**Iván Soma**[1]

# Az okosszerződések, mint a bizalom helyreállításának módja

## Bevezetés

A mai világban mindennapossá váltak a szerződések. A jogalkotó által megalkotott jogszabályok és meghatározott keretek között, a magánfelek könnyedén létrehozhatnak szerződéseket. A 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban Ptk.) biztosítja a felek számára a szerződéses szabadságokat. A szerződést úgy lehet meghatározni, hogy legalább két fél kölcsönös, egybehangzó akaratnyilatkozata, amely jogokat és kötelezettségeket keletkeztet.

Megállapodások szerződés nélkül is létrejöhetnek két fél között. Egy jól működő és jóhiszemű társadalomban a szokásjogi normák elegendőek ahhoz, hogy a felek a megállapodás szerint fognak cselekedni. Ez a társadalmi kép sajnos egy idealista gondolat, amely nem jellemző a mai világra. A becsület értéke és jelentősége a gazdasági világban, ahol mindenki érvényesülni szeretne, eltörpült. *A contrario* kikövetkeztethető, ha a becsület teljes és sérthetetlen lenne, akkor a szerződésekre nem is lenne szükség, hiszen a felek közti megállapodások anélkül is teljesülnének.

Megállapítható, hogy a szerződések elsősorban azért vannak, hogy az esetleges hibás vagy nemteljesítés esetén a sértett fél az igényét érvényesíteni tudja a másik féllel szemben. Tehát a bizalom hiánya miatt kialakult kételyt próbálja ellensúlyozni a szerződés és ma már nem a szerződő partner tisztességében és jóhiszeműségében bízunk, hanem a szerződésben.

Az okosszerződések egy új utat nyitnak a szerződéses világ számára, amelyben a bizalom központi elem maradt, illetve a technológia nyújtott védelemnek köszönhetően lehet bízni bennük. A tanulmányban elemzem a szerződések és a bizalom kapcsolatát, majd bemutatom a blokklánc technológiát, amely az alapját adja az okosszerződéseknek. Végül pedig az okosszerződések vizsgálom meg.

## I. A bizalom a szerződések világában

A bevezetőben már említettem, hogy a szerződések fontos szerepet játszanak a társadalomban, hiszen az egymás közötti együttélés velejárói a megállapodások, amelyek jogi szankciókkal vannak biztosítva.[2] A szerződéskötések pillanatában a felek megvizsgálják, hogy a szerződés valóban megfelelő a számukra, illetve az kellően biztosított. A szerződő felek saját érzéseikre hallgatnak azzal a kérdéssel kapcsolatban, hogy megbíznak-e a másikban, illetve, hogy a későbbiekben a szerződés megfelelő teljesítése megtörténik-e.

A hazai jogrendszerben a Ptk. a legfőbb jogforrás a szerződések szempontjából (természetesen az Alaptörvény mint a magyar jogrendszer magja, a szerződéses jogviszonyokra hatással van). A Ptk. első könyve tartalmazza azokat az alapelveket, amelyek követése kötelező. Ezekből ki kell emelni a jóhiszeműség és tisztesség elvét. A jogszabály kötelezi a feleket, hogy a jogok gyakorlása és a kötelezettségek teljesítése során a tisztességnek megfelelően kell eljárni, azonban ennek a teljesülésében a felek csupán bizakodhatnak.

A megállapodások elsősorban a bizalmon alapulnak, azonban ennek hiánya miatt van szükség a szerződésekre, amelyeket az állam elismer, illetve szankciókkal segíti azok teljesítését.[3] A szerződések a társadalom számára azért vonzóak, mert az azokból származó jogokat, illetve kártérítésre való igényt bírói úton érvényesíthetik, amelyet az állam biztosít. Az

---

[1] Joghallgató, SZTE Állam- és Jogtudományi Kar.

[2] VÉKÁS LAJOS: *Szerződési jog.* ELTE Eötvös Kiadó. Budapest, 2021 17. p.

[3] VÉKÁS 2021, 21. p

igényérvényesítés azonban sok időt és pénzt vesz el, hiszen az eljárás nem mindig hatékony, ez a jogrendszert kritikája.

