Vágujhelyi Ferenc
elnök
Nemzeti Hírközlési és Informatikai Tanács

Blockchain a közigazgatásban

Mi hívta életre a blockchaint?

A blockchain vagy blokklánc (a továbbiakban mindkét kifejezést használom) fogalma elég komplex. Könnyebb befogadni, ha előbb megértjük, milyen igény hívta életre. Az életünket meghatározó jogokkal és kötelezettségekkel (ingatlan, pénzkövetelés, szerződés) kapcsolatos információt hiteles formában szeretjük birtokolni. Egy szerződésben lefektetett jog kikényszerítését kedvezőbb a végrehajtással kezdeni, mint arról vitatkozni, hogy a felek egyáltalán mit is hagytak jóvá akaratukkal megegyezőként. Horribile dictu arról, hogy egyáltalán kik is a szerződő felek! A cél elérésének megvannak a hatékony és a kevésbé hatékony hagyományos és elektronikus formái, eszközei, a szóbeli megállapodástól a minősített elektronikus aláírással ellátott közjegyzői okiratig. A minősített elektronikus aláírásra épülő, joghatással bíró hitelesség alkalmazása egy jogrend hatókörén (pl. az EU-n) belül fenntartások nélkül működik. Ilyenkor van egy hitelesítő, aki egy állami hatóságtól kapta meg a működési engedélyt. A globális (EU-n kívüli) kapcsolatokban több ilyen közreműködőre is szükség lehet, sőt előfordulhat, hogy nincs is olyan közös technológiai platform, amely az összes érintett jogrendszerben támogatott. Előfordul az is, hogy a felek olyan ügyletbe kezdtek, ahol az állam közreműködését a legkevésbé sem kívánják, és a jogi kényszerítő erő helyett a technológiába épített garanciákra támaszkodva kívánják érvényesíteni követeléseiket (pl. illegális kereskedelem, adóelkerülés, bűnszervezetek). A fenti esetekben korlátozottan alkalmas vagy nem alkalmas az egyik ország hatósága által felügyelt hagyományos elektronikus aláírásra, és a jog által elismert hitelesítői *„tekintélyre”* épülő rendszer.

Az első blockchain megoldás a Bitcoin volt. Megalkotójának[1] az volt a célja, hogy egy olyan elektronikus pénzt teremtsen, amelyet virtuális pénztárcákban tartanak tulajdonosaik, mindenki csak a saját pénztárcájából költhet, de adott *„pénzérmét”* nem költhet el érvényesen kétszer. Hasonló szolgáltatást a világ valamennyi interneten szolgáltatást nyújtó pénzintézete biztosít. A bank központi rendszere csak a tulajdonosnak engedi meg, hogy a számlájához hozzáférjen, és adott pénz dupla elköltésének problémája fel sem merül egy centralizált rendszerben. Volt azonban még két követelmény, amelyet viszont a bankok nem tudnak teljesíteni: a rendszernek ne legyen központi felügyelete és legyen anonim! A rendszert felügyelő számítógépek (amelyeket hálózati csomópontoknak vagy node-oknak nevezünk) alkossanak egyenrangú hálózatot! Bárki (!) névtelenül (!) legyen képes ilyen node-ot csatlakoztatni a hálózatra, de akár több rossz szándékú node se hitelesíthessen a siker reményében szabálytalan tranzakciót. Na ehhez kellett a blokklánc. A felhasználók egyébként a bitcoin pénztárca (amely egy helyi adatbázis) segítségével férnek hozzá *„pénzükhöz”*, azaz nem kell egyfolytában egy vagy több node-hoz csatlakozniuk. Ma már számos más megoldás is született blokklánc alapon. Szerződéseket, megállapodásokat lehet ilyen módon tárolni, hitelesíteni. Ilyenkor a megállapodás fogalmaira vonatkozó szabály- vagy feltételrendszert be lehet programozni, amely ilyen módon technikai értelemben kikerülhetetlen, azaz kényszerítő erővel bír (pl. kriptovaluta átutalása következik be a megadott feltételek teljesülésének függvényében; kriptovaluta (rejtjelvaluta) az a kizárólag digitális formában létező fizetési eszköz, amelyet speciális rejtjelezési szabályoknak megfelelő műveletekkel hoznak létre, és számos tulajdonsága a hagyományos pénzéhez hasonló). Ilyen *„okosszerződéseket”* kezel pl. az Ethereum blokklánc rendszer saját kriptovalutáját, az ether-t használva.

A blokklánc tehát olyan informatikai technikai megoldás, amely külső tekintély (felügyelet, hatóság) nélkül, *egyenrangú szereplők között képes az adatok hitelességéről és a tranzakciók sorrendjéről konszenzust létrehozni.* A külső közreműködő hiánya a közigazgatás szempontjából azt jelenti, hogy se hatósági felügyeletnek, se külső döntéshozónak (pl. kamara, bíróság) nincs helye a rendszerben. A belső konszenzus függhet bizonyos, a rendszerbe programozott feltételek teljesülésétől, sőt ezektől függően akár ténylegesen végrehajthat érték-átruházást is (pl. közvetlenül kriptovalutában vagy értékek (pl. gyémánt[2]) nemzetközileg elfogadott követő-nyilvántartó rendszerében). Mielőtt tovább mennénk, tisztázzuk, mit is értünk a fókuszban lévő fogalmon, a hitelességen! A blokklánc ugyanazokat a technikai megoldásokat használja az adatok hitelességének formai ellenőrzésére, mint amelyet a közigazgatás a *„hagyományos”* elektronikus aláírásnál használ – a hozzá tartozó intézményi háttér nélkül. Így a blokklánc tárgyalása előtt jöjjön egy kis ismétlés!

