Kas *blockchain* on üksnes uus tehnoloogiline mänguasi või digirevolutsioon?

Mis on *blockchain*?

Tänapäeval kasutusel olevad panga või avaliku sektori andmete kogumise ja haldamise süsteemid on tsentraliseeritud ehk eksisteerib keegi (pank, ametiasutus), kes kontrollib kogu süsteemi (andmed, kirjed, tehingud jne). Samuti on praegused süsteemid n-ö *black-box*-süsteemid, kus kõik andmed ja tehingud ei pruugi olla süsteemi kõikidele osapooltele nähtavad (näiteks e-tervise andmebaasist on patsiendile nähtav ainult väike osa). *Blockchain*-tehnoloogia võimaldab selle andmebaasi muuta detsentraliseerituks, suurendades iga osapoole vastutust andmete õigsuse ja tehingute tõenduspõhisuse eest, kuid tõstes sellega ka süsteemi läbipaistvust ja usaldusväärsust (2). Teiste sõnadega on *blockchain* ehk plokiahel tehingute hajutatud (ehk detsentraliseeritud) andmebaas.

Kui tänaste andmebaaside puhul eksisteerib keegi, kes andmebaasi haldab, siis kuidas tõendada, et *blockchain*-tehnoloogial põhinevates andmebaasides tehtud tehingud on legitiimsed, kui seal puudub vahendaja? *Blockchain* lahendab selle olukorra, kopeerides kõik tehingud iga osapoole 'plokis'. Iga osapool saab tehinguid lisada, kuid tehingud muutuvad legitiimseks alles

siis, kui kõik osapooled neid aktsepteerivad. Plokid on järjestikku krüptograafiliselt "kokku aheldatud" ja juba aktsepteeritud plokke ei ole võimalik muuta. Nii on välistatud ka võimalus, et mõni andmebaasi osapool 'omavolitseks' ja tehinguid omavoliliselt muudaks või tühistaks. Seega on *blockchain*'i peamiseks omaduseks detsentraliseeritud usaldus – selle tehnoloogia abil saab ilma vahendajate/autoriteetideta usaldusväärseid teenuseid luua. Näiteks, kui süsteemile on öeldud, et kinnisvara müügis osalevad müüja, ostja, notar ja pank, siis muutub tehing andmebaasis legitiimseks alles siis, kui kõik osapooled on kinnitanud, et kõik andmed on õiged ja nad on tehinguga nõus. Täna kontrollib osapoolte autentsust ja tehingute õigsust andmebaasi haldaja (pank või ametiasutus), *blockhain*-tehnoloogiat kasutavas andmebaasis toimub see kontroll automaatselt.

Blockchain'i kasutusvaldkonnad

Blockchain'i kasutusvõimalused on väga mitmekülgsed. Levinuimateks võib pidada krüptoraha ja küberturvalisuse tagamise lahendusi. Tänu vahemehe ärajäämisele võimaldab antud tehnoloogia paljusid protsesse kiirendada, lihtsustada ning odavamaks muuta. Madalamast hinnast ja suuremast läbipaistvusest ning kiirusest tulenevalt uuritakse ja arendatakse *blockchain*'ide kasutamist finants-, pangandus- ja kindlustusvaldkonnas ning intellektuaalse omandi kaitsel ja avalike teenuste pakkumisel. *Blockchain*'i võimalusi nähakse eelkõige seal, kus esineb vajadus tõestada dokumentide ja andmete autentsust.

Finantsrakendused/krüptoraha

Finants- ja pangandussektori jaoks võib *blockchain'i* kasutuselevõtmine tähendada finantsteenuste ulatusliku automatiseerimise võimalust (3, 4, 5). Esimeseks ja kuulsaimaks rahvusvaheliseks *blockchain*'i kasutajaks on krüptoraha Bitcoin (tänaseks sugugi mitte ainuke krüptoraha). Krüptoraha on virtuaalne raha, mis kasutab turvalisuse tagamiseks krüptograafiat. Krüptoraha ei ole välja antud ühegi panga poolt, teda ei ole trükitud ega kellegi poolt kontrollitud. Kui klassikalise panganduse puhul usaldavad tehingu osapooled kolmandat osapoolt, kelleks on tavaliselt pank või valuutavahetuspunkt, siis krüptoraha vahetatakse hajutatud süsteemis, kusjuures üldjuhul jäävad kasutajad anonüümseks. Krüptorahaga tehtavad tehingud on väga odavad (kuni 10 eurosenti) ja pakuvad ajatembeldatud[4] kinnitust (ehk tõenduspõhisust).