A Ptk. több biztosítékról is rendelkezik, amelyek célja a szerződés megszilárdítása. A szerződése bebiztosítására különös szükség van, ha a megkötésének időpontja és a kötelezettség teljesítése között hosszabb idő telik el. Az idő múltával ugyanis előfordulhat, hogy valamely fél érdeke a szerződés megfelelő teljesítése iránt megszűnik.[4] Ez esetben is megállapítható, hogy minél nagyobb az érdekváltozás esélye a szerződés létrehozásának idejekor, annál több biztosítékban állapodnak meg a felek.

Fontos megemlíteni a szerződési szabadság elvét, amely az Alaptörvény által biztosított vállalkozási szabadságon és a tulajdonhoz való jogon alapul.[5] A magánautonómia elismeréséből származik a szerződési szabadság, amelyet a Ptk. is tartalmaz. A szerződési szabadság három elemből áll: a felek szabadon köthetnek szerződést, szabadon választják meg a szerződő felet és szabadon állapítják meg a szerződés tartalmát.[6] Ez a három elem biztosít a félnek egy bizonyos döntési lehetőséget, hogy milyen szerződést szeretne kötni és kivel. A döntés során objektív és szubjektív érvek is felmerülhetnek a félben, maga a bizalom is egy érv, hiszen két vagy több választási lehetőség közül inkább azt választják a szerződő felek, amelyikben jobban megbíznak.

A Ptk. több biztosítékot is rendez: kötbér, foglaló, jótállás, jogvesztés kikötése, tartozáselismerés.[7] Továbbá vannak a teljesítés fedezetének megerősítésre létrejött eszközök: zálogjog, kezesség, garanciavállalás.[8] Ezek a biztosítékok elősegítik a szerződés teljesítését, azonban nem tudják azt garantálni. Végső soron a szerződés megkötésének pillanatában a felek csak bizakodhatnak annak teljesülésében.

Az okosszerződések ezt a problémát küszöbölik ki. Az angol a *trustless* szót használja az okosszerződések jellemzésekor, amelynek két különböző értelmezése van. Jelenthet bizalomhiányt, tehát azt, hogy meghatározott személyek nem bíznak meg egymásban. A másik jelentése pedig a bizalommentes, ez jellemzi a blokklánc rendszereket, mivel az okosszerződés ezen a technológián alapul, így ez rá is vonatkozik. A rendszer által használt algoritmusok miatt a szerződés végrehajtása nem igényel harmadik felet, tehát nincs szükség az államra sem. A felek az algoritmus működésében megbízhatnak és abban, hogy a rendszer harmadik fél segítsége nélkül is tökéletesen működik.

## II. A blokklánc technológia

Az okosszerződések megfelelő megértéséhez elengedhetetlen a blokklánc technológia megismerése. Az angol nyelveben a *blockchain* szót használják, amely tükörfordításban blokkláncot jelent. A szó két elemből áll: blokk és lánc. A technológia elmagyarázásához és vizualizálásához szokás használni az elemeket, a valóságban egyetlen blokklánc rendszer sem tartalmaz valódi láncot vagy blokkot.

A blokklánc lényegében egy adatbázis, amelybe bármilyen adatot fel lehet tölteni, azonban az adat onnan nem távolítható el.[9] A legfontosabb tulajdonsága, hogy a rendszer elosztott, amit meg kell különböztetni a centralizált és decentralizált rendszerektől. A centralizált rendszer esetében egy központi szerver van, amelyhez csatlakozik a többi felhasználó, így minden kommunikáció a központi szereplőn keresztül történik. A decentralizált rendszerben több

[4] VÉKÁS 2021, 163. p
[5] Magyarország Alaptörvénye: M) cikk (1) bekezdés, XIII. cikk (1) bekezdés
[6] VÉKÁS 2021, 38-39 p.
[7] VÉKÁS 2021, 163. p.
[8] VÉKÁS 2021, 171. p.
[9] TOM LYONS, LUDOVIC COURCELAS, KEN TIMSIT: *Blockchain and the GDPR*. in European Union Blockchain Observatory & Forum eublockchainforum.eu, 2018. 14. p.

központi szerver csatlakozik egymáshoz, lényegében csomópontokat hoznak létre.[10] Az elosztott rendszerben a hálózatban fellelhető számítógépek, tehát a felhasználók egymáshoz kapcsolódnak ezáltal csomópontok jönnek létre (angolul: *node*). Ez esetben a minden felhasználó összeköttetésben áll a másikkal, anélkül, hogy lenne egy harmadik központi személy, amely felügyelné a kommunikációt. A hálózatot alkotó felhasználók egyenrangú felek, nincsen alá-fölé rendelt szereplő.[11]