[1] Satoshi Nakamoto névvel illetett személy vagy fejlesztői csapat (https://en.wikipedia.org/wiki/Satoshi_Nakamoto)

[2] https://www.everledger.io/

Mi az elektronikus hitelesség? (emlékeztető)

A közigazgatásban az információ hitelessége és a személyek azonosíthatósága az egyik központi kérdés. A hitelesség hagyományos kellékei mára elavultak, könnyen kijátszhatók, ezért a személyes megjelenésen és okmányon alapuló azonosítást is meg kellett reformálni pl. biometrikus azonosítók okmányon történő digitális elhelyezésével. A papíron elhelyezett, az információ hitelességét biztosítani hivatott kellékek, mint pl. a tollal történő aláírás, a pecsét, a dombornyomó az olcsó és kiváló minőségű multifunkciós másolóeszközök és 3D nyomtatók világában könnyen hamisíthatók, különösen az ügyintézéshez szükséges mértékig. Az elektronikus hitelességnek az Európai Parlament és a Tanács 910/2014/EU (eIDAS) rendeletében[3] meghatározott szabályai Magyarországon is hatályosak, alkalmazásuk kötelező. A 25. cikk (2) bekezdése szerint *„a minősített elektronikus aláírás a saját kezű aláírással azonos joghatású"*. Ezért praktikus, ha minden közigazgatásban dolgozó, sőt minden hivatásszerűen jogot alkalmazó szakember elemi szintű ismereteket szerez arról, hogy min is alapszik az elektronikus hitelesség.[4] Maga a jogi fogalom a blokklánc megjelenéséig kizárólag a hierarchikus hitelességi láncon alapult, amelynek végén a jog erejénél fogva hitelesnek tekintett elektronikus tanúsítványkiadó állt. A blokklánc egy hálózati konszenzuson alapuló hitelességére épül. A fogalom teljesen idegen a közigazgatás hierarchiára épülő logikájától, mégis több országban elindultak ezen az úton. De hová vezet ez az út? A jövőbe vagy zsákutcába? Az elektronikus hitelesség eszközeit használni könnyű, elvi alapjának megértéséhez viszont némi erőfeszítés szükséges. Aki az előbbi hivatkozáson található cikk gondolatmenetét követi, több mint elegendő ismeretre tesz szert. Ismétlésként a probléma és a megoldás természetéről következzen néhány gondolat!

Egy iratot (papír alapút vagy elektronikusat) akkor tekinthetünk hitelesnek, ha biztosak lehetünk abban, hogy

- ki írta alá,
- annak tartalma észrevétlenül nem változott meg az aláírás óta, és
- az aláíró nem tagadhatja le sikeresen az aláírás tényét.

Általában lényeges még az aláírás időpontjának bizonyíthatósága is.

Ezeket a feltételeket hagyományosan a *„papírra tintával"* módszerrel teljesítjük. Az ugyanezen technikát használó átvételi igazolás alapján pedig vélelmezhető, hogy a dokumentum az átvétel időpontjában már alá volt írva. A dokumentum adott példánya *„a hiteles"*, a hordozott információ általában másolható, de a hitelesség – a másolat ismételt hitelesítése nélkül – a másolt példányon elvész. Ennek az az oka, hogy a hagyományos hitelesség alapja az, hogy az információt hordozó tárgyon (pl. papíron) olyan jelet helyezek el (pl. kézi aláírás, pecsét), vagy olyan tárgyat kapcsolok elválaszthatatlanul hozzá (pl. bullát), amelyről azt feltételezem, hogy csak a szerző képes létrehozni, azaz a másológép nem. Az elektronikus irat viszont egy adatsor, amely végső soron nullák és egyesek sorozataként kerül tárolásra. Ettől az adatsortól várom el, hogy a hitelesség fenti feltételeit kielégítse, függetlenül attól, hogy milyen adathordozón vagy megjelenítő eszközön található, és kinek a birtokában van. Megjegyzem, hogy ez az adathordozó lehet papír is. A dokumentum teljes jelsorozatának papírra nyomtatott reprezentációja ugyanúgy megfelel az elektronikus hitelesség feltételeinek.[5] Ezért pontosabb lenne elektronikus helyett matematikai (még pontosabban számelméleti) hitelességről beszélnünk.

A fentiekből látszik, hogy az elektronikus hitelesség nem hasonlít a hagyományosra. Sőt, első ránézésre lehetetlen feladatnak tűnik egy elektronikus dokumentumról megállapítani, hogy ki hozta létre, amikor az dokumentumot reprezentáló adatsort mindenki éppen ugyanúgy tudja létrehozni (pl. másolással) vagy módosítani. Egy adatsor nem használható úgy aláírásra, mint a kézi aláírás, azaz pl. egy levél tartalma után kapcsolva, mivel erre az összekapcsolásra bárki képes, aki már kapott ilyen *„aláírással"* levelet. Ezért nem bír semmilyen hitelesítő erővel egy kézzel aláírt levélről vagy egy biztonsági okmányról készült fénykép. Ennek ellenére van megoldás.

