
Kes kaitseb, kui kood on seadus?

06. jaanuar 2022

Mis juhtub, kui posu tarku ja andekaid tarkvaraarendajaid ja (andme)teadlasi tuppa lukustada ning võtta neilt võimalus sisustada aega koduvälise meelelahutusega? „Paljugi“ võiks öelda, sest niivõrd hoogsat digilahenduste plahvatust, kui viimase pooleteise koroona-aasta jooksul nähtud, ei osanud ilmselt keegi ette kujutada. Finantssektorissee tõi koodikunstnike loominguplahvatus 2020. aasta kevadiste piirangute järgselt ilmingu, mida hakati tagantjärele nimetama detsentraliseeritud rahanduse (DeFi) rakenduste kuumaks suveks.

Sama asi uues kuues või paralleeluniversum?

DeFi rakendused ei ole oma olemuselt midagi uut. Vastupidi, nende eesmärk, nagu nime teine poolgi viitab, on suuresti kopeerida traditsiooniliste finantssüsteemide funktsioone. Kujutage ette panka ilma laenuhalduriteta või investeerimisplatvormi ilma maaklerite ja kesksete väärtipaberibörsideta. Kõik reeglid on plokiahela nutikatesse lepingutesse (*smart contract*) juba eelnevalt sisse programmeeritud ja tehingute toimumine sõltub sellest, kas soovitud tehing vastab sisseprogrammeeritud loogikale. Kolmandad osapooled tehingutesse ei sekku ja kood on seadus. See on mantra, mis käib DeFi rakendustega alati kaasas. Tihti on see ka osapoolte argument, miks muud seadused DeFi süsteemidele laieneda ei tohiks.

Sellisel süsteemil võib olla mitmeid võlusi. Näiteks ei esineks detsentraliseeritud lahendustes tõenäoliselt diskrimineerimist, kuna kõik asjaosalised on süsteemi jaoks päritoluta, soota ja vanuseta isikud ning tingimused rakenduvad kõigile võrdselt. Samuti tähendab vahendajate puudumine, et oma vara ei pea usaldama kolmandate isikute kätte, kelle pankrotistumisel võib ka enda kogutust ilma jääda. See võiks olla iseäranis tugev argument arengumaades, kus usaldus traditsioonilise finantssektori vastu võib olla õhuke. Arenenud riikides seevastu näib lummavana süsteemi autonoomsus, mis võimaldaks teenuseid pakkuda väiksemate kuludega ja seeläbi suurendada ligipääsu teenustele. Täielikult detsentraliseeritud süsteemis ei saaks esineda ka informatsiooni asümmeetriast tingitud süsteemset riski, kuivõrd kõik tehingud peaksid olema plokiahelas salvestunud ja seeläbi kõigile turuosalistele detailideni nähtavad.

Rahamängust tahab keegi alati võitjana väljuda

Siiski tuleb tõdeda, et DeFi nimetuse esimene pool võib olla kohati petlik. Ei tasu unustada, et kui rahamäng lüüakse käima, tahab keegi sellest alati võitjana väljuda. Ehkki DeFi lahendusi turundatakse täielikult detsentraliseeritud ja privaatsena, siis enamasti kehtib see vaid tehingute läbiviimise kohta. Kood jääb siiski seaduseks. Et seda mantrat edasi kanda, on lähtekood tüüpiliselt ka avalik (*open source*), võimaldades igaühel sellega soovi korral tutvuda. Tihti on DeFi rakendustel väga suur rõhk ka kogukonnal ehk rakenduse kasutajatel, kellega hoitakse üleval aktiivset suhtlust ja kelle soovidega arendustegevuses teataval määral arvestatakse. Et kogukonna rolli veelgi esile tõsta, toimuvad rakenduse arendussuundade või kas või vigade parandamise üle otsustamine väga tihti niiõelda valitsemistokenite (*governance token*) omanike seas läbiviidavatel hääletustel. Vastavaid tokeneid on aga igaühel võimalik endale osta või teenida ka tasuna rakenduse kasutamise eest.

Samas on mõeldamatu, et keegi kulutab kuid või aastaid arendustiimi töötunde selleks, et tuua turule rakendus, mille arvelt ise midagi ei teenita. Seetõttu on küllaltki tavapärane, et DeFi rakenduste arendajad säilitavad huvi ka protokollide edasise toimimise vastu. Võrdlemisi tavapärane on, et arendajad hoiavad enda käes arvestatavat osa valitsemistokenitest, lootuses et rakendus osutub populaarseks ja nende tokenite väärtus kasvab märkimisväärselt. Sellega kaasneb aga ka suurem otsustusõigus rakenduse tuleviku osas. Tasub meeles pidada, et arendajatel on alati parim teadmine sellest, kuidas süsteem toimib, ning see võib neile luua ka eelise rakenduses osalemiseks. Seega tekib küsimus, kui detsentraliseeritud ikkagi on lahendused, kus arendajad võivad jätta endale mitmeid eelisvõimalusi süsteemi puudutavate otsuste suunamiseks. Sellise mõjuvõimu juures ei saa täielikult välistada ka arendajate poolt läbiviidavaid tahtlikke pettuseid. On olnud juhtumeid, kus arendajad on endale loonud või hiljem lisanud nõ tagauksed, mille kaudu süsteemi enda kasuks tööle panna. Samuti on esinenud näiteid, kus arendajad on detsentraliseeritud vahetusplatvormidel automaatse turutegija süsteemi manipuleerinud, et klientide poolt vahetuseks antud tokenid omastada ning neile vastu pakutud tokenid hiljem väärtusetuks muuta.