Az első blokkláncon alapuló rendszer 2008-ban jelent meg, ez volt a Bitcoin. Azóta több ezer blokklánc alapú hálózat jött létre, ezek eltérnek egymástól és a technológia fejlődésével ezek a rendszerek is egyre jobbak, gyorsabbak és új megoldásokkal állnak elő. A hálózatok egymástól eltérhetnek aszerint, hogy privát vagy nyilvános. A nyilvános rendszerekhez bárki csatlakozhat és bárki végrehajthat tranzakciót, ilyen a Bitcoin is. Az ilyen jellegű rendszerek esetében az abba bekerült adatokat bárki láthatja és megismerheti. A privát hálózatok esetén, azonban csak az lehet felhasználó, akit jóváhagynak.[12] Különbséget tehetünk a valós identitáson alapúló és pszeudonim[13] módon működő rendszerek között. Az okosszerződések esetén a valós identitáson alapuló rendszerek a lényegesek, mivel ezek az érintettel közvetetten összekapcsolható információkat is kezelnek, így a szerződő felek megismerhetik egymás valós adatait.[14]

A blokklánc technológia újítása az általa használt rendszer felépítésében rejlik. Tehát az, hogy a hálózatot a felhasználók alkotják központi szereplő nélkül. A felhasználók gondoskodnak a blokklánc megfelelő működéséről, annak fejlesztésébe beleszólhatnak és többség véleménye dönt. A blokklánc sikeressége annak megbízhatóságán és fejlettségén múlik, ez a felhasználókon alapul, ezáltal kijelenthető, hogy a hálózatot alkotók érdekében áll, hogy az megfelelően működjön. Véleményem szerint ebből az érdekből következik az, hogy a felhasználók bízhatnak egymásban, hiszen ugyanaz a cél vezérli őket: a blokklánc biztonsága és sikere.

Ez a fokú bizalom némi biztonsági érzetet ad a blokklánc felé, azonban a puszta bizalom nem védi meg a rendszert a *hacker* támadásoktól. A technológia másik újítása a védelmi mechanizmusában rejlik, amely nem egy, hanem két szintű. Úgy gondolom, hogy ez a kettős biztonsági védelem teszi különlegessé a blokkláncot, hiszen a mai világban nagyon fontossá váltak az adatok védelme, így nem csak az okosszerződések esetén hasznos a technológia, hanem az adatvédelem szempontjából is. Fontos kiemelni, hogy sajnos sikeres támadások így is érik a blokklánc rendszereket, azonban ezekből a támadásokból tanulva tehetik még erősebbé a rendszert és javíthatják ki a hibáit.

A kettős védelem megértéséhez meg kell ismerni a blokklánc rendszer technikai hátterét, tehát azt, hogyan is épülnek fel, milyen szabályok és protokollok vonatkoznak a hálózatokra. Korábban már említettem, hogy a blokklánc leegyszerűsítve egy adatbázis, bármilyen adatot eltárolhatunk rajta. A felhasználó által megadott adatok egy blokkba kerülnek, miután a blokk megtelik az bekerül a rendszerbe, de még nem csatlakozik a blokklánchoz. [15] A csatlakozást megelőzően a blokkot ellenőrzik a csomópontok, ha meggyőződtek, hogy az adatok nincsnek

---

[10] ESZTERI DÁNIEL: *A blokklánc mint személyes adatkezelési technológia GDPR-megfelelőségéről*. Állam és Jogtudomány LXI. évfolyam (2020/4). 25-26. p.

[11] ESZTERI 2020. 26. p.

[12] LYONS, COURCELAS, TIMSIT 2018. 14. p.