Kezdjük azzal, hogy mit is írjunk alá? Nem ritka, hogy egy közigazgatási szerv nagy tömegű adatot ad át egy másiknak, abból a célból, hogy azt a fogadó saját nyilvántartásába felvegye, és hatósági munkájához felhasználja. Ilyenkor a fogadó félnek valahogy igazolnia kell azt, hogy ezeket az adatokat a másik hatóságtól kapta. Ha nem használunk elektronikus aláírást, ezt papíron kell megtenni. Ha például négymillió munkavállaló havi társadalombiztosítási jogszerzéséről beszélünk, akkor évente közel 50 millió, darabonként egy oldalra kinyomtatott adattartalmat kell praktikusan oldalanként igazolni. Ez képtelenség. Ehelyett egy hash függvénynek[6] nevezett számítást végeznek el az átadott teljes adatbázison, majd írnak egy néhány soros jegyzőkönyvet arról, hogy a fogadó hivatal átvett egy olyan adatbázist, amelynek hash-kódja pl. 4E710626535C1ABD6E-DE96C1C98239CF58811CDC5335B635F788F07D9. Ezt az átadó aláírja. Ha később kiderül, hogy az adatok megbízhatatlanok, és az átadó fél állítja, hogy a fogadó fél a betöltés során követhetett el hibát, mert az általa átadott adatbázisban nincs benne az adott hiba, akkor a következő a teendő: a küldő fél bemutatja a jó adatokat tartalmazó adatbázist, amelyet szerinte ő átadott. Ezt követően kiszámolják a hash értéket és megállapítják, hogy az egyezik-e a papírra vetett és ott aláírt, lepecsételt értékkel. Ha igen, a küldő félnek van igaza, ha nem, akkor bizony nem azt az adatbázist adta át. És ha a fogadó fél bemutatja azt az adatbázist, amelyre a jegyzőkönyvben szereplő értéket adja a számítás, akkor bizony igazolni tudja, hogy nem ő a felelős a rossz nyilvántartásért, hanem a küldő fél. A hash függvény tetszőleges méretű adatsorból olyan fix hosszúságú (pl. 256 bájtos) adatot számít ki, amelyet gyakorlatilag csak a

[3] http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32014R0910&from=HU

[4] Pl. Vágujhelyi Ferenc: A hitelességről (Jegyző és Közigazgatás XIX. évf. 2. szám 35. old., kifejezetten jogászoknak szánt betekintés)

[5] Logikai kísérlet: a kinyomtatott TELJES adatsorból pl. billentyűzeten keresztül újra létre tudom hozni a hiteles elektronikus dokumentumot, így a papírra nyomtatott verzió is hordozza a hitelességhez szükséges valamennyi információt.

[6] https://hu.wikipedia.org/wiki/Kriptogr%C3%A1fiai_hash_f%C3%BCggv%C3%A9ny

vizsgált adatsorból kaphatunk. A bemeneti adatok legkisebb változása az eredmény radikális változását vonja maga után, és visszafelé nem hajtható végre, azaz a hash értékből nem számíthatjuk ki azt a dokumentumot, amelyből készült. Alkalmazzuk az itt leírt papír alapú megoldást az elektronikus aláírásnál is! Ne magát a dokumentumot írjuk alá, hanem egy olyan, relatív kisméretű (hosszúságú) számot, amelyet csak az aláírni szándékolt elektronikus dokumentumból számolhattunk ki.

Hogyan hajtsuk végre az aláírást? Mivel minden elektronikus fájl értelmezhető számként – így az aláírandó hash-kód is – így maga az aláírási művelet egy számítást jelent a hash-kódon. Ezen számítás eredménye az elektronikus aláírás, amellyel szemben a következő elvárásaink vannak:

– az aláírást csak az hajthassa végre, aki erre jogosult,
– az aláírás és az eredeti dokumentum birtokában dönthesse el bárki, hogy az aláírás hiteles-e.

Mivel végső soron mindvégig számokról beszélünk, természetes, hogy a hitelesség ellenőrzését is egy számítás eredménye adja. A címzettnek rendelkezésére áll maga a dokumentum és az aláírt hash-kód. Ha az aláíró algoritmusnak (számítási módszernek) van egy olyan inverznek nevezett párja, amelyet az aláíráson végrehajtva az eredeti hash-kódot kapom, akkor a megoldás adott. A címzett kiszámolja a megkapott eredeti dokumentum hash-kódját, majd a megkapott aláíráson végrehajtja az aláírás inverz műveletét. Ha ekkor ugyanazt a hash-kódot kapta, akkor tudni fogja, hogy az aláírást az végezte, aki végre tudja hajtani az aláíró műveletet, azaz a jogosult. Fontos, hogy az inverz művelet ismeretében ne lehessen kikövetkeztetni az aláíró műveletet. Szerencsére vannak ilyen függvény párok. A gyakorlatban ugyanazt a műveletet végzi mindkét fél, de a bemeneti paraméterek kiegészülnek az aláíró esetében a titkos kulccsal, a címzett esetében a titkos kulcshoz tartozó nyilvános kulccsal. Ha az aláírási művelet pl. maradékosztályokon végzett hatványozás, akkor a két kulcs két hatványkitevő, amelyekre az a jellemző, hogy a titkos kulcs értékének megfelelő hatványozást elvégezve az aláírást kapom, majd az aláírást a nyilvános kulcs értékének megfelelő hatványra emelve az eredeti adatot, azaz a dokumentum hash-kódját kapjuk. Megfelelő méretű kulcsokat használva a nyilvános kulcs ismeretében a titkos kulcs irreálisan hosszú (akár az univerzum korát meghaladó) idő alatt számítható ki reális eséllyel. A titkos kulcsot az aláírónak természetesen titokban kell tartania.