4 Ajatembeldus (*time-stamping*) on *blockhain*-tehnoloogiaga kaasnev võimalus, kus igale süsteemis tehtud tehingule kinnitatakse kuupäev ja kellaaeg, mida ei saa hiljem muuta.

Samas ei kinnita ükski allikas, et krüptoraha lähitulevikus tavapanganduse üle võtaks ja seda peamiselt kolmel põhjusel:

1. Süsteemi anonüümsus (võimaldab muuhulgas rahastada kuritegevust).
2. Suur väärtuse kõikumine. Tänapäeval alluvad kõik krüptorahad väga laialdasele spekulatsioonile ning nende väärtus kõigub igapäevaselt tugevasti.
3. Tehnilised piirangud: protsess on aeglane, piiratud skaleeruvusega ja energiamahukas.

Suurt teadmatust valmistab see, milliseks kujuneb krüptovaluutade olukord tulevikus. Peamised eksperdid ei näe siiski ohtu keskpankadele, kuna keskpangad tavaliselt ülekande- ja teenustasude pealt märkimisväärselt ei teeni. Paljud keskpangad näevad *blockchain*'i pigem kui tehnoloogilist lahendust (mitte kui krüptoraha), mille abil suurendada nii klientide ligipääsu teenustele ja kui ka andmete korrektsust ja läbipaistvust.(4). Hajutatud süsteemis, mis on sõltumatu pankade vahendusest, on võimalik langetada finantsteenuste hinda ja kiirendada standardteenuste pakkumist (5).

Intellektuaalse omandi kaitse

Blockchain-tehnoloogial baseeruv andmebaas võimaldab turvalisemalt ja kiiremini fikseerida patendi olemasolu, mis tagab intellektuaalse omandi kaitse. Ühelt poolt pakub *blockchain* võimalust säilitada patenti originaalkujul, väljavaateta seda pahatahtlikult muuta ning kaitstes selle sisu. Patendi sisu kaitsmine muutub üha olulisemaks, kuna maailmas on sagenenud juhtumid, kus patendi kohta saadaolevat teavet kasutatakse ära selleks, et tuua toode turule enne, kui selle leiutaja seda teha suudab (2).

Automatiseeritud protsessid ehk nutilepingud

Üheks peamiseks *blockchain*-tehnoloogia majanduslikuks rakenduseks peetakse nutilepingut. Nutilepingu keskseks ideeks on arvutikoodipõhised tehingud. *Blockchain* pakub alustehnoloogiat, seadmaks tehingule kriteeriumid, millisel juhul ta automaatselt ja ilma täiendava autoriseeringuta ellu viiakse. Nii näiteks võib nutileping toodete tarnimisel iseseisvalt makseid korraldada ning samuti tarneahela toimimist organiseerida, esitades uusi tellimusi ning edastades automaatselt infot tarneahela osapooltele (6).

Avalikud teenused

Avalike teenuste puhul võib kasutusvaldkonnad jagada peamiselt kaheks: läbipaistvuse/küberturvalisuse tõstmine ja protsesside automatiseerimine.

Blockchain-tehnoloogia võimaldab oluliselt suurendada avalike teenuste küberturvalisust, läbipaistvust ja auditeeritavust. *Blockchain*'i salvestatud infot ei ole tagantjärele võimalik muuta ja seda saab sõltumatult kontrollida. Oluline on ära märkida, et sel eesmärgil ei pea *blockchain*'i salvestama tegelikke andmeid, vaid piisab nende sõrmejäljest ehk krüptograafilisest räsist. See võimaldab kontrollida, et andmeid ei ole juhuslikult või pahatahtlikult muudetud ning samuti veenduda, et logifailid andmete kasutamisest oleksid tõesed ja muutmatud. Üks tuntumaid *blokchain*'i kasutajaid avalikus sektoris on Eesti riik, kes kasutab *blockchain*-tehnoloogiat erinevate registrite ja süsteemide terviklikkuse tagamiseks (10).

