Jogi melléklet

Külgazdaság, LXIII. évf., 2019. március–április 19–31. o.)

A blokklánc-technológia nemzetközi kereskedelmi jogi összefüggései

KIRÁLY PÉTER BÁLINT

A 21. század elején a technológia rohamos mértékben fejlődik. Naponta jelennek meg újabb és újabb, az életünket megkönnyítő innovációk. Ezek közé tartoznak a blokkláncok és a hozzájuk kapcsolódó okosszerződések is, amelyek többek között a nemzetközi kereskedelmet is forradalmasíthatják. Az új technológiák jogi szabályozása azonban számos kérdést vet fel, amelyek közül a tanulmány kitér a bűncselekmények finanszírozásának, a transzparencia és magánérdek összehangolásának, az adatok sértetlenségének és valódiságának, és az interoperabilitásnak a kérdéskörére. Mivel a blokkláncokon keresztül határokon átnyúló tranzakciókat lehet lefolytatni, a felmerült problémákra a jogi és technológiai interoperabilitás szempontjait szem előtt tartó, nemzetközileg egységes megoldást kell találni, amely megteremti a biztonságos jogi környezetet és egyben ösztönzi az innovációt.

Journal of Economic Literature (JEL) kód: F10 Trade: General; K12 Contract Law; K20 Regulation and Business Law: General; K24 Cyber Law; K33 International Law.

I. Bevezetés

A blokkláncokat sokan már most a 21. század legfontosabb találmányának tartják, és jelentőségét tekintve az internethez hasonlítják. A blokklánc lényegében egy decentralizált vagy megosztott főkönyv, amely a kriptográfiai eljárásoknak köszönhetően alkalmas a tranzakciók hitelesítésére, méghozzá közvetítő személy vagy szerv nélkül. A blokkláncok segítségével anonim módon bonyolíthatunk le

https://doi.org/10.47630/KULG.2019.63.3-4.19

Dr. Király Péter Bálint, PhD-hallgató, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, Közigazgatási és Pénzügyi Jogi Tanszék. A SmartLaw Research Group tagja. E-mail: kiralypeterbalint@gmail.com

tranzakciókat. Alkalmazásuk rengeteg előnnyel járhat az élet különböző területein. Létrehozásuk célja az volt, hogy a hagyományos pénzügyi közvetítőrendszer hibáit kiküszöbölve egy gyorsabb, olcsóbb és biztonságosabb módszert hozzanak létre a pénzügyi tranzakciók lebonyolítására. Emellett biztosíthatják a tranzakciók transzparenciáját, igazolhatják az áruk származását, valós időben, megbízható és hiteles adatokkal láthatják el az hatóságokat, vagy pl. lehetővé tehetik a folyamatos adóbeszedést közvetlenül a tranzakciót követően emberi közreműködés nélkül. Felhasználási lehetőségeinek tárháza végtelen, az utóbbi időben pedig jelentős mértékben fel is gyorsult a blokklánc-technológiára épülő innovációk megjelenése, amely szükségessé teszi annak megvizsgálását, hogy vajon miként illeszthetők bele a blokkláncok és más kapcsolódó technológiák a jelenlegi jogszabályi környezetbe. A blokkláncok számos jogi kérdést vetnek fel, amelyek közül az alábbiakban a kereskedelmi jogi vonatkozásúakat kívánom felvázolni.

II. Fogalmi alapvetés[1]

A blokklánc egy megosztott *(distributed)* főkönyv vagy decentralizált adatbázis, amely nyilvános, és a kriptográfiai eljárásoknak köszönhetően hitelt érdemlően és visszamenőleg megváltoztathatatlan módon bizonyítja a rögzített adatokat (pl. megtörtént tranzakciókat) bármilyen közvetítő személy vagy szerv nélkül.[2] Egy ún. *peer-to-peer* protokollról van szó, ami azt jelenti, hogy a rendszerhez csatlakozó felhasználók számítógépei egy hálózatot alkotnak, és azon keresztül egymással közvetlenül kommunikálnak, központi számítógép nélkül. A blokklánchoz felhasználóként bárki csatlakozhat, és a csatlakozást követően tranzakciókat kezdeményezhetnek közvetlenül egymás irányába. Mindezt ráadásul anonim módon, a névtelenség fenntartása mellett tehetik meg. A tranzakciók hitelesítését is a felhasználók végzik a blokklánc rendelkezésére bocsátott számítógépes kapacitásuk által úgy, hogy a tranzakciókat blokkokba foglalva hozzáadják a főkönyvként működő blokklánchoz.[3]