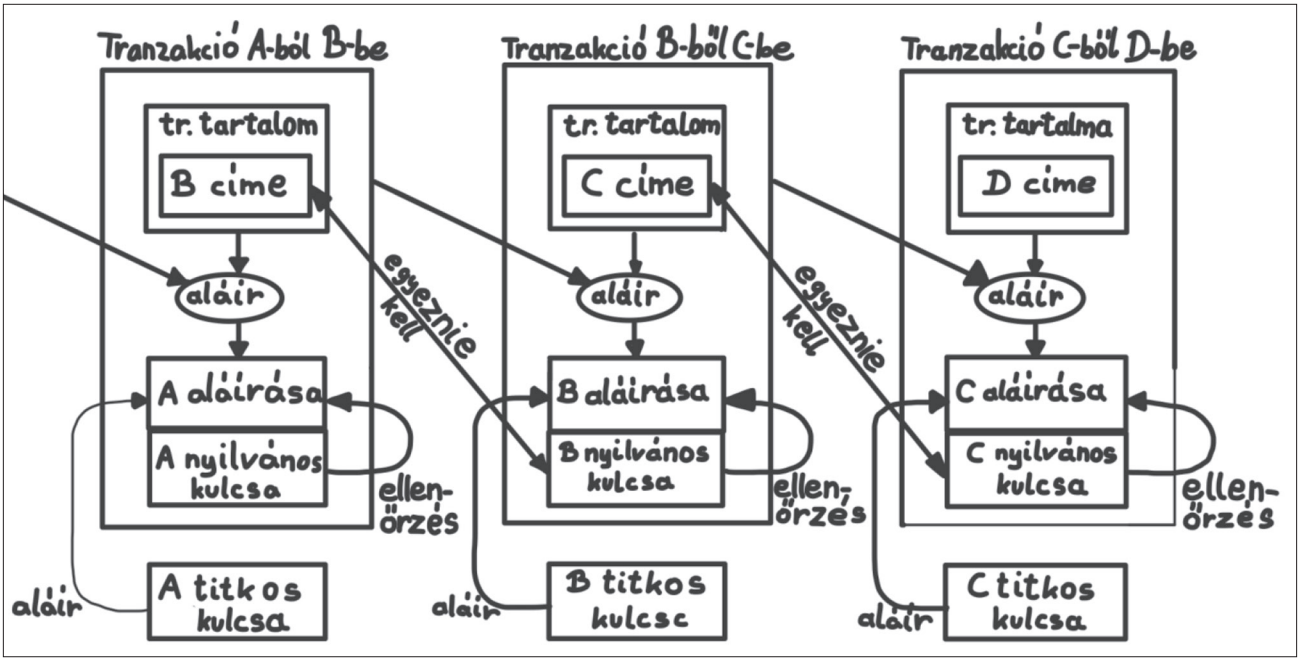
De honnan van a hitelesítésre használt nyilvános kulcs? A fenti művelet sikeres végrehajtása csak azt igazolja, hogy a nálam lévő nyilvános kulcshoz tartozó titkos kulccsal írták alá a dokumentum hash-kódját. Honnan tudom, hogy az konkrétan az a személy volt, aki a dokumentumon aláíróként szerepel? Itt következik az állam hatósági felügyeleti szerepe! A hatóság engedélyt ad az arra alkalmas szervezeteknek, hogy elektronikus hitelesítés-szolgáltatóként működjenek. Amikor az aláíró fél által használt program legenerálja a kulcspárt, a tulajdonosa elviszi ehhez a hitelesítőhöz vagy közjegyzőhöz. Ott pl. személyi okmányával igazolja magát, majd átadja a hitelesítőnek a nyilvános kulcsot egy olyan nyilatkozattal együtt, hogy a hozzá tartozó titkos kulcsot sajátjának ismeri el. Amikor valaki ellenőrizni akarja az aláírást, ettől a szolgáltatótól be tudja szerezni a szolgáltató elektronikus aláírásával felülhitelesített nyilvános kulcsot. A hitelesség biztosított.

A nyilvános kulcsokat tehát egy hitelesítő aláírja. Az ő aláírása jogi értelemben hierarchikusan magasabb szinten van, mint a *„közönséges”* aláíróknak. A hitelesítők gyakran olyan szolgáltatók, akik hierarchikusan még magasabb szinten lévő hitelesítők által tanúsított aláírást használnak. Ebből a rendszerből alakul ki a hierarchikus tanúsítványlánc vagy tanúsítványfa. Ez azonban nem mehet a végtelenségig. Kell, hogy legyenek legfelsőbb szintű ún. gyökértanúsítók. A belőlük ágazó tanúsítványfában szereplő valamennyi aláíráshoz akkor tartozik a kívánt joghatás, ha azok az állam által elismert gyökér-tanúsítói engedéllyel rendelkeznek. A hazai felügyeletet gyakorló hatóság az NMHH, de az Európai Unió eIDAS rendeletének megfelelően tanúsított minden aláírást el kell fogadni. A tanúsítványláncok használata, a hatósági engedélyezés és felügyelet módja fogalmilag is jól illeszkedik a szigorú hierarchiára épülő közigazgatásra.

Még a hatósági felügyelet alatt álló, hitelesített nyilvános kulcsokra épülő elektronikus hitelesség sem vert gyökeret a közigazgatásban, amikor a köztudatba berobbant a blockchain fogalma. A fentiek fényében van ennek egyáltalán értelme a közigazgatásban? A közigazgatásban nem az anonimitás, hanem a pontos azonosíthatóság az érték. Az ügyfél nem decentralizált, konszenzuson alapuló döntést vár, hanem azt, hogy a törvények által felhatalmazott hatóság ugyanezen törvények által szabott keretek közé szorítva, de a jog, az igazságszolgáltatás és a végrehajtó hatalom eszközeivel támogatva, hatékonyan kiszolgálja igényeit. Most hogy felfrissítettük a hash-kód és az elektronikus aláírás fogalmát, térjünk vissza az ezekre alapuló blokkláncra.

