BLOCKCHAIN ALKALMAZÁSI LEHETŐSÉGEK A KÖZGYŰJTEMÉNYEKBEN

Sík Zoltán Nándor[1]

Abstract

A cikk a blockchain-be való általános bevezetés után a közgyűjtemények esetén való alkalmazásokat veszi sorra, úgymint hitelesítés, felhasználó azonosítás, szerzői jogok kezelése, felhasználási engedélyek, belépők, jegyek digitális kezelése blockchain alapon. A cikk mindemellett a GDPR megfelelésre is kitér, valamint választási lehetőségeket vesz sorra a megvalósításhoz a már készen lévő keretrendszerek közül.

Blockchain application possibilities in public collections

After the general introduction of blockchain, the article takes into account its applications for public collections, such as authentication, user authentication, copyright management, usage licenses, digital access management based on blockchain. The article also addresses GDPR compliance and provides options for implementation from existing frameworks.

1. Az elosztott főkönyv és a blockchain

A jelen cikkben természetszerűleg csak a digitalizált, vagy már eleve digitálisan létező közgyűjteményi elemekkel foglalkozunk, hiszen a blokklánc (a továbbiakban az angol elnevezésével élve: blockchain) technológia alkalmazása csak ezen rendszerek és adatbázisok esetén értelmezhető. Mindenekelőtt meg kell különböztetnünk az Az elosztott főkönyvet (DL – Distributed Ledger) és azt megvalósító technológiát (DLT – Distributed Ledger Technology) a blochchain-től. Bár nem léteznek szó szerint *„kőbe vésett"* definíciók, de a distinkció e nélkül is megtehető.

Az elosztott főkönyv egy olyan decentralizált (központ nélküli) adatbázis, amelyet a különböző résztvevők kezelnek, és nincs olyan központi hatóság, amely bíróként vagy megfigyelőként közreműködne. (például a torrent protokollra épülő adatok is ilyenek).

A blockchain ezzel szemben pedig olyan infokommunikációs rendszer, amely decentralizált, adatbázisaként láncba rendezett adatblokkokat kezel, működése egyenrangú felek konszenzus kényszerérére alapul, valamint kriptográfiai algoritmusokat használ.

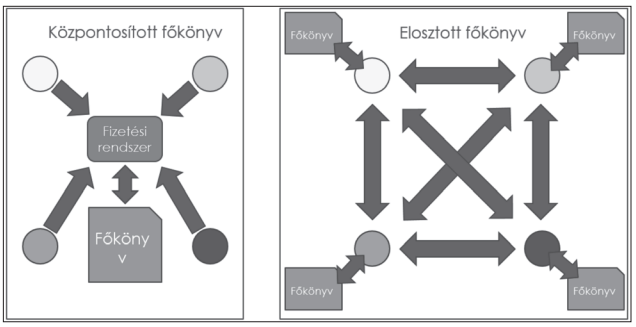
A blockchain tehát egy olyan, specializált elosztott főkönyv, amely a fentiek szerint további kritériumokat tartalmaz, amelyek a láncba rendezettség, az egyenrangú felek részvétele, az üzemeltető egyenrangú felek konszenzus kényszere, valamint a kriptográfiai algoritmusok használata. A blockchain-ben a fentiek mellett lehetséges számítógép programok tárolása és végrehajtása is, amelyeket okos szerződéseknek (a továbbiakban az angol kifejezéssel élve: smart contract) nevezünk.

Megjegyzendő, hogy léteznek más típusú elosztott főkönyvek is, amelyek nem blockchain alapúak, de hasonló tulajdonságokkal bírnak [ilyen pl. a tangle – egy fajta irányított aciklikus gráf rendszer (Directed Acyclic Graph – DAG), az Inter Planetary File System (IPFS), vagy az ún. hashgraph]. Ezekkel azonban a továbbiakban nem foglalkozunk.