Miként is történik mindez? A blokkláncok működését a *BitCoin* nevű blokklánc *Proof of Work* konszenzus mechanizmusának példáján keresztül szeretném bemutatni. A blokkláncok működésének lényeges eleme az ún. konszenzusmechanizmus, amely ahhoz szükséges, hogy a számítógépek megegyezésre jussanak a blokklánc frissítését illetően annak érdekében, hogy valamennyi számítógépen ezt követően

[1] A blokklánc-technológiához kapcsolódó fogalmakról lásd bővebben: *Glavanits–Király* [2018].
[2] *De Filippi–Wright* [2018], 13–14. o.
[3] *Reed* [2017], 3–5. o.

egységes legyen a blokklánc adattartalma.[4] A *BitCoin* esetén 10 percenként ún. blokkokba csomagolják a tranzakciókra vonatkozó adatokat, amelyeket ezt követően a hálózat számítógépei hitelesítenek (pl. megerősítik, hogy a vevőnek ténylegesen rendelkezésére állt az adott mennyiségű kriptovaluta).[5] Ezt követően az új blokk tranzakciókra vonatkozó adatsorát kiegészítik a megelőző blokk ún. fejrészével. A fejrész működését a személyi számhoz lehet hasonlítani, ugyanis a célja az, hogy általa azonosítható legyen az adott blokk. Mivel minden blokk rendelkezik fejrésszel és minden blokk tartalmazza a megelőző blokk fejrészét, ezért a blokkok sorozata egyfajta láncot alkot (innen a blokklánc elnevezés), amelyet végigkövetve eljuthatunk a legelső tranzakcióit magában foglaló eredeti blokkig. Miután a megelőző blokk fejrészét is hozzáadták az új blokkhoz elkezdődik az abba foglalt adatok titkosítása egy kriptográfiai rejtvény megfejtése révén.[6] A blokkláncot működtető valamennyi számítógép (az ún. bányászok) azon verseng, hogy melyikük tudja leghamarabb megoldani ezt a kriptográfiai rejtvényt, ugyanis amelyikük elsőként oldja meg, *bitcoint* (vagy más blokkláncok esetén másfajta kriptovalutát) kap jutalmul munkájáért. Ezt követően az új blokkot hozzáadják a blokklánchoz, majd megosztásra kerül a rendszer valamennyi számítógépén.[7]

A tranzakciók gyakorlatilag megváltoztathatatlanok, miután a blokklánchoz adták őket. Ennek oka, hogy a teljes blokklánc – amely folyamatosan frissül – megtalálható valamennyi számítógépen, és minden blokk utal a megelőző blokkra. Ennek eredményeként a rögzített tranzakciók elméletileg megváltoztathatatlanok. Ahhoz ugyanis, hogy egy hacker módosítani tudja valamelyik tranzakciót, ahhoz meg kéne változtatnia a tranzakciót magában foglaló blokkot, majd azt követően valamennyi a megváltoztatott blokkra épülő további blokkot, mivel valamennyi blokk tartalmazza a megelőző blokk fejrészét. Ráadásul ezeket a változtatásokat a blokkláncot működtető valamennyi számítógépen meg kellene tennie. Ez a blokkok hitelesítési mechanizmusa miatt csak akkor lehetséges, ha a hacker uralja a blokkláncot működtető hálózat számítógépes kapacitásának több mint felét, hiszen a tranzakcióra vonatkozó konszenzus létrejöttéhez a számítógépek több mint felének egyetértése szükséges.[8] Megfelelő mennyiségű számítógépes erőforrás rendelkezésre bocsátása esetén tehát azt mondhatjuk, hogy a blokklánc képes a tranzakciókat megbízható módon rögzíteni, mivel a teljes blokklánc folyamatosan frissítésre és megosztásra kerül a hálózat

[4] *Schwartz–Youngs–Britto* [2014].
[5] *Mukhopadhyay* [2018], 15–18. o.
[6] *Drescher* [2017], 23. o.
[7] *Hayes* [2014], 2. o.
[8] *Wurfel* [2018].

tagjai közt. Azaz minden egyes pillanatban a hálózat valamennyi számítógépe képes igazolni bármely tranzakció megtörténtét.[9]