[13] A pszeudonim jelentése álnevesített személyes adat, tehát a természetes személy azonosítására alkalmas. Nem összekeverendő az anonim szó jelentésével, ugyanis ebben az esetben már nem lehet azonosítani az adott személyt. NAIH álláspontja: https://www.naih.hu/tajekoztatok-kozlemenyek?download=96:a-nemzeti-adatvedelmi-es-informacioszabadsag-hat

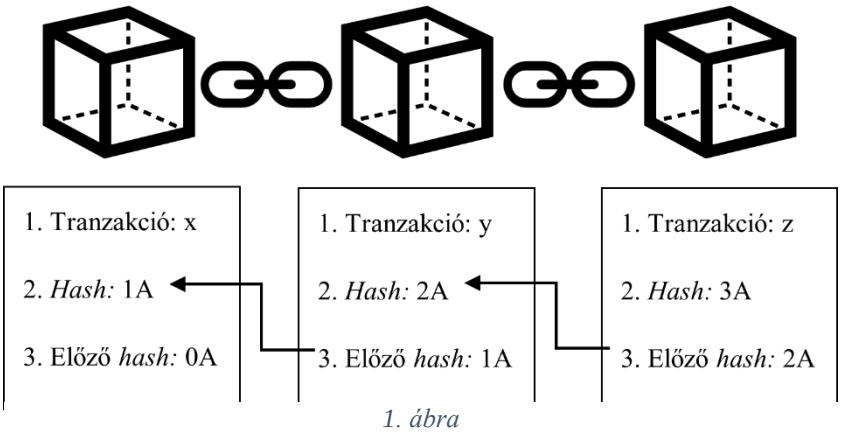
[14] ESZTERI 2020. 30-31. p.

[15] A blokkok eltérő mennyiségű adatot tudnak eltárolni. A Bitcoin 1 MB méretnek megfelelő adatot képes tárolni egy blokkban, de vannak olyan rendszerek, ahol 32 MB tárhellyel rendelkezik egy blokk. Forrás: https://www.bitstamp.net/learn/crypto-101/what-is-block-size/

manipulálva, akkor kapcsolódhat hozzá a lánchoz.[16] A csomópontok megegyezésen alapuló mechanizmusok segítségével vizsgálják a blokkokat (ilyen a *proof-of-work* vagy a *proof-of-stake*[17]), ezért a munkáért kapnak jutalmat a „bányászok". Ez a folyamat az első biztonsági kapu, mivel egy blokk, tranzakció ellenőrzése során a *node*-ok többségének kell megállapítania, hogy az adatok megfelelnek a valóságnak. Ebből következik, hogy a rendszerrel való visszaélés csak akkor lehetséges, ha a csomópontok többsége felett átveszik az irányítást.[18]

A tranzakció jóváhagyásával, illetve a csatlakozással a blokk kap egy azonosítót, ezt nevezzük *hash* értéknek. Ez lényegében egy ujjlenyomat, egy azonosító, amely miatt a blokk egyedi lesz.[19] A *hash* értéket a rendszer generálja egy algoritmus segítségével. Az algoritmus a tranzakcióból származó információt konvertálja egy számsorrá.[20] A blokkban található információk közül a legfontosabb maga az adat, illetve az ún. *timestamp*, vagyis időpecsét. Az időpecsét lényegében az igazolja, hogy az adott adat, a vizsgált időben létezett, valós volt.[21] A *hash* érték megváltozik, ha a blokkban szereplő valamely tranzakcióból származó információ vagy időpecsét megváltozik. Ez azért, fontos, mert a blokkok a saját azonosítójuk mellett tartalmazzák az eggyel korábbi (tehát a csatlakozás idején utolsó) blokk azonosítóját. Ha egy adott blokk *hash* azonosítója megváltozik, ez az érték nem fog megegyezi a hozzá kapcsolódott későbbi blokk által visszautalt azonosítóval (1. ábra). Ezt a hibát a rendszer észleli és jelzi a felhasználók felé.[22] Emiatt a mechanizmus miatt a blokkláncba bekerülő blokkok utólag már nem módosíthatóak, illetve ez biztosít egy plusz védelmet a *hackerek* ellen.