2. A blockchainről általában

A blockchain megvalósítása végül is egy infokommunikációs rendszer, amely a fentiek szerint központ nélküli, a résztvevők egy jól körül írható részének (csomópontok, a továbbiakban angol kifejezéssel élve: node-ok) kényszer konszenzusára alapul abban a tekintetben, hogy mely adatok kerüljenek a blockchain-be. A node-ok közt kialakult konszenzust a blockchain protokollja (rendszer leírása) szerint a továb-

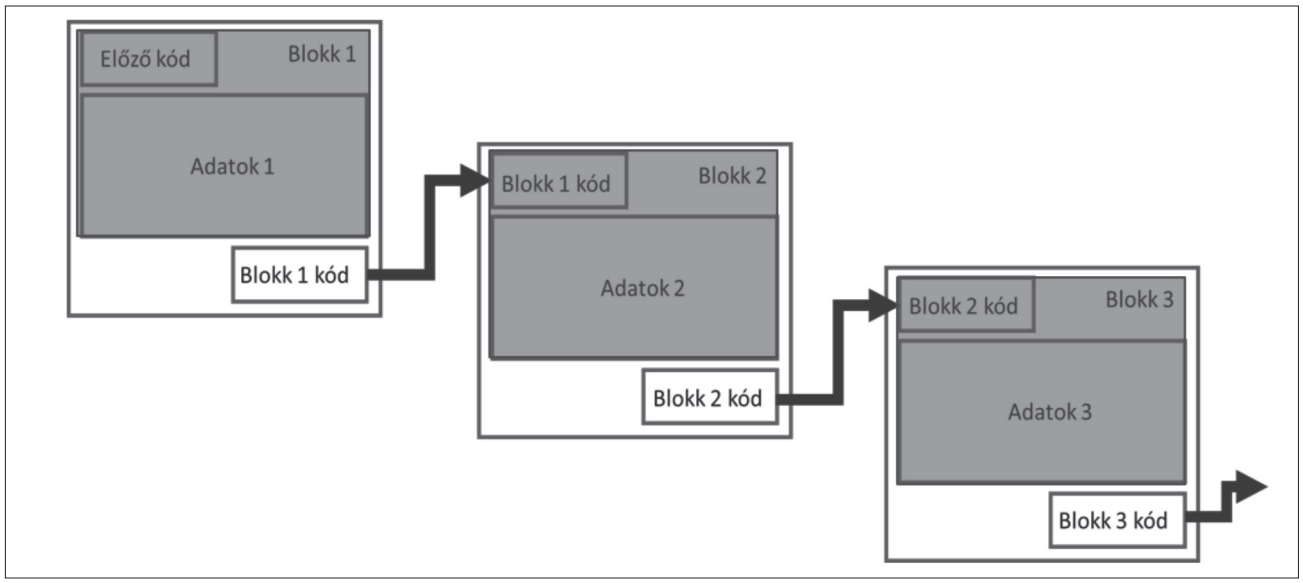
[1] Jogi szakokleveles villamosmérnök, MBA, politikai szakértő, valamint tőzsdei szakvizsgával és brókervizsgával rendelkezik. Villamosmérnöki diplomáját 1986-ban szerezte a Budapesti Műszaki Egyetemen. 1986-ban a SZÁMSZÖV Számítástechnikai Kisszövetkezetnél kezdett, 1987-től elnökség tagja. 1995-től 1998-ig az Integra Rt. igazgatója, majd vezérigazgató helyettese, 1998-1999-ig a Synergon Informatika Rt. üzletfejlesztési igazgatója, 1999-2000-ig a Hírközlési Főfelügyelet (ma Nemzeti Média- és Hírközlési Hatóság) informatikai igazgatója. 2000-2002-ig informatikai kormánybiztos, 2000-2003-ig a Nemzeti Hírközlési és Informatikai Tanács tagja, majd szakértője. 2011-től a Kormányzati Informatikai Fejlesztési Ügynökség elnöki tanácsadója. 2015. novembertől 2019 januárig a Nemzeti Hírközlési és Informatikai Tanács alelnöke. 2017-től a Magyar Államkincstár elnöki tanácsadója. Több szakkönyv és tudományos cikk szerzője.