Forradalmasíthatja a blokklánc a kereskedelmet az ún. okosszerződések révén (*smart contract*). Az okosszerződések számítógépes tranzakciós protokollok, amelyek képesek arra, hogy szerződés egészét vagy egy részét önvégrehajtóvá tegyék azáltal, hogy a felek között létrejött szerződés feltételeit átültetik számítógépes kódokba.[10] „*Az okosszerződés két vagy több felet és digitális javakat magában foglaló mechanizmus, amelynél egy vagy több fél javakat tesz bele az okosszerződésbe, majd ezeket a javakat a rendszer automatikusan elosztja a felek közt egy formula alapján, amelynek adatai a szerződés megkötésekor még nem voltak ismertek*."[11] Az okosszerződések lényege, hogy emberi közreműködés nélkül – pl. bíróságok nélkül – is végrehajtásra kerül a szerződés, vagyis az történik, hogy a blokklánchálózat számítógépei hitelesítik a szerződés végrehajtásának megtörténtét. Elméletileg bármely szerződés átírható egy blokklánc alapú okosszerződéssé.[12] Az okosszerződések tehát a felek közötti megállapodás végrehajtását kezelik és koordinálják egy decentralizált blokklánchálózaton keresztül. Az okosszerződésben a hagyományos szerződésekhez hasonlóan meghatározzák a szerződéses feltételeket és azok megsértése esetén alkalmazandó szankciókat.[13] Azonban az okosszerződés annyival több, hogy egyben ellenőrzi a feltételek teljesülését és végre is hajtja az ahhoz kapcsolódó következményt.[14]

III. A blokkláncok felhasználási lehetőségei a kereskedelem területén

A blokkláncok több ponton megkönnyítik a nemzetközi kereskedelem folyamatát.

Egyrészt a blokkláncok segítségével csökkenthető a nemzetközi kereskedelemhez kapcsolódó bürokrácia. A nemzetközi kereskedelemben az áru az útja során rengeteg, akár több száz kézen megy keresztül, mire eljut a céljához. Ennek során tömegével keletkeznek a dokumentumok, amelyek szükségesek az áru *A* pontból *B* pontba juttatásához és az ehhez kapcsolódó különböző jogi kötelezettségek teljesíté-

[9] *Kakavand–Kost De Sevres–Chilton* [2016], 4–5. o.
[10] *Rohr–Wright* [2017].
[11] *Buterin* [2014].
[12] *Liebkind* [2018].
[13] *Dewey–Amuial–Seul* [2016], 49–50. o.
[14] Smart Contracts. *BlockchainHub*, elérhető: https://blockchainhub.net/smart-contracts/.

séhez. A teljesség igénye nélkül e dokumentumok közé tartozik maga az adásvételi és fuvarozási szerződés, csomagjegyzék, számlák, a kereskedelem finanszírozáshoz kötődő iratok, fuvarokmányok, egészségügyi és származási bizonyítvány, vámnyilatkozat stb. Például ha tulipánokat szállítunk Hollandiából Kenyába, akkor ehhez jelenleg három különböző állami szerv által kiállított összesen hat okiratra van szükségünk. A blokklánc segítségével azonban, amint okosszerződés formába öntjük a tranzakcióról szóló szerződést, arról rögtön értesülnek az érintett hatóságok, akik azonnal ki tudják állítani a szükséges okiratokat (pl. az áru származásáról) online, a blokkláncon keresztül. Amint megvannak az áru továbbításához szükséges papírok, erről azonnal értesül valamennyi érintett személy, így időt és pénzt spórolhatnak meg. Szintén alkalmas a blokklánc arra, hogy az áruk reexport céljából történő, időleges behozatala esetén egyszerűbben megállapítható legyen, hogy valóban határidőn belül reexportálták-e a terméket vagy sem. Okosszerződés segítségével a behozatali vámok is automatikusan átutalásra kerülhetnek azt követően, hogy az áru megérkezett a vámkezelés helyére. A nemzetközi kereskedelem tehát magas adminisztrációs költségekkel jár, ráadásul az adminisztráció folyamata időigényes és ki van téve a hibázás és a csalás lehetőségének. Ezeket a problémákat lehetne orvosolni a blokklánc kereskedelmi alkalmazásával, hiszen a papírok helyett a blokkláncon rögzített minden jogosult számára hozzáférhető, valós adatok alapján tudnának dolgozni mind a felek, mind pedig a hatóságok.[15]

Másrészt lehetővé teszi, hogy elkerülhetőek legyenek a jogviták. Például ha online rendelünk egy terméket házhoz szállítással, és a szerződési feltételek közt szerepel, hogy a terméket a szerződés megkötésétől számított két napon belül kiszállítják, akkor a blokklánc rögzíti a szerződés megkötésének pontos idejét, majd a teljesítéssel a küldemény megérkezésének időpontját is. Ha viszont késedelmesen teljesítene, akkor a program automatikusan hozzáadja a fizetendő összeghez a késedelmi kamatot. Ezzel elkerülhetők a viták, hogy vajon jár-e árleszállítás a késedelmes kiszállítás miatt, vagy sem.[16]

Harmadrészt alkalmas lehet a tulajdonosi lánc és az eredetiség igazolására is. Például ha venni szeretnénk egy gyémántot és meg szeretnénk győződni arról, hogy az eredeti és valóban annyi karátos-e, amennyinek az eladó állítja, ahhoz el kell küldenünk egy szakértőhöz, ami akár heteket is igénybe vehet, ráadásul drága is. Továbbá külön meg kell győződnünk róla, hogy az eladó valóban tulajdonos-e és rendelkezhet-e a gyémánt felett. De mi van akkor, ha az eladó befolyásolta a szakér-