Teisalt võimaldaks *blockchain*-tehnoloogial põhinevad süsteemid regulaarseid väljamakseid riigikassast (toetused, lepingulised väljamaksed jms) potentsiaalselt optimeerida ning nende legitiimsust kontrollida. Suurbritannias katsetatakse *blockchain*'i-põhist sotsiaaltoetuste maksmise süsteemi. Toetuse saaja nõusolekul saab ta toetuse kätte mobiilimaksena ja saab seda ka kulutada mobiilimaksetena. Programmi eesmärk on aidata inimestel nende toetussummat hallata, luua efektiivsem sotsiaalsüsteem, vältida pettusi ning tekitada usalduslikum vahekord riigi ja kodaniku vahel. Samuti kaalutakse Suurbritannias suurema läbipaistvuse tagamise nimel pidada kõikide riiklike kulutuste üle arvet *blockchain*'i abil (2). See võimaldaks oluliselt lihtsustada nii riigi arvepidamist kui ka auditeerimist. Lisaks laseksid nutilepingud riiklikke projektitoetusi välja maksta nii, et nende kulutamine on võimalik ainult konkreetselt kokku lepitud tingimustel.(6).

Samuti nähakse *blockchain*-tehnoloogia kasutamise potentsiaali e-hääletamise läbiviimisel. Kui täna salvestatakse, loetakse, kontrollitakse ja hallatakse hääletamisel antud hääli tsentraalselt, siis *blockchain*-tehnoloogia võimaldaks igal hääle andjal teha seda ise, lubades enda poolt antud hääle salvestada. Iga süsteemi osapool näeks, kui keegi üritaks tema tehingut muuta või kustutada, sest tema logi oleks erinev teiste osapoolte logidest. Antud juhul jääks ära häälte kontrollimine ja lugemine andmebaasi haldaja poolt, kuna seda teeb süsteem automaatselt. Üheks *blockchain*-tehnoloogial põhineva e-hääletussüsteemi eeliseks peetakse võimalust tuua kodanikukohustuse täitmine kodanikule lähemale (luues n-ö alt üles kodanikuühiskonda), pakkudes suhteliselt odavat ja lihtsat häälte kogumise süsteemi. Samas on esitatud ka vastuväiteid, kuna süsteem võimaldab jääda anonüümseks ning tehnoloogiliselt on hääletussüsteemile ligipääsemine liiga keeruline (2).

Lisaks Eestile on *blockchain*'i rakendamisel avaliku sektori hüvanguks saavutatud edu neis riikides, kus puuduvad varasemad tsentraliseeritud põhiregistrid. Näiteks kasutatakse Ghanas, Keenias ja Nigeerias *blockchain*-tehnoloogiat maakatastri digitaliseerimisel. Sellega asendatakse ebausaldusväärsed või olematud avalikud maaregistrid ning võimaldatakse omandiõiguse kaitse detsentraliseerimist ja demokratiseerimist. Sarnaselt on ka Honduras

ning Gruusia võtnud kasutusele *blockchain*-tehnoloogia, et oma maaregistreid paremini pettuste eest kaitsta (1). Rootsi testib *blockchain*-tehnoloogial põhineva kinnisvaraandmebaasi loomist, võimaldamaks tehingu osapooltel (pank, riik, vahendaja, ostja ja müüja) kontrollida tehingu käiku, muutes kogu tehingu protsessi läbipaistvamaks ja hoides samal ajal kokku nii aega kui ka raha (2). Poliitikavaldkonnas on antud tehnoloogia kasutusel Taanis erakonnasiseste valimiste läbiviimisel.

Võimalused ja väljakutsed

Blockchain-tehnoloogia võimaldab tõsta usaldust e-teenuste vastu, pakkudes sõltumatut auditeerimist.	*Blockchain*-tehnoloogia võimaldab kiirendada, detsentraliseerida, automatiseerida ja standardiseerida andmepõhiseid protsesse nii avalikus kui ka erasektoris. See võib põhjalikult muuta varade ülekandmise ja arvepidamise viise, avaldades mõju nii era- kui ka avalikule sektorile.
Eestil on võimalus *blockchain*'iga seotud teadmisi ja teenuseid eksportida (näiteks rahvusvaheliste finantsteenuste või andmekaitse valdkonnas). Eesti oma kogemuste, digiühiskonna arengu ja väiksusega on hea *blockchain*-tehnoloogia kasutamise testplatvorm.	Krüptorahade puhul puudub seadusandlik ja rahvusvaheliselt kokku lepitud raamistik, mis kaitseks kasutajate anonüümsust ja autoriõigusi ning sätestaks *blockchain*'i-põhiste süsteemide kasutamise järelevalve (7).
Tulenevalt krüptoraha anonüümsusest on rahapesu, illegaalse kaubanduse ja terrorismi rahastamise oht suur (7).	Puudub üldine usaldus uue tehnoloogia vastu ja kogemus selle kasutamisel. (3).
Vaja on kindlaks teha, mil määral riiklik regulatiivne sekkumine on vajalik, et tõkestada pahatahtlikku kasutust. (5).	Vähenev tööjõuvajadus sektorites, mida *blockchain*'i innovatsioon puudutab (esmajoones kindlustus, pangandus ja kinnisvara) ning suurenev IKT-sektori tähtsus.