1. ábra
A központi és az elosztott főkönyv (DL) közötti különbség

biakban minden részt vevő elfogadja, azaz a protokoll ezt kikényszeríti. A rendszer felépítéséből adódóan igen magas rendelkezésre állású, gyakorlatilag bármilyen adat tárolására alkalmas. Azonban a blockchain-ben praktikus okokból (pl. a rendszer működési sebessége), ha nincs erre feltétlenül szükség, fizikailag sokszor nem minden adatot tárolnak, csak az adatok digitális lenyomatát, más szóval kivonatát, zanzáját (a továbbiakban angol kifejezéssel élve: hash). A blockchain az „értékek i*nternetjé*”-nek is nevezhető, mivel a blockchain azonosítóját tudják. A rendszer kialakításából adódóan maga a blockchain biztosítja, hogy a rendszer – és legtöbbször a blockchain rendszerben résztvevő minden fél – tudja, hogy egy-egy adat (jelsorozat) pontosan kihez, melyik wallethez tartozik. Azonban ez nem jelenti azt, hogy a rendszer be is tudja azonosítani a wallet mögött lévő fizikai személt, vagy személyeket. Ebből következően a blockchain-ben tárolt adatnak így értéke van, mivel nem *„duplikálható”*, egyszerre csak egy tulajdonoshoz tartozhat. Más szóval a blockchain-ben tárolt adat nem úgy viselkedik, mint a digitális világban megszokott adatmásolás (copy-paste), hiszen az adott wallet és a benne tárolt adat csak az adott wallet-ben értelmezhető, hiába másoljuk, az a wallet-en kívül – köszönhetően a használt kriptográfiai algoritmusoknak – értéktelenné válik. Egészen pontosan olyan, mint egy kinyomtatott pénz, amelynek másolása egy rosszul sikerült pénzhamisításhoz hasonlítható. Mindamellett a blockchain-ben tárolt *„érték”* pénzként való értelmezése a mai napig vitatott az egész világon.

A blockchain rendszereknek azonban több fajtája is megkülönböztethető: azok lehetnek nyilvánosak (publikusak), amihez bárki, egyenrangú félként csatlakozhat (public blockchain), illetve nem nyilvános (privát) blockchain-ek, amik-



2. ábra
A blockchain láncba rendezett adatblokkjai

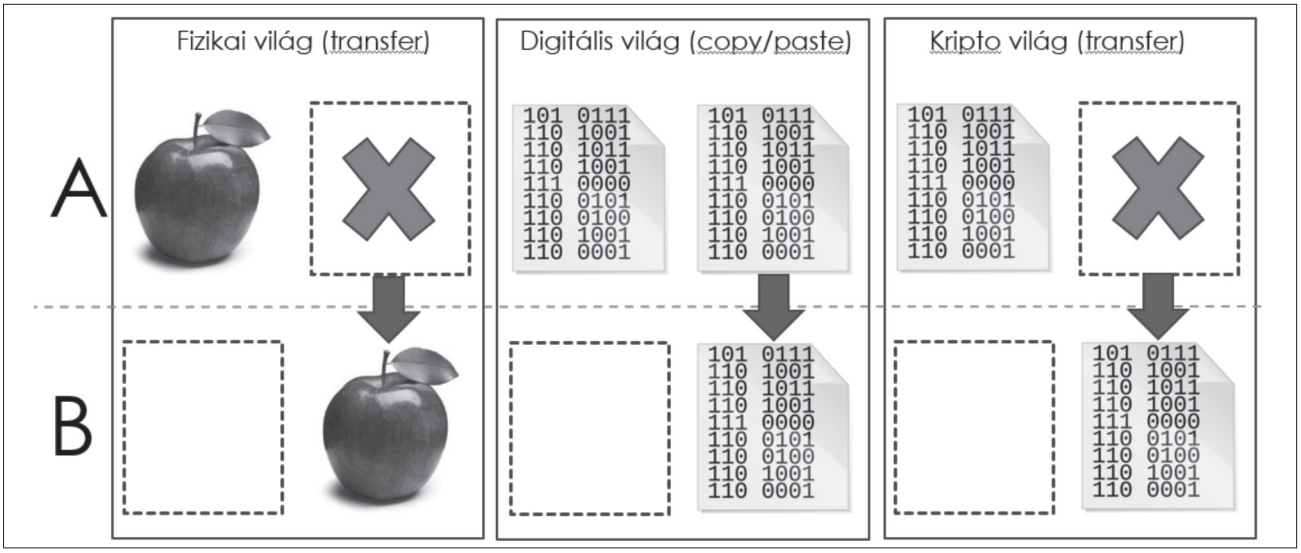
egyik alaptulajdonsága miatt egy-egy, benne tárolt adathoz egyértelműen egy és csak egy tulajdonos tartozik. Az első, blockchain-re alapuló megvalósítást, a Bitcoin rendszert éppen a fenti tulajdonság miatt hozták létre.

Mivel az adat tulajdonlása a blockchain-ben ún. pénztárcákon (a továbbiakban angol kifejezéssel élve: wallet) keresztül valósul meg[2], így a wallet tulajdonosa maga rendelkezik az adattal. Így mások nem feltétlenül tudják, hogy ki is valójában az adat tényleges tulajdonosa, csak a wallet ún. hez csak adott felhasználóknak lehet hozzáférésük (permissioned blockchain). Mindemellett az is meghatározható, hogy kinek milyen funkcionalitása, ill. jogosultsága legyen egy adott blockchain rendszerben.