[15] *Ganne* [2018], 25–34. o.
[16] *Thompson* [2017].

tőt, vagy hamis iratokkal próbálja bizonyítani a tulajdonjogát? Erre kínál megoldást a blokklánc, amellyel a példabeli gyémánt kérdéses tulajdonságai azonnal igazolhatók, ráadásul gyakorlatilag meghamisíthatatlan módon.[17]

Negyedrészt a blokklánc segítheti a feleket a kereskedelem finanszírozásakor. A kereskedelmi tevékenység finanszírozása gyakorta elengedhetetlen, különösen jelentős értékű áruk esetén. Ennek oka, hogy az eladó értelemszerűen előre szeretné megkapni a pénzét, míg a vevő csak az áru megérkezését követően hajlandó fizetni, és természetesen egyik fél sem kívánja a szállítás költségeit vállalni. Éppen ezért van szüksége a feleknek több esetben a bankoktól ellátásilánc-finanszírozásra vagy hitellevélre. Mindezek azonban egyrészt időben és pénzben is költséges folyamatok, ráadásul a feleknek szüksége van egy közvetítő intézményre (esetünkben a bankra), amely biztosítja, hogy az egymást egyébként nem ismerő felek megbízzanak egymásban (jobban mondva egymás bankjában). Ezt a problémát küszöbölik ki a blokkláncok azáltal, hogy lehetővé teszik számunkra, hogy megbízzunk a másik félben anélkül, hogy ehhez egy közvetítő személyt vagy szervet kellene igénybe vennünk. A blokkláncokat eredetileg éppen azzal a céllal hozták létre, hogy ezáltal „kikerülhetők" legyenek e közvetítő intézmények, és ezáltal egy gyorsabb, olcsóbb és biztonságosabb módszert hozzanak létre a pénzügyi tranzakciók lebonyolítására. (A pénzügyi szolgáltatók észlelték, hogy a blokkláncok fenyegetik a pozíciójukat a pénzügyi tranzakciók lebonyolítása terén. Mára már a pénzügyi szolgáltatók is elkezdték fejleszteni saját blokkláncaikat a saját költségeik csökkentése érdekében.)[18] A blokkláncok emellett megkönnyíthetik az ellátásilánc-finanszírozást, különösen a kis- és középvállalatok számára, mivel a blokkláncon rögzített adatok segítségével a bankok egyszerűen nyomon követhetik a tranzakciós láncbeli pénzmozgásokat, a vállalatok pénzügyi történetét, és általában az ún. *„know-your-customer"* szabályok betartását. [19]

Végül a blokklánc-technológiával elérhető a kiberbiztonság és a transzparencia magasabb szintje, valamint alkalmassá teszi a tranzakciók automatikus és valós idejű végrehajtását az okosszerződéseken keresztül. A tranzakciók transzparenciája miatt a hatóságok is könnyebben ellenőrizhetik a különböző jogi kötelezettségek teljesítését. Lehetővé válik továbbá, pl. a folyamatos adóbeszedés közvetlenül a tranzakciót követően emberi közreműködés nélkül. A blokklánc valós időben, megbízható és hiteles adatokkal láthatja el a hatóságokat a felhasználókról – anélkül, hogy a

[17] *Bullock* [2017].
[18] *Holman–Stettner* [2018], 26–39. o.
[19] *Ganne* [2018], 17–19. o.

felhasználóknak kellene az adatokat bejelenteniük –, hiszen a rajta tárolt adatokhoz közvetlenül és azonnal hozzáférhet. Ennek következtében a hatóságoknak lehetőségük van arra, hogy ne csak utólagosan, retroaktív módon ellenőrizzék az adatok valódiságát, hanem azokat a tranzakciók megtörténtét követően rögtön megvizsgálhassák. Mindez elősegíti a hatóságok nemzetközi együttműködését, hiszen azok a blokkláncon keresztül ráláthatnak mind az érintett jogalany tevékenységére, mind a többi hatóság jogalannyal kapcsolatos cselekményeire.[20] Ehhez természetesen már nem csak a kereskedelem digitalizására van szükség, hanem a kapcsolódó szolgáltatások és kötelezettségek digitalizálására is. Ha ugyanis az állami hatóságok továbbra sem fogadják el a blokklánc alapú dokumentumokat, hanem papíralapú okiratokat kérnek az exportőr, illetve importőr vállalkozásoktól például a vámkötelezettségek teljesítésekor, akkor nem éri meg nekik pénzt befektetni egy újabb platform alkalmazásába és párhuzamosan működtetni azt az offline eljárás mellett.[21]

IV. Jogi problémák

A blokkláncok és az okosszerződések bár automatizálják a nemzetközi kereskedelmet, megteremtik a szükséges bizalmat a felek között közvetítő személyek és szervek igénybevétele nélkül, és ezáltal időt és pénzt spórolnak meg számunkra, azonban nem oldanak meg minden problémát. Sőt, jogi szempontból számos megoldandó kérdést vetnek fel. Az alábbiakban ezeket a felmerülő kihívásokat kívánom ismertetni.