A blokklánc

A blockchain-t képzeljük el egy olyan főkönyvként, ahová soronként adatokat írhatunk. Minden sornak van tulajdonosa, azaz egy olyan felhasználó, aki rendelkezhet róla. Ők a kliens programmal/programokkal férhetnek hozzá az adataikhoz. Bárki írhat ilyen programot. A node-ok a hitelesítéssel és a blokkok létrehozásával foglalkozó számítógépek. Ők általában valamilyen haszon reményében végzik tevékenységüket. Node programot is bárki írhat, ha betartja a rendszer szabályait, így üzeneteit, sikeres blokk létrehozásait a többi node érvényesnek fogadja el. A kliensek a node-oknak továbbítják az általuk létrehozott tranzakciókat. A hitelesítést hasonló nyilvános-titkos kulcspárral végzik, mint az elektronikus aláírásnál, de itt a nyilvános kulcsot nem hitelesíti senki, általában nem lehet tudni, hogy ki áll mögötte. A kliens által generált nyilvános kulcs azonosítja a főkönyvi bejegyzéshez (pl. pénztárcában lévő értékhez) való hozzáférési jogot, így az ahhoz tartozó titkos kulcs használata önmagában igazolja az érvényességet, hiszen a titkos kulcsot értelemszerűen az ismeri, aki a kulcspárt generálta. Ha bármely kliens program betartja a protokollt, a tranzakcióit a node-ok elfogadják. Időnként a node-ok az új tranzakciókat egy fájlba írják, amely tartalmazza az előző fájl hash-kódját, azaz az előző fáj visszamenőleges módosításával

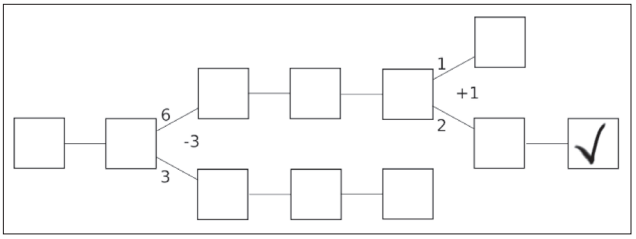


1. ábra
Blokklánc tranzakció a Bitcoin rendszerben.
A titkos kulccsal történik az elektronikus aláírás, és azzal lehet tranzakciót végrehajtani, pl.: pénzt költeni. A nyilvános kulccsal történik annak ellenőrzése, hogy a tranzakciót az arra jogosult hajtotta-e végre, és ez reprezentálja a „pénztárca" címét. A láncolatot alkotó érvényes tranzakciókat a blokkláncban teszik közzé (lásd 2. ábra).

megszakadna a hash-lánc. A blokkok ilyen logikai összekötéséből származik a blokklánc (blockchain) név. A sorok feletti felügyelet jogát át lehet adni másnak. Csak példaként – a tényleges működést inkább csak érzékeltetve – Bitcoin esetén a sor tulajdonosa az összérték változatlanul hagyása mellett fizethet, azaz másnak átadja a sorhoz való hozzáférés jogát. Ezt pl. úgy teheti meg, hogy ha 100 egysége van, abból átad 20-at valakinek, 5 századot *„költségtérítésként"* annak a node-nak, aki feldolgozza a tranzakcióját és 79,95 egységet saját magának, mivel azt nem költötte el. Minden tranzakció során nyilvános kulcsú digitális aláírással látja el a küldő az előző tranzakció hash értékéből, és a következő tulajdonos (tehát a fogadó fél) nyilvános kulcsából álló csomagot. Ezzel igazolja, hogy az összeget az adott nyilvános kulcs mögött álló fogadó félnek szánta. Mivel ennek titkos kulcspárjával csak ő rendelkezik, így majd csak ő költheti el. A hash, a cím és az aláírás bekerül az éppen aktuális blokkba, így a nyilvános kulcsunk ismeretében mások is igazolhatják, hogy érvényes volt a tranzakció. A blokk lezárása után már a blokkot megkapó node-ok (a hálózatot felügyelő számítógépek) az új tulajdonosoknak engedik az adott sorra a tranzakció végrehajtását. A főkönyv tehát tranzakciók sorozatát tartalmazza. Egy felhasználó onnan tudja, hogy mennyi Bitcoinnal rendelkezik, hogy megnézi a neki címzett, illetve az általa kezdeményezett tranzakciók egyenlegét. Így a blokkláncban a blokkok lánca mellett a tranzakciók is a blokkok között átnyúló logikai láncot alkotnak.

Eddig olyan, mint egy hierarchikus rendszerben. A hitelesítő node a szabályos tranzakciókat elfogadja, beírja a főkönyvbe és blokkonként hitelesíti. Ha egyetlen hitelesítő lenne, akkor az ő hibás vagy rossz szándékú működése megbízhatatlanná tenné a rendszert. Ezért van szükség a node-ok hálózatára, akik folyamatosan szinkronizálják egymással a jóváhagyott és a jóváhagyásra váró tranzakciókat. Ez viszont újabb problémát vet fel: melyik node által készített új blokk legyen a hálózat közös következő blokkja. A megoldás az, hogy legyen olyan bonyolult (időigényes) feladat egy blokk lezárása, hogy időegységenként (pl. 10 percenként) átlagosan csak egy node végezzen vele. A feladat egyszerű: a blokkra jellemző (hash) értékhez illesszünk olyan számot, hogy az arra kiszámolt hash érték kezdődjön pl. 5 darab nullával. Ehhez próba-szerencse alapon sok számítást kell végezni. Statisztikusan a leggyengébb teljesítményű node-nak is van valamennyi esélye, hogy ő találja meg először a helyes értéket. Ennek ellenére előfordulhat, hogy közel egyidőben zár le két különböző tranzakciókból összeállított blokkot két node. Ebben az esetben két verziója lesz a főkönyvnek. A node-ok egy részénél az egyik, másik részénél a másik. Ilyenkor az a szál *„nyer"*, amelyikhez rövidebb idő alatt írnak több blokkot, mint a másikhoz. A node-oknak ugyanis a beléjük programozott szabályrendszer szerint azt a főkönyvet kell folytatniuk, amelynek több lezárt blokk van az előzményében.