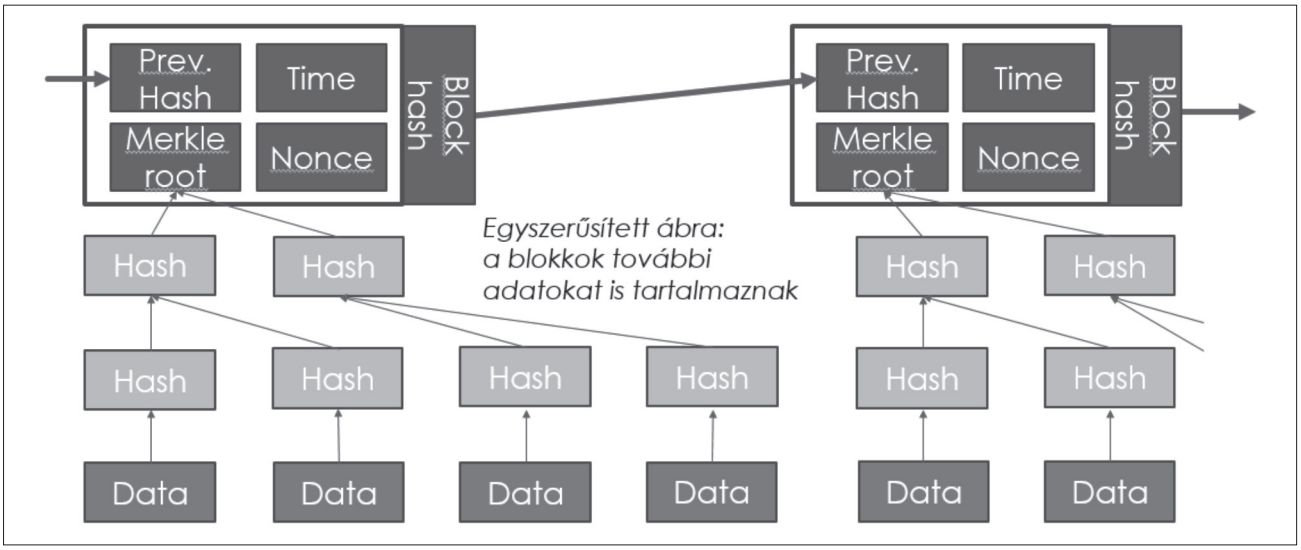
A blockchain rendszerek a fentiek alapján alkalmasak arra, hogy egymással hierarchikus, vagy más típusú függelmi viszonyban nem (!) álló felek között egy adat hitelességét, annak létezését, bármely fél által könnyen bizonyítani lehessen (külső fél által pedig nagy biztonsággal elfogadható legyen a blockchain-ben tárolt adat hitelessége).

Belátható tehát, hogy az olyan blockchain, amelyet csak egyvalaki üzemeltet, illetve az adott blockchain rendszer csak nála létezik, egyszerűen helyettesíthető egy megfelelő biztonságú adatbázissal. Ilyen esetben a blockchain nyilvánvalóan

[2] A pénztárca ez esetben egy ún. nyilvános kulcsú kriptográfiai eljárás eredményeként jön létre. A pénztárca mindenki által ismert azonosítója az ún. nyilvános (publikus) kulcs, míg a hozzá tartozó titkos (privát) kulcs kizárólag a pénztárca tulajdonosa által ismert.



3. ábra
Az értékek internete – a „dolgok" közvetítése a fizikai, a digitális és a „crypto" világban