Nem oldja meg a blokklánc a joghatóság kérdését, sőt még inkább megnehezítheti annak megállapítását. Ha belegondolunk, akkor a blokklánc egy olyan decentralizált főkönyv, amelynek tevékenysége egyik államhoz sem kötődik, akkor miként alakul a joghatóság kérdése az esetleges jogviták esetén? A blokklánc az okos szerződések által egyszerűsítheti a jogviták rendezését, de ha valamiért a felek mégis bíróságra kívánják vinni az ügyet, akkor továbbra is fennáll a joghatóság problémája, hiszen határon átnyúló, vagy online ügyleteknél ez mindig kérdéses lehet. Szintén nehézséget jelenthet, hogy melyik állam adóhatósága jogosult adót szedni a blokkláncon végrehajtott tranzakció után, hiszen felmerülhet a kérdés, hogy pl. hol keletkezett az érték, amit meg kívánunk adóztatni.

[20] *WU / NET Team* [2017].
[21] *Ganne* [2018], 27. o.

A blokkláncok veszélyét jelenti továbbá az, hogy alkalmasak lehetnek pénzmosásra, valamint a terrorizmus és egyéb bűncselekmények finanszírozására. Ez többek közt a blokkláncok által biztosított anonimitásnak köszönhető, továbbá annak a ténynek, hogy általuk kihagyható a közvetítő személy vagy szerv. Holott éppen ezek a közvetítő intézmények töltik be az „őrök" szerepét a pénzmosás és a terrorizmus finanszírozása elleni harcban, hiszen az ezek megakadályozását és felderítését szolgáló normák rajtuk keresztül érvényesülnek. A másik oldalról viszont éppen a blokkláncok főkönyv jellege jelentheti a megoldást erre a veszélyre, így akár kihasználhatjuk a bennük rejlő potenciált a pénzmosás és más bűncselekmények finanszírozásának felderítésére. A blokkláncokon ugyanis a tranzakciók mindenképp rögzítésre kerülnek, méghozzá nyilvánosan, és még ha az ember számára a pénz útja követhetetlen is, egy a pénzmosás kockázat elemző program lefuttatásával azonosíthatókká válhatnak az illegális tevékenységből származó összegek.[22]

További kérdést vet fel a transzparencia és a magánérdekek összehangolása. Megfelelő jogi védőhálót kell biztosítani a felhasználók számára a róluk tárolt adatok kapcsán. Ez különösen az üzleti titok esetében lehet releváns probléma, ugyanis a vállalkozásoknak érdeke fűződhet ahhoz, hogy az adataihoz ne férjenek hozzá pl. a versenytársai. Így szükséges lehet annak előírása, hogy pontosan mely hatóságok férhetnek hozzá a felhasználó blokkláncon tárolt adataihoz. Másik releváns kérdés e körben az elfeledtetéshez való jog, amelynek lényege, hogy mindenkinek biztosítani kell azt a jogot, hogy kérje adatainak törlését, ha annak felhasználása nem felel meg az adatvédelmi szabályoknak.[23] Emellett is lehetnek olyan esetkörök, amikor a jogszabály azt mondja ki, hogy bizonyos idő elteltével a tárolt adatot a nyilvántartásból törölni kell. A problémát ebben az esetben az jelenti, hogy a blokklánchoz egyszer már hozzáadott adat nem változtatható meg és nem is törölhető, vagy legalábbis a törléséhez ún. „*hard fork*ra" van szükség.[24] *Hard fork*ról akkor beszélünk, amikor a blokklánc protokollját akként módosítják, hogy annak eredményeként a korábban létrejött blokkok érvénytelenné válnak. Ezáltal gyakorlatilag törölhetők a korábban rögzített adatok egy esetleges hiba esetén. Természetesen ehhez is szükség van a többség egyetértésére.[25] A kérdés tehát az, hogy mi történik akkor, ha egy jogszabályi rendelkezés vagy bírói döntés ellenére a blokkláncban tárolt adatokat nem tudják törölni a fejlesztők, mert hiányzik az ehhez szükséges konszenzus.

[22] *Sprenger Balsiger* [2018], 1–3. o.
[23] *Walker* [2012], 272. o.
[24] *Bambara–Allen* [2018], 79–80. o.
[25] *Hacker* [2017].