Egy csalárd céllal működő node így megkísérelheti olyan érmék kifizetésének címzettjét megváltoztatni saját magára, amelyet másnak már kifizetett. Ilyenkor rendelkezik a forrás titkos kulcsával, azaz a pénz az övé volt, az aláírási lánc szabályos marad. Ha egy ilyen blokkot sikerül lezárnia, a node-ok egy része ezt érvényesnek is fogadhatja el. Addigra azonban a node-ok többsége már az első költésről szóló tranzakciót igyekezett egy lezárt blokkba betenni, s ez jó eséllyel előbb sikerült nekik – mivel jóval nagyobb számítási kapacitást képviselnek – mint a csaló node. Ettől függetlenül a csaló megpróbálhatja érvényesként terjeszteni a saját lezárt blokk-



2. ábra
A négyzetként jelölt blokkok tranzakciók (lásd 1. ábra) sokaságát tartalmazzák. A szabálykövető node-ok azt a blokkot választják ki érvényes utolsónak, amelyben szabályos a blokk és tranzakciólánc, és a leghosszabb blokklánc előzi meg. Ennek kiszámításához kellett az elágazás óta a többség munkája. A csaló node-ok nem képesek annyi blokkot létrehozni, mint a többség, így az ő száluk egyre jobban lemarad, a hálózat annak használatát elutasítja.

ját, amellyel így két különböző verzióra (vagy szálra) szakad az addig egységes főkönyv. A kisebbségben lévő, ezért kevesebb számítási kapacitással rendelkező node (vagy node-ok) viszont lassabban tud új blokkokat létrehozni, így az ő szála egyre rövidebb lesz a másikhoz képest. A korábban együttműködő node-ok is átállnak a hosszabb szál használatára. A hibás blokkot tartalmazó szál elhal. Röviden ez a blokklánc konszenzuson alapuló hitelessége.

A módszer zseniális abból a szempontból, hogy több ezer egyenrangú számítógép hogyan tud egyetértésre jutni egy több ezer példányban lemásolt, és egymástól függetlenül vezetett, de folyamatosan szinkronizált nyilvántartás adattartalmáról. A módszer a rossz szándékú node-ok hamis adatait tartalmazó blokkokat az algoritmus sajátossága miatt *„kiejti"* a rendszerből mindaddig, amíg a csaló node-ok nem képesek számítási teljesítményben felülmúlni a szabályosan működőket. A teljes bockchain-ben rendkívüli informatikai beruházási költségeket jelent tényleges számítási kapacitás-többséget szerezni. Ha az ilyen hálózat többségben lévő csaló node-jai szabálytalanul működnek a saját hasznukra, akkor a károsultak azt hamar észreveszik. Ekkor pedig a felhasználók és a becsületes node-ok kilépnek a hálózatból, nullára írva annak értékét. A node-ok hardverébe történő beruházás gyorsabban megtérül a szabályos működésből befolyó bevételekkel, mint csalással.

Hogyan illeszkedik a közszférába?

Ki a gazdája egy blokklánc-alkalmazásnak?

Egy blokklánc rendszert felfoghatunk egy egyenrangú hálózatba kötött szuperszámítógépként. Így a sok-sok példányban lévő főkönyv minden node-é. Nyilvános blokklánc esetén, amelyhez bárki csatlakozhat, a tárolt adat mindenkié. A rendszert ugyanakkor csak a leprogramozott szabályok felügyelik, az egész rendszer felett senkinek sincs kontrollja. Ha valaki olyan node-ot regisztrál a rendszerbe, amelynek beprogramozott szabályai sértik a blokklánc szabályait, úgy a tranzakcióit nem hitelesíti a többi node (nem vesz át tőle adatot). Így viszont felmerül a kérdés: a tagok miről dönthetnek? Gyakorlatilag csak arról, hogy részt vesznek-e a rendszerben. Ez a szemlélet idegen a közigazgatástól.

De akkor hogyan tud fejlődni a rendszer?

Ez egy neuralgikus pontja a nyilvános blokklánc-rendszernek. A Bitcoin esetén öt programozónak van írási joga a node-ok által használt programok forráskódjához.[7] Ha új szabályt visznek be a rendszerbe, a node-ok többségének ezt el kell fogadnia, és telepíteni kell az új szoftvert, vagy saját szoftverüket kell megfelelően módosítani. Az ilyen rendszerek fejlődése állandó zajos viták, és a többség által elfogadható döntések mellett történik. A fejlesztők kiválasztása közel sem demokratikus elveket követ, és ezek a senki által nem választott programozók meghatározó módon befolyásolhatják sok-sok felhasználó életét. A szabályrendszert tehát nem választott képviselők felügyelik, a társadalmi kontroll hiányzik.

Milyen joghatóság van a blokklánc felett?