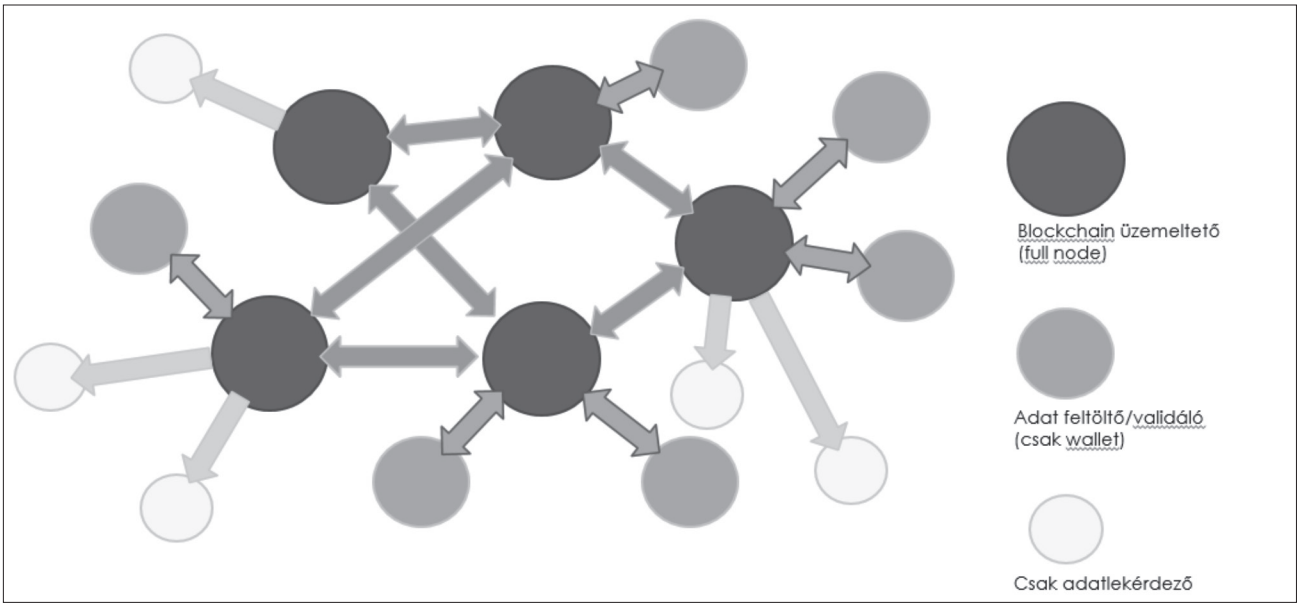


4. ábra
A blockchain blokkjainak adattartalma

nem sok előnyt kínál (vagy semennyit). Tehát a blockchain használatának akkor van értelme, amennyiben több, egymással egyenrangú, egymástól nem függő szervezetek használják. Ezek a szervezetek az ún. teljes csomópontok (ún. full node-ok, amelyeket a továbbiakban szintén csak node-oknak nevezünk, hacsak nem értelemzavaró, ha nem különböztetjük meg őket), amelyeknél a teljes blockchain megtalálható (másolat, azaz replikátum). Amennyiben ugyanis csak egy node üzemel, az lehetővé teszi az uú. *„alternatív valóság"* előállítását (a blockchain adott szintig való visszafejtésével és más irányú újraépítésével), így tehát a hitelesség megkérdőjelezhető (még akkor is, ha az adott üzemeltetőnek nem érdeke a változtatás). Itt megjegyzendő, hogy bár az adott node-nál megtalálható a blockchain replikátuma, mégsem tud vele mit kezdeni, azon felül, hogy hitelesíti vagy továbbítja. Azaz a blockchain olyan, mint egy főkönyv és nem olyan, mint a benne szereplő egyes tételek értéke, vagyis annak birtoklása. Így a node-ok más szóval könyvelőnek is tekinthetők.

A fentiek szerint tehát akkor van értelme a blockchain használatának, amennyiben más node-ok is tárolják a blockchainben lévő adatokat, és önmagában egyik node sem képes a fenti módon alternatív valóság előállítására. Azaz a node-ok között valamilyen szempont szerinti többségi, a protokollon alapuló kényszer konszenzus van közöttük a blockchain-ben lévő adatokkal kapcsolatosan. Belátható az is, hogy – mivel az adott node-ok azonos informatikai (benne kriptográfiai) protokollt használnak a blockhain, illetve ennek alapvető jellemzőjeként a konszenzus fenntartásához – minél több node vesz részt a blockchain-ben, annál kisebb esélye van az egyszer már kialakult konszenzus megtörésének (értsd, a lezárt blokkok más blokkal/blokkokkal való helyettesítésének kísérletéhez[3]).

[3] A sikeres kísérlethez 1) a csaló kénytelen a megváltoztatott adatot tartalmazó blokktól újraszámolni mindent úgy, hogy közben utolérje a többieket és 2) szabálytalan műveletet ezekbe a blokkokban sem tehet, mert azokat a többiek elutasítanák.