Problémát jelenthet, hogy a nyilvántartott adatok sértetlenségében csak addig lehetünk biztosak, amíg a rendszerhez csatlakozó számítógépes kapacitás több mint felét az állam birtokolja. Valós veszélyről van szó, amelyet mi sem bizonyít jobban, mint hogy 2019 januárjában az *Ethereum Classic* nevű blokklánccal szemben egy ún. 51 százalékos támadást fedeztek fel. A hackerek 1,1 millió dollár értékű kriptovalutát tulajdonítottak el. Ezt az tette lehetővé, hogy a hackerek a nevezett blokkláncot működtető számítógépes kapacitás több mint felével rendelkeztek, és így képessé váltak az ún. *double spending-re*.[26] A double spending az a jelenség, amikor egy adott egység kriptovalutát kétszeresen költenek el, kihasználva azt, hogy kriptovaluta nem más, mint egy digitálisan tárolt adat, amely könnyen reprodukálható. Az elkövető a double spending során elhiteti a blokklánccal – pontosabban a hitelesítést végző számítógépekkel –, hogy egy adott tranzakció nem történt meg, ami által lehetővé válik, hogy a meg nem történtté tett tranzakcióban elköltött kriptovaluta ismételten felhasználásra kerülhessen. Lényegében felülírják a blokkláncot, és egy új tranzakciós láncolatot hoznak létre a korábbi helyett, úgy, hogy közben ismételten elköltik a kérdéses kriptovaluta-mennyiséget. Mindez ahhoz vezet, hogy megrendül a felhasználók blokkláncba vetett bizalma, holott annak működésének éppen a bizalom a központi eleme.[27] Kiváló megoldást kínálhat erre az EU esetében, ha valamennyi tagállam a GDP-je vagy lakosságszáma vagy valamely más mutató arányában lenne köteles bizonyos számú *node*-ot fenntartani, és a rendszer működéséhez rendelkezésre bocsátani. Rajtuk kívül más *node* nem csatlakozhatna a rendszerhez (vagy ha csatlakozhat, akkor is a tagállamok birtokolnák a *node*-ok több mint felét).

További probléma, hogy a blokklánc csak a bevitt adatok sértetlenségét tudja biztosítani, de a bevitt adatok valódiságát nem. Tehát ha biztosítani tudjuk is, hogy a bevitt adatokat senki nem változtatta meg jogosulatlanul, azt továbbra sem tudjuk pusztán a blokklánc alkalmazásával biztosítani, hogy a bevitt adatok megfelelnek a valóságnak, és nem hamis vagy téves adatokat vittek fel a blokklánc főkönyvébe. Természetesen felmerülhet valakiben a kérdés, hogy ez miért is jelent problémát, hiszen a jelenlegi főkönyvek is így működnek: egy könyvelő is dönthet úgy, hogy hamis adatokat ír be a főkönyvbe, illetve az is előfordulhat, hogy emberi hibából kifolyólag tévesen rögzített bizonyos adatokat. A könyvelők munkáját azonban ellenőrzik a könyvvizsgálat során. A problémát ezzel az jelenti, hogy a könyvvizsgáló személyével ismételten behozzuk a centralizáció intézményét az egyébként a decentralizáció elvét valló blokkláncok rendszerébe. Jogi szempontból ez valószínűleg ter-

[26] *Jenkinson* [2019].
[27] *Chiu–Koeppl* [2017].

mészetesnek hangzik, azonban nem szabad elfelejteni, hogy a blokkláncokat azzal a céllal hozták létre, hogy közvetítő személy vagy szerv (azaz állam, könyvvizsgáló, bank stb.) nélkül, ún. *peer-to-peer* módon (azaz közvetlenül) lehessen tranzakciókat lebonyolítani egy olyan rendszeren keresztül, amely esetén a felek közti bizalmat maga a program teremti meg. A bevitt adatok utólagos állami ellenőrzése tehát szembe megy a blokklánc lényegével, amelynek bevezetése a blokkláncok elkötelezett hívei körében minden bizonnyal jelentős ellenállásba ütközne. Ehhez kapcsolódó másik kihívás, hogy mi történjen a tévesen bevitt vagy hamis adattal. Miként lehet korrigálni a hibákat egy olyan rendszerben, ami arra épül, hogy ne lehessen utólag megváltoztatni a bevitt adatot?