A blokklánc technológia előnyei közé tartozik, hogy gyors, nincsen harmadik (központi) fél, emiatt a tranzakciók is olcsóbbak. Továbbá állandóan működik és nagyobb védelmet kínál, mint egy banki rendszer. A technológia hátrányai között érdemes kiemelni, hogy a hálózat nagy




*1. ábra*

[16] KIANA, DANIAL: *Kriptovalutákról mindenkinek*. Panem Könyvek. Budapest 2022. 55. p.
[17] A *proof-of-work* jelentése „a munka bizonyítéka". Egy zár feltörése és a kódjának megfejtése időt, pénzt és energiát igényel, ha sikerül, akkor azt egyszerűen lehet ellenőrizni, hiszen a megadott kombinációval már könnyedén kinyitható a zár. A blokkláncokban a bányászok a „megoldást" keresik és az első kap fizetséget. A *proof-of-work* esetén az van előnyben, aki a legnagyobb számítógép kapacitással rendelkezik. A *proof-of-stake* jelentése „a letét bizonyítéka". Ebben az esetben a csomópont, hogy validáló lehessen feltesz egy meghatározott mennyiségű *tokent*, amely lényegében letétként működik. Ha az adott blokk nem megy át a többi csomópont ellenőrzésén, akkor a letétbe helyezett összeget elveszti. A *proof-of-stake* mechanizmusban annak van előnye, aki minél több *tokennel* vagy *kriptovalutával* rendelkezik. A *proof-of-stake* mechanizmust egyre több blokklánc hálózat használja, mivel kevésbé terheli a környezetet és ellenállóbb az esetleges támadásokkal szemben. Forrás: DANIAL 2022, pp. 71-72.
[18] TRINH ANH TUAN, GYŐRFI ANDRÁS: *A blokklánc*. In: Győrfi András (szerk.): Kriptopénz ABC. HVG könyvek. Budapest, 2019. 63. p.
[19] DANIAL 2022, 53. p.
[20] ESZTERI 2020 29. p.
[21] NAKAMOTO, SATOSHI: Bitcoin: *A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
[22] DANIAL, 2022, pp. 53-55.

költségek árán működik, hiszen minden számítógép elektromos áramot használ, emiatt nem kedvez a környezetvédelemnek. Egy blokklánc minél hosszabb, annál több időbe telik, hogy egy tranzakciót jóváhagyjanak. Hátrányai között említeném, hogy a technológia még mindig nem teljesen biztonságos és folyamatos *hacker* támadások érik. A jogalkotó számára is komoly fejtörést okoznak a blokklánc hálózatok, hiszen nehéz jogszabályok közé szorítani egy valóságban megfoghatatlan dolgot (pl.: az adatvédelmi szabályok hogyan tudnak érvényesülni egy ilyen rendszerben).

A blokklánc technológia még nagyon új, így nehéz eldönteni, hogy mire lehet felhasználni, illetve a jelenlegi felhasználási módok közül melyek lesznek azok, amelyek komoly potenciával rendelkeznek és a jövőben széles körű lesz az elterjedtségük. Napjainkban a kriptovaluta az, amely a legnagyobb figyelmet kapja, hiszen a társadalom ebben látja a legtöbb pénzt, illetve 2024-től lép hatályba az Európai Unió rendelete, amelynek célja a kriptoeszköz piac szabálykeretbe helyezése.[23]

Az egyszerű, lemásolható adatokkal és fájlokkal szemben, olyan egyedi információkat tud eltárolni, amelyek felett megjelenik a rendelkezés jog, illetve a tulajdonjog. A blokklánc képes különböző adatbázisok helyettesítésére és modernizálására (pl.: anyakönyvi kivonatok, ingatlan nyilvántartás), továbbá tulajdonjog keletkeztet virtuális alkotások felett (lásd *NFT*-k[24]). Az okosszerződések létrejötte is a technológiának köszönhető, amelyek egyre nagyobb jelentőséggel bírnak és nem kizárt, hogy teljesen megreformálják a mostani szerződéseket.

## III. Az okosszerződések

A tanulmány célja, hogy feltárja az okosszerződés és a bizalom kapcsolatát. Valóban helyreállítja a bizalmat a szerződésekben, vagy csak egy hamis ígéret? Az okosszerződés fogalmát *Nick Szabo* hozta létre 1994-ben publikált tanulmányában: egy digitalizált tranzakciós protokoll, amely automatikusan végrehajtja a szerződést.[25] Tulajdonképpen az előre meghatározott szerződéses feltételek teljesülése esetén a szerződés magától végbemegy, ezáltal megszeghetetlen.[26] *Szabo* egy kávéautomata működésével hasonlította, amely gép esetében, ha megfelelő mennyiségű pénzt dobunk be, akkor elkészíti a kávét (adott esetben visszajárót is ad), ha nem teszünk elegendő értékű pénzt, akkor nem készít kávét. Az automata programjában ezek a feltételek előre meg vannak határozva és amennyiben ezek megvalósulnak, akkor magától végrehajtja a további feladatot (vagyis a szerződést).[27]