5. ábra
Privát (permissioned) blockchain publikus lekérdezéssel

A nyílt (publikus) blockchain rendszerekben az alternatív valóság előállításához az u.n. munkabizonyíték (Proof-of-Work – PoW) alapján konszenzus kényszert biztosító rendszerekben csalás sikeres végrehajtásához olyan mértékű összefogásra, illetve a csaló, illetve a csalásban szereplő szervezetek olyan számítástechnikai kapacitására van szükség (ún.: 51% attack), amely gazdaságilag nem éri meg. Az ún. érdekeltségi (Proof-of-Stake – PoS), illetve hasonló[4] mechanizmusok alapján konszenzus kényszert biztosító rendszerekben pedig a blokk lezárásához szükséges érdekelt felek (ún. stake holderek) között való részvételhez pedig a *„letét"* olyan mértékű, hogy szintén nem éri meg gazdaságilag, mivel csalás esetén az adott node(ok) elvesztik a letéteiket. Megjegyzendő, hogy ezek a letétek szintén értékkel bíró digitális jelsorozatban értendők. Ezeket az értékkel bíró jelsorozatokat funkciójuktól függően hívják cryptocurrency-nek, illetve token-nek, manapság összefoglaló néven cryptoasset-nek, azonban ezekkel csak a későbbiekben, a blockchain tényleges felhasználásánál foglalkozunk, ott is csak a szükséges mértékig.

Mindemellett meg kell jegyezni, hogy a blockchain-ben tárolt adatok nem bizonyítják az adatok valódiságát, pusztán azt, hogy az adat változtatás nélkül került a blockchain-be, és az utólag gyakorlatilag nem változtatható anélkül, hogy az igen könnyen és gyorsan ne derülne ki, így hitelesnek tekintendő. Azonban az, hogy az adott hamis adatot ki, azaz melyik wallet helyezte be a blockchain-be, egyértelműen azonosítható, pont a wallet-je alapján. Meg kell jegyezni továbbá azt is, hogy az adat csak akkor válik a blockchain részévé, így a fentiek szerint gyakorlatilag változtathatatlanná, amennyiben azt már egy u.n. lezárt blokk tartalmazza. Az adat annál kevésbé változtatható, minél több lezárt blokk követi az adott adatot tartalmazó blokkot, hiszen a fentiek szerint annál kevésbé éri meg gazdaságilag a blockchain visszafejtése az adott adat utólagos szándékos[5] megváltoztatásához.

Az adatoknak a blockchain-ből való kvázi *„eltávolítására"* azonban van lehetőség, és bár a rendszer tulajdonságaiból adódóan adat nem törölhető a blockchain-ből, az adat *„elégethető"* (burn). Ugyanezt az eljárást lehet alkalmazni a már nem szükséges, hamis, vagy akár jogszabály alapján (pl. GDPR[6]) törlendő adatok esetében. Az adat elégetése a blockchain-ben ugyanis nem más, mint egy olyan wallet-be való továbbítás, amelynek a visszafejtő (ún. privát) kriptográfiai kulcsát megsemmisítettük, eldobtuk. Ezzel ugyanis biztosítjuk, hogy az adat a továbbiakban senki számára ne legyen hozzáférhető, hiszen az egyetlen, aki hozzá tudna férni, a wallet tulajdonosa, ami a fentiek szerint az eldobott kulcs miatt nem létezik. A blockchain-ben az így eldobott adatok a rendszer tulajdonságaiból adódóan egyetlen node-nál sem szerepelhetnek még meglévőm, el nem égetett adatként, hiszen a blockchain replikátumok minden node-nál ugyanazok.

A fentiekben leírt privát (permissioned) blockchain-ek (jó részében) pedig az egyes szereplők eleve ismertek és validáltak, tehát a csalás kísérlete azonnal rábizonyítható az adott node-ra, illetve wallet-re, mindamellett, hogy a protokoll itt is a fentiek szerint kizárja a csalás lehetőségét.

3. A blockchain alkalmazása a közgyűjteményeknél

A blockchain alkalmazása a digitális közgyűjtemények esetében a fentiek szerint magától értetődik, hiszen a blockchain igen sok funkciójára szükség van, vagy lehet az egyes köz-

[4] Lásd pl. a Ripple/Stellar consensus Protocol-t, vagy a delegated Byzantic Fault Tolerant (dBFT) konszenzus rendszert.

[5] Szándékolatlanul pedig senki nem fektet energiát a blockchain visszafejtésébe – itt nem ejtünk szót a véletlen elágazásokról, és az esetlegesen ebből adódó, véglegessé váló ún. fork-okról, a blockchain kettéválásáról.