Nagu näha, on enamik väljakutseid seotud krüptorahadega, mis on vaid üks *blockchain*'i kasutusvaldkondi. Väga oluline on seda eristada, vältimaks näiteks olukorda, kus krüptoraha kontrollimiseks reguleeritakse ja piiratakse kogu tehnoloogiat, takistades muude valdkondade innovatsiooni ja teenuste arengut.

Blockchain'iga seotud võimalused on asjatundjatele küll teada, kuid tänapäeval veel suuresti kasutamata. Üheks põhjuseks on kindlasti asjaolu, et olemasolevate andmebaaside üleviimine *blockchain*-tehnoloogiale on aja- ja ressursimahukas töö, mida keegi niisama ette võtta ei soovi. Seega on *blockchain*-tehnoloogial põhinevaid andmebaase lihtsam luua seal, kus tsentraliseeritud registreid veel ei ole.

Fakt, et *blockchain*'i tehtud sissekannet ei saa tagantjärele muuta ega kustutada, on nii antud tehnoloogia tugevus kui ka nõrkus. Nimelt on olemas oht, et *blockchain*'i andmed võivad kahjustada andmekaitset ja privaatsust, ning seda juhul, kui *blockchain*'i on salvestatud tegelikud andmed, mitte andmete krüptograafiline sõrmejälg. *Blockchain* ei garanteeri anonüümsust ning mida suuremaks muutub andmete hulk inimeste kohta, seda lihtsamaks muutub ka konkreetsete isikute tuvastamine. Andmete muutumatus takistab "õigust olla unustatud", mille kohaselt on inimestel õigus teatud tingimustel nõuda enda kohta käivate andmete kustutamist (2).

Mõju Eestile

Eestit peetakse Euroopa üheks arenenuimaks *blockchain*-tehnoloogia kasutajaks avalike teenuste pakkumisel. Nagu mainitud, on peamiseks eesmärgiks küberturvalisuse ja protsesside läbipaistvuse suurendamine.

Blockchain-tehnoloogiat integreeritakse Eestis üha enam riiklike infosüsteemide baastarkvarasse. Riigi Infosüsteemi Ametil (RIA) võimaldab *blockchain*-tehnoloogia tagada nii andmete, süsteemide ja protsesside terviklikkuse kui ka andmete loomise aja kontrollimise ning tõendamise. RIA vahendab ühe baastaristu alusteenusena nii riigiasutustele kui ka teistele avalikke ülesandeid täitvatele asutustele *blockchain*-tehnoloogiat (5, 10). Alates 2016. aastast on riiklikku andmevahetuskihti X-tee integreeritud andmebaase hakatud järgemööda *blockchain*-tehnoloogia abil turvama (10). Näiteks kasutatakse e-tervise andmebaasis *blockchain*'i-põhist ajatemebeldust, mis annab süsteemile juurde lisaturvakihi. Samuti toetab *blockchain*-tehnoloogia X-tee turvalisemaks muutmist.

Registrite ja Infosüsteemide Keskuse (RIK) jaoks seisneb *blockchain*'i peamine väärtus võimaluses kontrollida regulaarselt ning kiiresti suuri andmehulki ning teha kindlaks, et andmetes ei ole toimunud pahatahtlikke muudatusi. Riiklike registrite töö muutub tänu sellele kiiremaks ja efektiivsemaks; kuna tehingutel puudub vahendaja, siis saab praegu vahendaja rolli täitev RIK oma ressursse mujale suunata ning süsteem kontrollib end ise. Samuti suureneb pettuste avastamise ja andmete tõenduspõhisuse tõenäosus, kus RIK saab info kiiresti vastavatele uurimisorganitele edastada. Sellise lahendusega on RIKi haldusalas turvatud näiteks Kinnistusraamat, Äriregister, Riigi Teataja, Avalikud Teadaanded, Digitoimik jne.