Mivel globális elosztott rendszerről beszélünk, ilyet nem lehet megnevezni. Egy-egy node is működhet olyan szerver felhőben (cloud-ban), amelyet fizikailag olyan gépek hoznak létre, amelyek sok-sok ország területén vannak. Ezért mondják, hogy a blokchain-ügyletek mögött nincs jogi, *„csak"* technológiai kényszer. Ez persze jóval hatékonyabb, mert automatikusan végrehajtásra kerül, de adott szituációban lehet nagyon igazságtalan. Ha például egy okosszerződés feltételeit definiáló kódot rosszul írnak meg, akkor az egyik fél kisemmizheti a másikat. Ez erkölcsi értelemben mindenkinek nyilvánvaló lesz, bizonyíthatóan sértheti valamennyi ország polgári jogát, ezt akár bíróság ki is mondhatja (a jogügylet érdemi tartalmáról). Ugyanakkor az blokchain-nen belül senki, de még az állam kényszerhatalma sem lesz képes a bajt orvosolni, ennek ugyanis matematikai akadályai vannak. Az állam annyit tehet, hogy saját területén igyekszik elérhetetlenné tenni a szolgáltatást, bár ennek is szerény lenne a hatékonysága. Az internet ilyen szintű korlátozását vagy könnyű kikerülni, vagy – ha valóban hatékony – óriási károkat okozna a gazdaságban (pl. a vállalatok azonnal külföldre telepítenék az érzékeny gazdasági és technológiai adataikat).

Milyen felhatalmazás alapján, kik módosítják?

Nincs demokratikus kontroll. Ha a fejlesztők nem félnek attól, hogy a felhasználók és/vagy node üzemeltetők otthagyják a rendszert, bármit megtehetnek.

Mi látszik a blokkláncban tárolt adatokból?

Minden. Ha például pénzügyi szolgáltatásként használjuk, az összes ügyfél valamennyi tranzakciója látszik. A tranzakciók mögött álló személyek viszont nem, mert ez az információ nincs a rendszerben. Pont fordítva működik, mint a bankok: náluk a számla tulajdonosa ismert, de a tranzakciók

[7] https://github.com/bitcoin/bitcoin vagy https://github.com/ethereum/

titkosak. Itt minden tranzakció nyilvános, de azok alanyai ismeretlenek.

A fentiek a ma működő nyilvános blokklánc megoldásokra, különböző mértékben vonatkoznak.

Következtetés

Mindenki mást lát kockázatnak és lehetőségnek, de abban valószínűleg egyetértünk, hogy a blokklánc-evangélistáknak valószínűleg nem a közigazgatási alkalmazások lebegtek a szemük előtt. Ugyanakkor a rendszer annyira rugalmas, hogy jól célzott módosításokkal sokkal közelebb hozható a közszféra elvárásaihoz. Zárt blokklánc létrehozható egy joghatóság alatt. Itt a felhasználókra és a node-okra szigorú belépési és működési szabályokat írhat elő az állam. A hálózatban használt kulcsokat például felül lehet hitelesíteni eIDAS szerinti aláírásokkal, így kizárva az anonimitást, vagy ún. *„fair anonimitási"* rendszert létrehozva, ahol előre meghatározott feltételek szerint, hatósági engedéllyel törhető fel az anonimitás. A közigazgatásban a node-okra is *kikényszeríthető* szabályozási kényszert alkalmazó, hatóság által felügyelt, a felhasználókat jól azonosító rendszert lehetne bevezetni. Az adatok teljes transzparenciáját újabb, felülhitelesítő rejtjelező kulcsok használatával lehetne megszüntetni. Ebben az esetben viszont kizárjuk az összes olyan elvárás teljesülését, amelyek a blockchain-t életre hívták. Az egyetlen kézzelfogható előny az elosztott rendszerből fakadó robusztus (és költséges) védelem a külső támadásokkal szemben. Összességében ezekkel a feltételekkel a blokklánc használata a közigazgatásban kevésbé lehetőség, inkább teher. A cikk elején említett nemzetközi tervek sorsát érdemes figyelemmel kísérnünk. Megvalósításuk esetén elsőként nyilván azt kell megfogalmazniuk, hogy milyen előnyt remélnek a választott technológiától. Várjuk a híreket!

