tekstitüübiga on tegemist. Tõlkides informatiivset teksti, nagu antud töös tegin, ei saa lubada samasuguseid vabadusi nagu mõnede ilukirjanduslike tekstide tõlkimise juures. Mõisted ja definitsioonid pidin tõlkima korrektselt, täpselt, sidusalt, sest lähteteksti rahateoreetiliste määratluste puhul ei piisa lihtsalt mõtte või stiili edasi andmisest – definitsioonid peavad sihttekstis säilitama samad seosed mis lähtetekstis. Eriti selgelt tuli see esile tõlkeosa peatükis 2.2 Bitcoini süsteem, aga oli ka ülejäänud tekstis läbivalt oluline. Mõneti on siin hea paralleel matemaatika-alase tekstiga. Oletame, et tõlgime Pythagorase teoreemi kirjeldavat tekstilõiku. Igale lähtekeele mõistele peab leidma täpse sihtkeele vaste ja lause tervik peab tingimata looma identse tähenduse, et säiliks teoreemi kirjeldatav seos suuruste vahel. Lugedes saksa keeles lauset „In

einem rechtwinkligen Dreieck ist die Summe der Quadrate der Katheten gleich dem Quadrat der Hypotenuse“ ja eesti keeles lauset „Täisnurksel kolmnurgal on kaatetite ruutude summa võrdne hüpotenuusi ruuduga“ peab mõlemas keeles lugeja (kes on teadlik, et kaateteid tähistatakse a ja b ning hüpotenuusi c) olema võimeline võtma lause sisu kokku valemiga $a^2 + b^2 = c^2$.

Teisalt pean tõlkestrateegiate puhul tõdema, et näiteks Pymi liigituse põhjal kasutasin käesolevas tõlketöös üksnes strateegiaid „autopiloot“ (tõlkija lähtub tõlkimisel keeleoskusest ja teiste samalaadsete tekstide tundmisest, terminid saadakse sõnastikest ja teatmikest) ja kopeerimine (lähtekeele sõnade ja/või struktuuri ülevõtmine sihtkeelde). Ülejäänud Pymi strateegiad ei tulnud valitud teksti tüübi tõttu üldse kasutusele. Need oleksid kindlasti osutunud vajalikuks näiteks ilukirjandusliku teksti tõlkel.

Põhiliseks väljakutseks antud projektis tõlgitud teksti tüübi puhul on kahtlemata terminid. Põimub arvutiteadus ja majandusteadus, mille rahvusvaheline meedium on juba aastakümneid olnud inglise keel – sellest tulenevalt on kasutatavate mõistete kogum algselt ingliskeelne. Minu projekti lähtekeel on aga saksa keel, milles on teatud osa ingliskeelseid mõisteid jäetud ingliskeelsele kujule, teine osa aga tõlgitud saksa keelde. Tõlkija seisab silmitsi oluliste valikutega: mõistete puhul, mis juba eestikeelses kirjanduses käibivad, tuleb otsustada, kas need on otstarbekad ja täpsed või oleks mõistlik võtta kasutusele uus tõlge; mõistete juures, mida eesti keeles siiani polegi kasutatud, peab analüüsima, kas on häid tõlkevasteid või kasutada ingliskeelseid. Lisaks on väljakutse seegi, et isegi kui kõik mõisted (ükskõik mis tehnikaid kasutades) eestistada, kas tekiks liiga suur lõhe tõlke ja tegeliku erialapraktika vahel. Pean sellega silmas olukorda, kus krüptorahade kaevandajad ja/või kauplejad erialases suhtluses kasutavad otse ingliskeelseid mõisteid, kuid tekst, mis valdkonnast ülevaate annab, üritab juurutada eestipäraseid mõisteid, millest aga valdkonna sisering ei pruugi aru saadagi. Siin ei olegi ühest vastust ega lahendust, see jääbki tõlkijale väljakutseks.

KOKKUVÕTE

Nagu sissejuhatuses kirjeldatud, oli magistriprojekti eesmärk tõlkida Alexander Berentseni ja Fabian Schäri teose „Bitcoin, Blockchain und Kryptoassets" valitud peatükid eesti keelde ning analüüsida tõlkimisel tekkinud probleeme ja nende lahenduskäike.

Töö alguses põhjendasin oma valikut teema aktuaalsusega. Tõin välja, et plokiahela näol on tegemist suhteliselt uue revolutsioonilis-disruptiivse tehnoloogiaga, mille mõju võib juba lähitulevikus avalduda rahandusvaldkonnast väljapoole. Lisaks avaldasin, et teemavaldkond pakub mulle ka isiklikult huvi.

Projekt koosnes praktilisest ja teoreetilisest osast. Praktilise osa raames tõlkisin tervenisti teise peatüki, mis annab piisava ülevaate plokiahelast ja bitcoinist ning mis on samuti veel mõistetav inimesele, kes ei oma erialalisi teadmisi arvutiteaduse valdkonnast. Samuti tõlkisin alapeatüki 5.3, mis käsitleb bitcoinide nn kaevandamist ehk juurdetekitamist, mis omakorda tekitas arvutimaailmas palju pahameelt.