Ideetasandil Eesti oma Estcoin'i loomine, mis kujutaks endast turvalist krüptoraha võimaldamaks e-residentidel Eesti riiki otse investeerida – eesmärk on tõsta usaldusväärsust ja kaasata investorite hulka ka riik, kusjuures tulu suunataks Eesti arengu hüvanguks (11).

Erasektoris on *blockchain*-tehnoloogia tuntuimaks arendajaks Eestis AS Guardtime. Guardtime pakub *blockchain*'i-põhiseid lahendusi kaitsetööstuse, telekommunikatsiooni, kindlustuse, tarneahelate haldamise jms vallas. Veel on Eestis *blockchain*'i rakendamist katsetanud LHV Group reaalajas teostatavate rahaülekannete näol ning varade ja nende omanikusuhete registreerimisel (13). Nasdaq OMX gruppi kuuluv AS Eesti Väärtpaberikeskus katsetab ja arendab Eestis aktsionäride koosolekute e-hääletussüsteemi, millega saab aktsionäridele, kes koosolekul viibida ei saa, luua võimaluse osaleda hääletusprotsessis, lisaks ka hääletusprotsessi paremini läbi viia ning tulemusi fikseerida (5, 12). BITNATION[5] pakub koostöös e-residentsuse programmiga e-residentidele notariteenust (5, 12). Need on mõned näited praegu Eestis toimivatest erasektori algatustest *blockchain*-tehnoloogia kasutamisel.

Eestil on olemas kõik eeldused viia oma IT taristu üle *blockchain*-tehnoloogiale – kõrge digitaalmajanduse areng, elanikkonna suur usaldus e-teenuste vastu, riigi e-teenuste arendamise kogemus, olemasolev X-tee andmevahetuskiht, IKT-alased teadmised, väike kogukond ning ID-kaardil põhinev isikutuvastus. *Blockchain*-tehnoloogia vajab plahvatuslikuks kasvuks head seadusandlikku keskkonda (digitaalne allkiri ei maksa midagi, kui tal ei ole seadusandlikku jõudu) ning turvalist isikutuvastamise süsteemi (tagamaks süsteemi usaldusväärsus) (12). Eestil on võimalus eraldada terad sõkaldest – eristada *blockchain*-tehnoloogiat ja krüptoraha. Hoovad järgmise digirevolutsiooni vallapäästmiseks on riigi kätes – luues soodsa seadusandliku keskkonna, loob riik eeldused digiühiskonna viimiseks järgmisele tasandile.

5 *Blockchain*-tehnoloogiat kasutav ettevõte: http://www.cuber.ee/en_US/

Autorid

Katre Eljas-Taal

Technopolis Group
Eesti juhataja

Anne Veerpalu

NJORD Advokaadibüroo
partner,
Tartu Ülikooli infotehnoloogia
õiguse doktorantja IT-õiguse
magistriprogrammi õppejõud

Ivo Lõhmus

Guardtime AS,
avaliku sektori programmijuht

Jari Romanainen

Technopolis Group poliitika-
nõunik, Soome innovatsiooni-
agentuuri Tekes endine nõunik

Allan Allik

Kasutatud allikad

1. Réchard et al (2016): European Parliamentary Research Service: Global Trendometer. Essays on medium- and long-term global trends.
2. Boucher et al. European Parliamentary Research Service (2017): How blockchain technology could change our lives.
3. Gabison (2016): Policy Considerations for the Blockchain Technology Public and Private Applications. European Commission
4. Koeppl & Kronick (2017): Blockchain Technology – What's in Store for Canada's Economy and Financial Markets?
5. Rahandusministeerium (2017): Analüüs virtuaalvääringute võimaliku tunnustamise ja kasutamise poliitika väljatöötamiseks
6. Deloitte (2016): CFO Insights. Getting smart about smart contracts
7. Euroopa Parlament (2016): MEPs call for virtual currency watchdog to combat money laundering and terrorism
8. Fraunhofer (2017): Blockchain - Technologien, Forschungsfragen und Anwendungen
9. Kompetenzzentrum Öffentliche IT (2017) Mythos Blockchain - Herausforderung für den Öffentlichen Sektor
10. RIA (2016): E-riik 2018: X-tee vahendab sellest nädalast alusteenusena plokiaheldust
11. Kaspar Korjus (2017) : Estonia could offer 'estcoins' to e-residents
12. Kaspar Korjus (2017): Welcome to the blockchain nation: https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4
13. http://www.cuber.ee/en_US/