Végül problémaként merülhet fel az interoperabilitás kérdése. Jelenleg az egyes államok önállóan kezdték el fejleszteni saját blokkláncaikat, amelyeken rögzített adatok nem érhetők el más blokkláncok felhasználói számára. Természetesen ez valahol érthető folyamat, hiszen az egyes államoknak a saját jogszabályaiknak megfelelő, azt végrehajtó blokkláncokra van szükségük. Mindez azonban feleslegesen megtöbbszörözi a nemzetközi kereskedelem rendszerét, hiszen az egyes vállalatoknak így valamennyi blokkláncon regisztrálniuk kell ahhoz, hogy hozzáférhessenek az azon tárolt adatokhoz és azon keresztül teljesíteni tudják kötelezettségeiket. Ehelyett célszerűbb lehet egy közös nemzetközi blokklánc létrehozása (amelyhez az is szükséges lenne, hogy nemzetközileg egységes követelményeket, formanyomtatványokat stb. fogadjanak el az államok), vagy az egyes nemzeti blokkláncokon található adatokat másik blokkláncra átkonvertáló közvetítő platform alapítása.[28]

V. Összegzés

A blokkláncrendszereket a 21. század elejének egyik legfontosabb találmányának tarthatjuk. A felhasználási lehetőségeik tárháza végtelen. Alkalmas lehet a tulajdonosi lánc és az eredetiség igazolására,[29] forradalmasíthatja a blokklánc a kereskedelmet az ún. okosszerződések révén,[30] és egyes szerzők pedig a pénzügyi közvetítőrendszer radikális változását vizionálják a megjelenésüknek köszönhetően, hiszen a jelenleg használt technológiákhoz viszonyítva egy olcsóbb, gyorsabb és

[28] *Ganne* [2018], 30–34. o.
[29] *Kim–Laskowski* [2017], 6–7. o.
[30] *Schroeder* [2015], 1–59. o.

közvetlenebb módját biztosítja a tranzakciók megvalósításának.[31] Sőt, egyes vélemények szerint teljesen feleslegessé teheti a ma ismert bankrendszert.[32]

Ahogy bemutatásra került, a blokkláncok a nemzetközi kereskedelem folyamatát is megkönnyíthetik. A piaci szereplők, valamint egyes államok észlelték az új technológiákban rejlő potenciált, ezért elkezdték fejleszteni saját blokkláncaikat. A jogi védőháló a blokkláncon kötött okosszerződések és azok végrehajtása kapcsán azonban még nem kiforrott. Nincsenek rendezve például a felelősségi és fogyasztóvédelmi kérdések, hogy mely hatóságok hatáskörébe tartozik a viták eldöntése (egyáltalán szükség van-e ilyenre, ha az is beprogramozható, hogy milyen jogsértés esetén milyen jogkövetkezményt alkalmazzon az okosszerződés, stb.). Ezen szabályok meghatározása azért is sürgető probléma, mert a különböző befektetőket, vállalatokat és bankokat távol tarthatja a blokkláncok alkalmazásától a bizonytalan jogi helyzet. Nehézséget okoz az is, hogy a jelenleg működő nemzetközi kereskedelemre fejlesztett blokkláncok esetén (pl. *We.trade*) az okosszerződésben csupán a fizetést garantáló elemeket rögzítik és automatizálják, míg a felelősség és egyéb kérdések továbbra is csak egy offline szerződésben kapnak helyet. Álláspontom szerint ahhoz, hogy a nemzetközi kereskedelem valóban gördülékeny módon működhessen, egy nemzetközi blokkláncra vagy a különböző blokkláncok közt hidat képező közvetítő platformra van szükségünk, mert a párhuzamosan működő blokkláncok csak feleslegesen megtöbbszöröznék a rendszert azzal, hogy például egy vállalatnak több blokklánchoz is csatlakoznia kell ahhoz, hogy a különböző ügyfeleivel kereskedni tudjon. Ahhoz, hogy egy egységes blokkláncrendszeren keresztül lehessen a tranzakciókhoz kapcsolódó valamennyi hatósági ügyet elintézni, ahhoz nemcsak egy közös platformot kell kifejleszteni, hanem egységes jogi követelményekre és szabályozási keretre is szükség van.[33] Véleményem szerint ennek a közös szabályozási keretnek a megteremtésében a nemzetközi szervezeteknek (például a Kereskedelmi Világszervezetnek) kellene élen járnia, és arra ösztönöznie az államokat, hogy az innováció során szem előtt tartsák a jogi és technológiai interoperabilitás szempontjait.

[31] *Koch–Pieters* [2017], 1–4. o.
[32] *Hockett–Omarova* [2016], 1208. o.
[33] *Ganne* [2018], 26–40. o.

Irodalomjegyzék

Bambara, Joseph J. – Allen, Paul R. [2018] (szerk.): Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions. McGraw-Hill Education, New York.