Teoreetilises osas andsin ülevaate tõlketeooria lähtealustest, tekstitüüpidest ja nende määratlemisest, samuti sellest, kuidas teksti eesmärk mõjutab tõlkestrateegia valikut. Seejärel analüüsisin konkreetse tõlgitud teksti näitel võtmeterminite tõlkimist eesti keelde, seostades erinevatel juhtudel termini tõlke vastava tõlkestrateegiaga, viies kokku teooria ja praktika.

KASUTATUD KIRJANDUS

Clayton. V (2015). The Needless Complexity of Academic Writing. A new movement strives for simplicity. Loetud aadressil https://www.theatlantic.com/education/archive/2015/10/complex-academic-writing/412255/ (20.11.2019)

Berentsen, A. & Schär, F. (2017). Bitcoin, Blockchain und Kryptoassets: Eine Umfassende Einführung. Norderstedt: BoD – Books on Demand

Drawing the distinction between the uppercase "B" and lowercase "b" in Bitcoin [ajaveebipostitus] (2014, 29. detsember). Loetud aadressil https://blog.blockchain.com/2014/12/29/drawing-the-distinction-between-the-uppercase-b-and-lowercase-b-in-bitcoin/ (17.09.2018)

Duden. Kättesaadav www.duden.de (27.11.2019)

Eesti Keele Instituut. (kuupäev puudub). *Keelenõuvakk.* Loetud aadressil http://keeleabi.eki.ee/index.php?leht=4&act=1&otsi=tsitaat (25.11.2019)

Esterm. Kättesaadav www.termin.eki.ee/esterm/.ee (27.11.2019)

Hosp, J. & Mäger, K. (tõlk.) (2018). Krüptoraha. Bitcoin, Ethereum, plokiahel ja ICO ja palju muud. Tallinn: Tänapäev

Lätt, P. (2015, november). Euroopa Kohus: bitcoin'ide vahetus on käibemaksuvaba nagu tavapärane valuutavahetus. *Maksumaksja*. Loetud aadressil http://www.maksumaksjad.ee/modules/smartsection/item.php?itemid=1950 (18.10.2018)

Newmark, P. (1988). A Textbook of Translation. Hertfordshire: Prentice Hall

Pym, A. (2018). A typology of translation solutions. Loetud aadressil https://minerva-access.unimelb.edu.au/bitstream/handle/11343/214404/art_pym.pdf?sequence=1&isAllowed=y (10.11.2019)

Sauga, A. & Saul, E (toim.) (2018). Kõik sai alguse Bitcoinist. Tallinn: Paradiis

Reiss, K. (2004). Type, kind and individuality of text: Decision making in translation. Tõlk. S. Kitron.

—— Venuti, L. (toim.) (2004). The Translation Studies Reader. London/New York: Routledge, 160 –172.

Veerpalu, H., & Demchuk, N. (2017). Plokiahela tehnoloogia võidukäik. Loetud aadressil https://www.ituudised.ee/uudised/2017/12/03/plokiahela-tehnoloogia-voidukaik (06.05.2018)

Venuti, L. (2004). The translation studies reader. London/New York: Routledge.

Vermeer, H. J. (2004). Skopos and commission in translational action. Tõlk. A. Chesterman.

—— Venuti, L. (toim.) (2004). The Translation Studies Reader. London/New York: Routledge, 221–232.

Vinay, J.-P. & Darbelnet, J. (2004). Comparative Stylistics of French and English: A Methodology for Translation. Tõlk. J.C.Sager & M.-J.Hamel, Amsterdam: Benjamins.

—— Venuti, L. (toim.) (2004). The Translation Studies Reader. London/New York: Routledge, 85–90.

SUMMARY

Rene Torop

“Bitcoin, Blockchain, Kryptoassets: Eine umfassende Einführung” valitud peatükkide tõlge ja tõlke analüüs

“Bitcoin, Blockchain, Kryptoassets: Eine umfassende Einführung” translation of selected chapters and translation analysis

Master’s project

2019

65 pages

This master's thesis has two main objectives: a practical translation exercise, and a theory-guided analysis of the translation process. The text chosen to be the subject of my translation from German into Estonian („Bitcoin, Blockchain und Kryptoassets“ by Alexander Berentsen and Fabian Schär) centers on the basics of crypto finance, outlining the bitcoin system and the concept of blockchains. The motivation behind the text selection lies both in the practical relevance of, and my personal interest in the topic. In the theoretical part, I provide a concise overview of the theory of translation, as well as some of the most widely known translation strategies. Analytically, the work is mainly built on theorists such as Newmark, Pym, Vinay and Darbelnet. My thesis demonstrates that, while the translation of a text from the field of economics is relatively less complicated than translating other types of text (especially fiction), some key challenges remain, notably in finding suitable translations for new terms and notions such as *blockchain*, *mining pool*, *soft* and *hard fork*, just to name a few.

Lõputöö autori kinnitus

Olen lõputöö kirjutanud iseseisvalt. Kõigile töös kasutatud teiste autorite töödele, põhimõttelistele seisukohtadele ning muudest allikaist pärinevatele andmetele on viidatud.

Autor: Rene Torop .....

(allkiri)

.....

(kuupäev)

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Rene Torop,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „“Bitcoin, Blockchain, Kryptoassets: Eine umfassende Einführung” valitud peatükkide tõlge ja tõlke analüüs“,

mille juhendaja on Terje Loogus,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

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

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

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

Rene Torop

28.12.2019