*Szabo* négy elemet emel ki a szerződések vonatkozásában, amelyek szerinte az alapelvként követendőek az okosszerződések megalkotása során. Elsőként a megfigyelhetőség elve, amely biztosítja, hogy a felek megfigyelhessék egymás szerződésszerű teljesítését. Második az ellenőrizhetőség elve, amellyel a fél bizonyítani tudja külső személyek (akár bíróság) felé, hogy a szerződés teljesítették vagy megszegték. Szerinte ez a két elv képes meghatározni, hogy a szerződést szándékosan sértették meg vagy jóhiszemű hiba miatt.[28] Harmadik elv a korlátozott megismerhetőség, tehát a felek annyiban ismerhessék meg a szerződés tartalmát, teljesítésének feltételeit amennyire szükséges, ez kiterjed a harmadik személyekre is. A negyedik elv a

[23] AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a kriptoeszközök piacairól és az (EU) 2019/1937 irányelv módosításáról (továbbiakban: MiCA)
[24] *NFT: non-fungible token*, vagyis nem helyettesíthető token.
[25] NICK, SZABO: *Smart Contracts*. 1994. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
[26] ESZTERI 2020 31. p.
[27] NICK, SZABO: *Smart Contracts: Building Blocks for Digital Markets*. 1996. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
[28] SZABO 1996.

végrehajtás, ennek az elvnek a célja az, hogy minimalizálja a végrehajtás szükségességét. Ez úgy érhető el, ha a szerződésbe belefoglalnak néhány ösztönzőt, amelyek arra sarkallják a felet, hogy a szerződést teljesítse (kamat, zálog, kötbér, foglaló).

Az okosszerződéseket a blokkokba helyezik el és nem írásban kötik meg, hanem szoftveres formában készülnek el,[29] ezáltal egy kis programként működnek, amely végrehajtja a szerződést, ha a feltételek bekövetkeznek.[30] Az okosszerződések a való életben az *Ethereum* blokklánc hálózatnak köszönhetően jött létre.[31] A szerződés szempontjából fontos, hogy megfelelő védelemmel legyen ellátva és az illetéktelen személye ne jusson hozzá a tartalmához, a blokklánc technológia a titkosítást kulcsokkal oldja meg. Minden felhasználó számára a rendszer generál egy nyilvános és egy privát (magán-) kulcsot, ezek hosszú jelsorozatok, amelyek segítségével biztosított az információk biztonsága. Tegyük fel, hogy egy felhasználó információt szeretne küldeni egy ismerősének a hálózaton keresztül. Először a saját privát kulcsával kódolja az adatot, majd hozzárendeli a címzett fél nyilvános kulcsát. A rendszer többi felhasználója a címzett nyilvános kulcsának felhasználásával csak annyit ismerhet meg, hogy két felhasználó között tranzakció történik, viszont annak tartalmát már nem. Az így elküldött adat csak úgy ismerhető meg, ha a címzett fél hozzárendeli a saját privát kulcsát és csak ennek a segítségével tekintheti meg.[32]A kulcsok bonyolult sorozatokból állnak, amelyeknek a megfejtése a jelenlegi technikai háttérrel közel lehetetlen. A két kulcs között van kapcsolat, de a nyilvános kulcs alapján nem lehet megfejteni a privát kulcsot. *Szabo* elmélete alapján a nyilvános kulcs bárki által elérhetőnek kell lennie, míg a privát kulcsot a tulajdonoson kívül nem szabad másnak ismerni.[33]