A blockchain és a fejlődő világ

A fenti problémákat látva elismert szakértők vetették fel, hogy a blokklánc legyen inkább azon országok közigazgatási informatikai megoldása, ahol a centralizált rendszereket az állam nem volt képes létrehozni, vagy hatékonyan működtetni. Számos olyan országot találhatunk, ahol nincs működőképes földhivatali nyilvántartás. Sőt, a jogrendben sem tisztázottak a fogalmak és szabályok (gondoljunk bele, hogy egy ilyen nyilvántartás messze több jogosultságot és tényt kezel, mint a tulajdonjog). Egy ilyen országban az ingatlanokat a bitcoinokhoz hasonló módon lehetne átruházni, a komplexebb ügyleteket az Ethereum rendszer okosszerződéseihez hasonló módszerekkel kezelni. Egy ilyen rendszer még a bérleti jogviszony nyilvántartására is képes lenne, sőt – a bérleti díj fizetésétől függően – automatikusan állapítaná meg a rendelkezés jogát. Ugyanakkor a kezdeti állapotot ki hozná létre? Mire használható egy ilyen rendszer hiteles ősfeltöltés nélkül? Ez azonban – éppen a vázolt körülmények miatt – lehetetlen. Ezekben az országokban nem az informatikai megoldás hiánya a legnagyobb probléma, hanem az általunk ismert jogrend hiánya. Ráadásul az ilyen elképzelt környezetben a digitálisan írástudó polgárok, akik a jogérvényesítésben hagyományosan is jobb képességekkel rendelkeznek, egy újabb, számukra előnyt biztosító eszközt kapnak vélt vagy valós jogaik érvényesítésére. Lehetséges, hogy a blokklánc a társadalmi igazságtalanságok, szélsőséges esetben elnyomás új lehetőségeit teremti meg? A gyenge infrastruktúrájú országokban az új *„nyugati"* technológia nem a gyarmatosítás új formája?[8] Ahelyett, hogy ők is demokratikus kontroll alatt, jól működő, hierarchikus közigazgatást építenének ki, a fentiekben felvetett problémákkal küzdő, nehezen érthető, általuk nem kontrollálható irányt javasoljunk nekik? Azokban az országokban, amelyek etnikai, vallási vagy más okból végletesen megosztottak, és nincs lehetőség tartós konszenzust elérni, a blokklánc talán elfogadható megoldást jelent. Csak a bevezetéséről kell konszenzusra jutni, utána technikai akadálya van a szabályok felrúgásának. Ilyenkor a rendszer ellen lázadó fél csak a használat megszűntetéséről dönthet. A korrupció elleni harcban, ha az állam nem képes központi ellenőrző rendszereket kiépíteni, a blokklánc jó megoldás lehet, mert technikailag lehetetlenné teszi a visszamenőleges vagy logikailag szabálytalan tranzakciók rögzítést követő érvényesítését. Ebbe a politikai vagy közigazgatási hatalom nem tud beleszólni, mivel a nemzetközi node rendszerrel rendelkező hálózatban ennek egyrészt technikai, másrészt matematikai akadályai vannak. Az ilyen rendszerek létrehozása esetén persze létre kell hozni azt az érdekeltségi rendszert, amelyben a node-okat megéri működtetni. Ha viszont minden erőforrás (node) felügyelete a megosztottságtól vagy korrupciótól szenvedő állam hatáskörében van, akkor a rendszer mit sem ér. A zárt, hierarchikus rendszerben működő blokklánc értelme még alátámasztásra szorul.

Hogyan tovább?

Figyelemmel kell kísérnünk a nemzetközi hírforrásokat, műhelyeket, projekteket. Motiválni kell és el kell indítani a hazai műhelymunkát. De milyen kutatási-fejlesztési vagy innovációs célt tűzzön ki maga elé egy ilyen műhely? Közvetlen közigazgatási javaslatot nehéz lenne ajánlani, de két témát érdemes lehet megvizsgálni a közigazgatás határterületéről.

Az egyik az egészségügyi adatok hozzáférésének beteg általi engedélyezése az orvos számára. A finanszírozást végző szerv – hasonlóan bármely egészségbiztosítóhoz – ellenőrizni, tárolni és elemezni kívánja az ellátottak és az ellátások adatait, ezért ilyen tartalmú adattárházat hoz létre. Egy ilyen adattárházhoz azonban nem egyértelmű, hogy az ellátó orvos mikor, milyen feltételekkel férhet hozzá. Az pedig nyilvánvaló, hogy az adatokat a pénzügyi kontroll céljából kezelő szervezetnek a hozzáférési jog megadásához nincs köze. A blokklánc technológia használatával megoldható lenne, hogy a tényleges adatra hivatkozó referenciát a központi adattár automatikusan feltöltené egy blockchain-be úgy, hogy a beteg rendelkezhessen arról, hogy azt kinek továbbítsa, azaz adjon betekintési jogot. Ha a beteg egy orvosnak ilyen adatot látha-

[8] https://www.cryptocoinsnews.com/will-bitcoin-blockchain-build-finance-developing-economies/

tóvá akar tenni, akkor a rendszeren belüli tranzakcióval átadja neki az említett referenciát. Ha az adattárháznak az orvos rendszere ezt bemutatja, és a tranzakciót valóban a beteg aláírásával (titkos kulcsával) hitelesítették, az adathoz hozzáférést ad (akár meghatározott időtartamra). A blockchain-be vetett bizalom megrendülése esetén az adattárház bármikor leválasztható a kizárólag hivatkozásokat tartalmazó rendszerről. Egy ilyen megoldás mellett érvként hozható fel, hogy az adat tulajdonosa maga a beteg, az adattárház gazdája csak adatkezelő. A hozzáférésről való döntés nem hatósági feladat.

Közbeszerzések. A blokklánc rendszerben tárolt adatok teljes transzparenciája, a visszamenőleges manipulálhatóság elleni biztonság igénye logikusan helyezi a közbeszerzési folyamatot a blockchain műhelymunka fókuszába. Az üzleti titkokat tartalmazó dokumentumoknak csak a hash-kódját kellene a manipulálhatóság kizárása miatt a rendszerben tárolni, de az eljárások átláthatóságot igénylő eseményei és adatai, mind a blokkláncba kerülnének.

Konkrét kutatási területet csak alapos tájékozódás után érdemes kiválasztani, de magát a tájékozódást már most sem nem korai elkezdeni!

Ez az írás tehát nem kiáltvány a blokklánc közigazgatásba történő bevezetéséért. Ugyanakkor a működő megoldások sikere, és megfontoltnak tartott kormányok támogató kezdeményezései arra figyelmeztetnek, hogy esetleg mi nem ismerjük fel a bonyolult technológia által a közigazgatás előtt feltáruló lehetőséget. Az átláthatóság és megszakíthatatlanság, azaz visszamenőleges manipulálhatatlanság két komoly érték. Vajon ki tudja-e *„bányászni"* ezeket a kincseket a technológiából a magyar közigazgatás?