[6] Europea Union – General Data Protection Regulation, hatályba lépett 2018. 05. 25-én.

gyűjtemény típusoknál (levéltári, könyvtári, audiovizuális, múzeumi gyűjteményeknél), vagy akár mindegyiknél akár egyedileg, akár egymással összekapcsolt módon, így a közgyűjtemények közötti átjárást lehetővé téve (természetesen csak a blockchain adott funkcionalitását értve az átjáráson).

3.1. Dokumentum hitelesítés

A közgyűjtemények esetén (talán egyetlen kivétel a múzeumi tárgyak egy része) a fentiekben leírtak szerint tehát akkor van értelme a blockchain, fenti szempontú – tehát a digitalizált adatok hitelességét bárki számára bizonyító – bevezetésének, amennyiben nem egy, központi full node tárolja a blockchain-t, hanem más full node-ok is. Ilyen full node-ok lehetnek maguk az egyes közgyűjtemények ágazati integrátorai, és/vagy az adott ágazathoz tartozó szervezetek (múzeumok, könyvtárak, levéltárak, audiovizuális archívumok). Ezek a node-ok részt vesznek a blokkok ún. lezárásában, tehát a blockchain építésében (nem csak a replikálásban), és amely rendszerben valamilyen, a résztvevők által nem megjósolható eredményt adó algoritmus alapján határozzák meg azt, hogy melyik node zárja le a következő blokkot. Rendező elvként kimondható, hogy olyan, egymástól független szereplők részvételének van értelme, amelyek maguk is hozzá tudnak tenni adatokat a blockchain-hez, azaz például olyan adatokat, illetve adatok hash kódját illesztik bele a blockchain adott blokkjaiba, amely adatokkal csak ők rendelkeznek, vagy amely adatoknak ők az adatgazdái, függetlenül attól, hogy az másutt is létezik (például akár az ágazati integrátornál). Mindamellett a blockchain-nel kvázi az is biztosítható igény esetén, hogy két, digitálisan teljesen megegyező, de különböző helyeken meglévő adat csak egyszer kerüljön a blockchain-be (hiszen sokszor megkérdőjelezhető az is, hogy mi értelme van más aspektusból – azaz a blockchain-en kívül – adott digitális közgyűjteményi adat több helyen való tárolásának).

Amennyiben azonban van olyan közgyűjteményi, digitalizált adatuk, amely másutt nincs meg, de a közgyűjtemények teljes körű digitalizálásakor szükség van rá, ezek az intézmények is juttathatnak be adatokat a blockchain-be. Természetesen nem kötelező mindenkinek, aki adatokat tölt fel a blockchain-be, full node-ot üzemeltetnie (ezek a résztvevők wallet-ekkel rendelkeznek, de azokkal biztosan, hiszen wallet nélkül nem tehető adat a blockchain-be). A blockchain tárigénye ugyanis egyre nő, illetve a blokkok lezárásához mindenképpen kell valamilyen, eléggé bonyolult és ezért számításigényes kriptográfiai algoritmus futtatására alkalmas teljesítményű hardver, és amivel nagy valószínűséggel nem minden résztvevő rendelkezik.

Ezek a node-ok is jogosultak azonban a blockchain-be való adatfeltöltésbe azzal, hogy ők biztosan nem fognak blokkot lezárni (és a blockchain-t replikálni), hanem azt valamelyik full note teszi meg. Azonban a blockchainben lévő adatok validálását, hitelesség ellenőrzését ezek a résztvevők is meg tudják tenni. Az adatok valódiságáért, valamint – hash kód esetén – a blockchainbe feltöltött, a hash kód alapját képező adat rendelkezésre állásáért, sértetlenségéért, bizalmasságáért[7] a fentiek szerint természetesen az adat (hash kód) feltöltője felel, függetlenül attól, hogy ki zárta le a blokkot. Ha a blockchainbe nem az alapadat, hanem csak a hash kód kerül be, akkor az alapadat megismerhetősége is az adat kezelőjének a feladata (hiszen ez esetben csak nála van meg, a blockchain csak azt biztosítja, hogy az adat hiteles-e).