Ebastabiilne vundament lükkas Pisa torni kaldu. Kas ka koodi monopoli?

Teisalt ei ole investorid detsentraliseeritud rahanduse rakendustes päriselt kaitstud isegi siis, kui

tegemist on tõeliselt detsentraalse rakendusega ja ükski keskne osapool seda kuidagi mõjutada ei saa. Lausa kahest ohust korraga pakkus näite 2016. aastal The DAO nimelise detsentraliseeritud investeerimisfondi ümber toimunu. Fondi panustati lühikese ajaga märkimisväärsed 150 miljonit USA dollarit, kuid automaatsena kavandatud investeerimistegevuseni ei jõutudki, sest keegi pahalane avastas osakute ostmise faasis DeFi süsteemidele omaselt avalikuks tehtud lähtekoodist loogikavea, mis võimaldas tal kolmandiku fondist varadest tühjaks teha.

Veelgi huvitavamaks võib pidada seda, mis The DAO vea avastamise järgselt aset leidis. Kuivõrd The DAO rajamine oli kujundatud Ethereumi plokiahelale, tekkis sealse kogukonna seas pikk arutelu selle üle, kuidas tekkinud olukorrast välja tulla. Hoolimata asjaolust, et kood peaks olema seadus ja teoorias on plokiahelal toimuvad tehingud pöördumatud, toimub plokiahelasse andmete kirjutamine teatavasti konsensusmehhanismi baasil. See võimaldas Ethereumi kaevandamisvõimekusest enamikku omavatel isikutel otsustada jäiga jagunemise (*hard fork*) kasuks, kus 85% kaevandamisvõimekusest jätkas plokiahela kirjutamist enne The DAO ründamist salvestunud plokist, tekitades seeläbi uue plokiahela haru, kus rünnakut kunagi ei toimunudki ja The DAO likvideeriti. Seejuures otsustasid vähemusse jäänud kaevandajad jätkata vana haruga, kus rünnak siiski toimus, mistõttu eksisteerib tänaseni kaks Ethereumi plokiahela paralleeluniversumit.

See näide on oluline, kuna jagunemise kasuks otsustanud enamus hülgas selle käiguga plokiahela fundamentaalsed põhimõtted nagu tehingute pöördumatus ja koodi kohtlemine seadusena. Kood püsis seadusena seni, kuni enamus otsustas teisiti. Et The DAO ründamine näis enamuse õiglustundele vastuvõetamatu, kuulutati ajutiselt seaduseks koodi asemel justnimelt enamuse otsus. See seab aga ohtliku pretsedendi, kus majoriteet võibki sisuliselt otsustada minorige rahakoti üle. Plokiahelas ei moodustu enamus seejuures mitte individuaalsete kasutajate häältest, vaid see sõltub sisuliselt kasutaja jõukusest. Töö tõendamise (*proof of work*) protokollides kirjutavad uued plokid enamikku kaevandamisressurssi omavad kasutajad, panuse tõendamise (*proof of stake*) protokollides aga valitakse plokkide kinnitajad juhuslikult nende panuse suuruse järgi. Kui mõnel isikul või grupil on vastavat ressurssi piisaval määral, võidakse seeläbi omandada kontroll kogu ahela üle ja salvestada sinna teadlikult valeinfot, mis võimaldab teiste osaliste arvelt rikastuda. Plokiahela süsteemides teatakse seda 51% rünnakuna.

Klientide kaitse ei saa olla subjektiivne küsimus

Regulaatorid üle maailma toetavad vastutustundliku innovatsiooni arengut ja kaasavad oma ala tippeksperite, et omada uute tehnoloogiate osas kõige kaasaegsemat teadmiste pagasit. Seejuures tuleb tõdeda, et regulaatorid puutuvad kokku ka selliste DeFi rakenduste loojatega, kes soovivad vaid kinnitust, et nende ärimudelile ei rakenduks finantssektori regulatsioonid ja tegevusloa nõuded. See on kurvastav, kui innovatsiooni põhifookus koondub sellele, kuidas vältida klientide kaitseks ettenähtud seaduseid, mitte sellele, kuidas kliendile parimat teenust pakkuda.

Tasub arvestada, et DeFi teenuste arendajaid, kes ise ka pärast rakenduse lansseerimist jätkavad süsteemis tegutsemist, tuleks kohelda kui tsentraalseid teenuseosutajaid, kes peaksid reguleeritud finantsteenuste pakkumiseks ka vastavasisulise tegevusloa hankima. Arvestades kõiki võimalusi, mis neil võib esineda klientide varalise seisuga mõjutamiseks, näib see üsna elementaarse nõudena. Kui tegevusloa hangitud ei ole, tuleks ehk küsida, mida sellist nende süsteemis peitub, mille pärast nad kliendi ees vastutada ei taha.

Mari-Liis Kukk