A blokkláncba feltöltött okosszerződés folyamatának hitelesítését a csomópontok végzik. A szükséges információkat ismerniük kell ahhoz, hogy a szerződést hitelesíteni tudják (pl.: pénzösszeg, utalás ideje, kriptopénztárca címe). Könnyebben megérthető egy bérleti szerződés példáján keresztül, ahol két fél van: bérlő és bérbeadó. A valóságban gyakran előfordul az a helyzet, hogy valamelyik fél nem teljesít, a bérleti szerződés esetén előfordulhat, hogy a bérlő előre kifizeti a kauciót és bérleti díjat, azonban a bérbeadó nem adja oda a kulcsot vagy a bérbeadó előre odaadta a kulcsot, de a bérlő később sem fizeti ki a szerződésben foglalt összeget. A felek az okosszerződésben meghatározhatják, hogy az összeg kifizetését követően a kulcs automatikusan átkerül a bérlőhöz (pl.: megkapja a lakás belépőkódját SMS-ben).[34] Az okosszerződések segítségével megvalósulhat az ún. okos tulajdon (*smart property),* amely a szerződés teljesülését követően automatikusan ahhoz a személyhez társítja a kulcsot, aki a tulajdonosa a dolognak (pl.: lakás, autó).[35]

Az online vásárlás során a bizalom fontos kérdés, hiszen a fogyasztó a vásárlásakor nem ismerheti meg, nem nézheti meg közelről az adott terméket, nem találkozik az eladóval. Az ilyen vásárlások sokszor kudarcba fulladnak, hiszen elképzelhető, hogy a terméket előre kifizetik, viszont az nem érkezik meg és az eladó kötelezettségének teljesítése nélkül eltűnik. Az online vásárláskor olyan okosszerződéseket lehet kötni, amelyben a vevő fél számlájáról a termék ára letétbe kerül, addig, amíg a terméket át nem veszi. A termék átvételekor aláírásával igazolja, hogy átvette a csomagot, ezt követően a pénz átkerül az eladó számlájára. Amennyiben

[29] ÜVEGES ANDRÁS JÓZSEF: *Az Európai Unió Általános Adatvédelmi rendeletének (GDPR) egy értelmezése a blokkláncalapú rendszerekben*. In.: Deák Anita (szerk.): Felderítő Szemle. Katonai Nemzetbiztonsági Szolgálat, Budapest XIX. (2020). 1. szám. 202 p.
[30] BÁGI VERONIKA et al.: *A kriptovaluták lehetséges megjelenése a magyar jogrendszerben*. Kinstellar. 2017/18. II. félév 13. p.
[31] TUAN, GYÖRFI 2019, 72. p.
[32] ESZTERI 2020, 28. p.
[33] SZABO 1996.
[34] TUAN, GYÖRFI 2019, 73. p.
[35] SZABO 1996.

a termék nem megfelelő és visszaküldésre kerül (ha ez biztosított az eladó részéről), akkor a folyamat megfordul és a pénz addig van letétbe, amíg a csomagot az eladó fél át nem veszi.

Korábban kifejtettem, hogy a bizalom miként hat a hagyományos szerződésekre. Az okosszerződések esetében a felek megbízhatnak az algoritmusban anélkül, hogy közvetítőre vagy harmadik megbízható félre lenne szükség. Tulajdonképpen a másik fél szerződésszerű magatartásába vetett bizalom elvész, mivel az okosszerződés biztosítja, hogy mindkét fél megfelelően teljesítsen. Így kijelenthető, hogy az okosszerződések nem helyreállítják a felek egymáshoz fűződő bizalmát, hanem helyettesíti ezt, a rendszer biztonságán és megfelelő működésén alapuló bizalommal.

Az okosszerződések előnyei, hogy nincs szükség harmadik félre, emiatt olcsóbbak. A végrehajtás is automatikus, nem kell külső fél segítsége. Nem szükséges a szerződő fél magatartásába vetett bizalom (*trustless*) A szerződés külső felek számára is látható (a tartalma általában nem), illetve örökre megmarad a blokkláncban, így bármikor visszakereshető, átlátható. A blokklánc technológiának köszönhetően biztonságos, illetve utólagosan megmásíthatatlan (bár ez utóbbi hátrány is, hiszen, ha a felek közös megegyezéssel akarnak szerződést módosítani, akkor azt újból fel kell tölteni a blokkláncra). Az okosszerződés hátránya, hogy a technológia még nem fejlődött ki teljesen, a blokkláncokat folyamatosan érintő hibák, illetve támadások miatt sérülékenyek. Mivel új technológia ezért kiforrott jogszabály sincsen, amelyet alkalmazni lehet rá. [36]

## IV. Záró gondolatok

Az okosszerződéseknek még kell egy kis idő, hogy teljesen kiforrjanak, azonban technika és a társadalom fejlődésének köszönhetően, véleményem szerint előbb be fog következni mint azt sokan várják. Egyre nagyobb teret nyernek, nem véletlenül, hiszen nagyobb biztonságot nyújtanak a hagyományos szerződéseknél. Az okosszerződéseket úgy lehet megírni, mint egy programot, meg kell adni a feltételeket és azt, hogy ezek teljesülése esetén mit kell a szerződésnek teljesíteni (pl.: lakásbérlet esetén havonta a bérlő számlájáról levonja a lakbér összegét, cserébe a bérlő megkapja a lakás kulcsát).