Bullock, Mike [2017]: Blockchain in Plain English. Elérhető: https://www.linkedin.com/pulse/blockchain-plain-english-mike-bullock

Buterin, Vitalik [2014]: DAOs, DACs, DAs and More: An Incomplete Terminology Guide. *Ethereum Blog* (May 6, 2014). Elérhető: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Chiu, Jonathan – Koeppl, Thorsten V. [2017]: The Economics of Cryptocurrencies – Bitcoin and Beyond. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048124

De Filippi, Primavera – Wright, Aaron [2018]: Blockchain and the Law: The Rule of Code. Harvard University Press, London.

Dewey, Josias N. – Amuial, Shawn S. – Seul Jeffrey R. [2016]: The Blockchain: A guide for Legal and Business Professionals. Thomson Reuters, Danvers, MA.

Drescher, Daniel [2017]: Blockchain Basics – A Non-technical Introduction in 25 Steps. Apress, New York.

Ganne, Emmanuelle [2018]: Can Blockchain revolutionize international trade? World Trade Organization, Genf. Elérhető: https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf

Glavanits Judit – Király Péter Bálint [2018]: A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége. *Jog-Állam-Politika,* 3. sz. (*Megjelenés alatt*)

Hacker, Philipp [2017]: Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2998830

Hayes, Adam [2014]: What factors give cryptocurrencies their value: An empirical analysis. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579445

Hockett, Robert C. – Omarova, Saule T. [2016]: The Finance Franchise. *Cornell Law School research paper,* No. 16–29. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820176

Holman, Daniel – Stettner, Barbara [2018]: Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches. In: [*N.n.*]: The International Comparative Legal Guide to: Anti-Money Laundering. Global Legal Group, London. Elérhető: http://www.allenovery.com/publications/en-gb/Documents/AML18_AllenOvery.pdf

Jenkinson, Gareth [2019]: Ethereum Classic 51% Attack — The Reality of Proof-of-Work. *Cointelegraph* (Jan 10, 2019). Elérhető: https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work

Kakavand, Hossein – Kost De Sevres, Nicolette – Chilton, Bart [2016]: The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. Elérhető: https://papers.ssrn.com/sol3/papers.cf m?abstract_id=2849251

Kim, Henry – Laskowski, Marek [2017]: Agriculture on the Blockchain – Sustainable Solutions for Food, Farmers, and Financing. Blockchain Research Institute, Toronto. Elérhető: https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3028164

Koch, Christoffer – Pieters, Gina C. [2017]: Blockchain Technology Disrupting Traditional Records Systems. *Financial Insights,* Vol. 6., Issue 2. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=29975 88

Liebkind, Joe [2018]: DAOs, Blockchain, and the Potential of Ownerless Business. Investopedia (Apr 9, 2018). Elérhető: https://www.investopedia.com/news/daos-and-potential-ownerless-business/

Mukhopadhyay, Mayukh [2018]: Ethereum Smart Contract Development – Build Blockchain-based Decentralized Applications Using Solidity. Pact Publishing, Birmingham.

Reed, Jeff [2017]: Blockchain – 4 in 1 Bundle Book: Blockchain, Smart Contracts, Investing in Ethereum. *FinTech*, [s.l.].

Rohr, Jonathan – Wright, Aaron [2017]: Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets. *Cardozo Legal Studies Research Paper,* No. 527. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104

Schroeder, Jeanne L. [2015]: Bitcoin and the Uniform Commercial Code. *Cardozo Legal Studies Research Paper,* No. 458. Elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2649441

Schwartz, David – Youngs, Noah – Britto, Arthur [2014]: The Ripple Protocol Consensus Algorithm. Elérhető: https://ripple.com/files/ripple_consensus_whitepaper.pdf

Sprenger, Pascal – Balsiger, Franziska [2018]: Anti-Money Laundering in Times of Cryptocurrencies. Elérhető: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf

Thompson, Collin [2017]: How does the Blockchain Work? (Part 2). The top 5 things that you need to know. The Blockchain Review (Oct 2, 2016, Updated August 10, 2017.) Elérhető: https://medium.com/blockchain-review/blockchain-essentials-for-dummies-ba2d8851f1ca

Walker, Robert Kirk [2012]: The Right to be Forgotten. *Hastings Law Journal,* Vol. 64., Issue 1. Elérhető: https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1194&context=hastings_law_journal

WU/NET Team [2017]: Blockchain: Taxation and Regulatory Challenges and Opportunities. A Background Note. Elérhető: https://www.wu.ac.at/fileadmin/wu/d/i/taxlaw/institute/WU_Global_Tax_Policy_Center/Tax___Technology/Backgrd_note_Blockchain_Technology_and_Taxation_03032017.pdf

Wurfel, Sarah [2018]: Blockchain is unhackable but these are 5 possible vulnerabilities of "the new Internet". *Blockchain Crypto Journal* (December 1, 2018). Elérhető: https://captainaltcoin.com/blockchain-hacks/