DAO

Esitatud teave ei ole käsitletav õigusnõuandena ega -selgitusena. Soovitame seotud osapooltel oma tegevust eelnevalt hinnata ja õiguslikult kvalifitseerida, kasutades vajadusel kutselist õigusnõuandjat. Uuenduslike lahendite tarbijatel soovitame hinnata riske oma rahaliste vahendite kasutamisel.

Samuti soovitame tutvuda Euroopa Liidu krüptovaraturge käsitlev määruse (MiCA) eelnõu ja sellega seotud ettepanekutega.

Detsentraliseeritud autonoomne organisatsioon (DAO) toimib plokiahelas arvutiprogrammina kodeeritud reeglite ehk nutilepingute järgi. See on mõeldud olema läbipaistev, täielikult liikmete kontrollitav ning keskse juhtimiseta. Teisisõnu on DAO digitaalne koostöövorm, mille funktsioonid on matemaatiliselt automatiseeritud. DAO juhtimis- ja kontrollifunktsioonid on jagatud horisontaalselt liikmete vahel, mis välistab vajaduse keskselt juhitud struktuuri järele. DAO-sid kasutatakse näiteks detsentraliseeritud rahanduses (DeFi), mille rakenduste haldamiseks on vaja detsentraliseerituse ehk keskse juhtimise puudumise printsiibi täitmiseks samal põhimõttel töötavat organisatsiooni.

DAO asutamiseks tuleb kirjutada n-ö targad lepingud, kuhu kodeeritakse organisatsiooni toimimise reeglid. Seega peab DAO-l olema alguses siiski keskne arendustiim. Hilisemad valitsemisotsused tehakse organisatsiooni valitsemistokenite omanike hääletustel. Tuues paralleeli traditsiooniliste aktsiaseltsidega, kujutavad valitsemistokenid endast sisuliselt hääleõigusi organisatsiooni üldkoosolekul ehk neid võib ühel isikul olla rohkem kui mõnel teisel. Erinevate DAO-de valitsemistokeneid võib olla võimalik nii teenida kui ka osta.

Milline on DAO-de õiguslik staatus?

DAO-d võib liigitada kahte kategooriasse: registreeritud DAO-d, mis on ehitatud üles konkreetse riigi seaduste kohaselt ja registreeritud vastavas äriregistris, ning registreerimata DAO-d, mis on loodud väljaspool riiklike seadustega määratletud õigusraamistikku ja pole äriregistris registreeritud. Enamik käibivatest DAO-dest on registreerimata ja nende õiguslik staatus on praegu ebaselge, võib sõltuda konkreetsetest asjaoludest ning ei ole välistatud nende kvalifitseerimine kehtivas õiguses sätestatud alustel ja juba olemasolevate õigusinstituutide kaudu. Näiteks kui DAO ei ole äriseadustiku mõistes registreeritud äriühing, vajab selgitamist, kas ta peaks siiski deklareerima ja tasuma makse või avama pangakonto ning kui jah, siis kellel saaks olla volitus või kohustus teha seda detsentraliseeritud autonoomse organisatsiooni korral, kui eesmärk on olemuslikult välistada juhtide ja esindajate olemasolu.

Lisaks DAO-de õigusliku määratluse ebaselgusele on nende tegevuses osalemise puhul teisigi riske:

Küberriskid – DAO-de „tarkade lepingute“ turvalisus ei pruugi olla tagatud. Selle põhjuseks võivad olla näiteks tahtmatult tehtud vead protokolli koodis, mida ründajail on võimalik ära kasutada. See

stsenaarium realiseerus esimese DAO-ks nimetatud riskifondilaadse organisatsiooni puhul, millest häkkeril õnnestus kodeerimisvea tõttu vara röövida. Samuti on võimalikud tahtlikud arendajate poolt endale jäetud „tagauksed“ organisatsiooni aluskoodis, mille läbi DAO-d hilisemas arengufaasis ise rünnata. DAO-d kasutavad üldiselt mõnda plokiahelat (nt Ethereum), mis pole DAO enda kontrolli all. See teeb need haavatavaks ka rünnetele, mis on suunatud plokiahela vastu üldiselt. Võivad aset leida ka n-ö 51% rünnakud, mille käigus plokiahela validaatorite enamus plokiahelaga manipuleerib.

Valitsemis-/juhtimismudelist tulenevad riskid – DAO-de juhtimisotsused (nt „tarkade lepingute“ muutmine) tehakse valitsemistokenite põhisel hääletusel, kus teatud arv tokeneid võrdub häälega. Üksikute rühmade või isikute kätte võib aga koonduda suur hulk valitsemistokeneid, millega on võimalik hääletusi mõjutada. See seab kahtluse alla organisatsiooni detsentraliseerituse. Suure osa tokenitest võivad enda kätte jätta näiteks DAO arendajad, et enda tehtud töö eest tulevikus tulu teenida.

Samuti võib esineda kartellide teket valitsemistokenite omanike seas. Plokiahela anonüümsuse tõttu ei pruugi olla võimalik kindlaks teha valitsemisõiguste reaalseid omanikke ehk avalikus koodis tunduvad tokenid olevat võrdselt jaotunud, aga reaalsuses mitte. Lisaks valitsemistokenite üksikute isikute kätte koondumise probleemile võivad DAO „targad lepingud“ olla tavakasutajatele raskesti mõistetavad, mis annab selle arendajatele – kes lepinguid hästi tunnevad – eelise organisatsiooni tegevuse mõjutamisel.

Inaktiivsed „osanikud“ – DAO-de tegevuses võib esineda olukordi, kus suur hulk valitsemistokenite omanikke jääb otsuste tegemisel inaktiivseks. Seetõttu ei pruugi olla võimalik muudatuste tegemine organisatsiooni „tarkades lepingutes“ või muude juhtimisotsuste langetamine. See võib põhjustada nii turvariske kui ka DAO tegevuse jõudmist tupikusse. Kirjeldatud olukorra vältimiseks võidakse DAO-de aluslepingutes seada otsuste vastuvõtmiseks madal häältekünnis, mis aga võimendab mõjuvõimu üksikute isikute kätte sattumise riski.

Otsustusprotsessi pikaajalisus – kuivõrd muudatuste tegemiseks DAO-de „tarkades lepingutes“ ning ka muude organisatsiooni puudutavate otsuste langetamiseks on keskse juhtimisorgani puudumise tõttu tarvis hääletust, võib otsustusprotsess olla pikaajaline. Näiteks investeerimisfondina tegutsevas DAO-s võib aga pikk valiku tegemise aeg tuua kaasa varalised kaotused investoritele.

DAO-de reguleerimisel on oluline leida tasakaal usaldusväärse õigusraamistiku ning tehnoloogia arendamiseks vajaliku eksperimenteerimisvabaduse ja innovatsiooni vahel. OECD rahapesuvastane töökond (FATF) kutsus oma hiljutises virtuaalvara ja selle teenusepakkujaid käsitlevas juhendis üles panema selle vastutuse DeFi rakenduste loojatele, omanikele ja operaatoritele, kes säilitavad rakenduse üle kontrolli või piisava mõju, isegi kui need rakendused näivad detsentraliseeritud.