Érdekes kérdés, hogy az okosszerződések milyen hatással lesznek az jogászok életére. Az okosszerződés tartalmához továbbra is kell a megfelelő szakami tudás, amivel a jogászok rendelkeznek. Azonban egy már korábban megírt okosszerződés később közel azonos tartalommal újra felhasználható lesz, ami már nem igényli a jogi tudást. Összegezve az okosszerződések veszélyt jelenthetnek az jogászok számára, azonban, ahogy a mesterséges intelligencia sem képes teljesen helyettesíteni az emberi munkát és gondolkodást, úgy az okosszerződések sem.

A társadalmunkban a bizalom kiemelkedő szerepet kap, hiszen mindennapos kapcsolataink a többi emberrel vagy tárgyakkal ezen alapulnak. Amennyire jelentős, annyira törékeny is a bizalom és ez kihatással van a szerződések világára is. A gazdasági élet szereplői között a kapcsolatot a szerződések tartják össze. Ha a felekben elveszik a bizalom azt az okosszerződés nem fogja helyreállítani. A felek az okosszerződések megkötésekor a rendszerben, a technológiában bíznak, nem pedig egymásban. Tehát kijelenthető, hogy a felek bizalmát nem helyreállítja, hanem megalapozza, létrehozza az informatikai technológiába való bizalmat. Véleményem szerint, az okosszerződések elterjedésének legnagyobb gátja az lehet, hogy az emberben könnyebben alakul ki bizalom egy másik személyben, mint egy informatikai rendszerben, technológiában, amelyet nem láthat meg a tárgyi világban, nem foghatja meg. Ha ezt a gátat a társadalom leküzdi, akkor az okosszerződés alapvető eszközzé válik a mindennapokban.

[36] https://ethereum.org/en/smart-contracts/

**Hivatkozások**

2013. évi V. törvény a Polgári Törvénykönyvről
Az Európai Parlament és a Tanács rendelete a kriptoeszközök piacairól és az (EU) 2019/1937 irányelv módosításáról
BÁGI VERONIKA et al.: *A kriptovaluták lehetséges megjelenése a magyar jogrendszerben*. Kinstellar. 2017/18. II. félév
ESZTERI DÁNIEL: *A blokklánc mint személyes adatkezelési technológia GDPR-megfelelőségéről*. Állam és Jogtudomány LXI. évfolyam (2020/4).
https://www.bitstamp.net/learn/crypto-101/what-is-block-size/
https://ethereum.org/en/smart-contracts/
KIANA, DANIAL: *Kriptovalutákról mindenkinek*. Panem Könyvek. Budapest 2022. 55. p.
Magyarország Alaptörvénye (2011. április 25.)
Nemzeti Adatvédelmi és Információszabadág Hatóság álláspontja: https://www.naih.hu/tajekoztatok-kozlemenyek?download=96:a-nemzeti-adatvedelmi-es-informacioszabadsag-hat
NAKAMOTO, SATOSHI: Bitcoin: *A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
NICK, SZABO: *Smart Contracts*. 1994.
https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
NICK, SZABO: *Smart Contracts: Building Blocks for Digital Markets*. 1996.
https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
TRINH ANH TUAN, GYŐRFI ANDRÁS: *A blokklánc*. In: Győrfi András (szerk.): Kriptopénz ABC. HVG könyvek. Budapest, 2019.
ÜVEGES ANDRÁS JÓZSEF: *Az Európai Unió Általános Adatvédelmi rendeletének (GDPR) egy értelmezése a blokkláncalapú rendszerekben*. In.: Deák Anita (szerk.): Felderítő Szemle. Katonai Nemzetbiztonsági Szolgálat, Budapest XIX. (2020). 1. szám.
VÉKÁS LAJOS: *Szerződési jog.* ELTE Eötvös Kiadó. Budapest, 2021