3.2. Közgyűjtemények, illetve integrátorok együttműködő blockchain-jei

Más oldalról, mivel a blockchain-ben teljesen mindegy, hogy milyen adatot, illetve milyen adat hash kódját tároljuk, ezért a blockchain használata nem feltétlenül kell kötődjön egy ágazati integrátorhoz, vagy közgyűjteményekhez, hanem adott esetben a többi ágazati integrátor, illetve a hozzájuk tartozó intézmények is részt vehetnek a blockchain fenntartásában (péáldául az Országos Levéltár, a Nemzeti Múzeum, a Magyar Nemzeti Filmalap (MNFA) és a Műsorszolgáltatás Támogató és Vagyonkezelő Alap (MTVA), mint ágazati integrátorok, de például a Budapesti Levéltár, a Természettudományi Múzeum, vagy a Magyar Távirati Iroda (MTI) is részt vehet akár full node-ként, akár csak wallet-tel rendelkező adatfeltöltőként). Megjegyzendő, hogy a blockchain alkalmazása esetén nincs hierarchia az ágazati integrátor és a hozzá tartozó, vagy akár más közgyűjtemények között (tehát például az MTVA és az Országos Levéltár is ugyanolyan, egyenrangú szereplő a blockchain-ben).

Az adott ágazati integrátoroknál és/vagy közgyűjteményeknél a fenti típusú blockchain tehát alapvetően egy privát (permissioned) blockchain (azon belül is konzorciális vagy fél-konzorciális típusú). Ehhez azonban alapvető funkcionális okokból, azaz adat hitelesség ellenőrzése céljából bárki – azaz a digitalizált közgyűjtemények bármely felhasználója – hozzáférhet (ez a dolog természetéből adódóan csak olvasási jog és wallet sem kell hozzá, hiszen adatfeltöltés a felhasználó oldaláról nem történik és nem is történhet).

A fentebb leírt okfejtésből látszik, hogy magát a közgyűjteményi adatot nem érdemes a blockchainben tárolni, hiszen óriási az az adatmennyiség, amely a blockchain működésének ellehetetlenülését hozza magával. Azonban a hash kód alapjául szolgáló közgyűjteményi adat fellehetőségének helyét értelmes a blockchain-be beilleszteni. Ennek azonban vannak korlátai, hiszen a közgyűjteményi adat átkerülhet egyik szervezettől a másikhoz, sőt duplikálódhat (bár ennek nem sok értelme van), a blockchain-be ezért sok esetben értelmetlen újra rögzíteni. Hacsak pont nem az a cél, hogy az adott digitalizált adat minden fellehetőségi helyének, idősoros követése rendelkezésre álljon (remélhetőleg a digitalizált közgyűjteményi adat selejtezésére nem kerül sor, de ha mégis, a blockchain azt is tudja kezelni, például a fent leírt burn eljárással).

[7] Az információbiztonság u.n. CIA alapelve a Confidentiality, Integrity, Availability szavak betűszava.

3.3. Felhasználói regisztráció és validáció

Mindazonáltal a blockchain nem kizárólag az adatok hitelességének bizonyítására használható. Bármely, a nyilvánosság számára nyitva álló, illetve korlátozott hozzáférés esetén is cél lehet a felhasználói/hozzáférési regisztráció, és annak érvényességi ellenőrzése. Ehhez az adott felhasználónak wallet-tel kell rendelkeznie, valamint a wallet generálásához szükséges a felhasználó adatait valamilyen módon ellenőrizni (authorizáció). Mindezek után szükséges a megfelelő felhasználói adatok hash kódjának a blockchain-be való feltöltése. Ezzel viszont bármely más, az adott közgyűjtemény és/vagy ágazati integrátor rendszeréhez kapcsolódó más szolgáltató is megbizonyosodhat arról, hogy a felhasználó regisztrált, milyen profil beállításai vannak, érvényes-e a regisztrációja, és milyen engedélyekkel rendelkezik.

3.4. Digitális belépőjegy, olvasójegy, kölcsönzési jegy, megtekintési engedély

Azoknál a közgyűjteményeknél, ahol lehetőség van még nem digitalizáls művek megismerésére is, a hagyományos belépőjegy, olvasójegy, kölcsönzési jegy, megtekintési engedély digitálisra váltható, és ezen jegyek/engedélyek alapján az adott felhasználó azonosítója (és adott esetben a felhasználói adatok) a közgyűjtemény rendelkezésére állnak. Ezzel bizonyítható az is, hogy az adott jegy/engedély felhasználásra került, mikor és milyen időtartamban, esetleges figyelmeztetés az időtartam lejáratára, sőt pl. kölcsönzés esetén az adott műnek a felhasználónál való elérhetősége. Ennek módja a blockchain-en futó smart contract-ok használata (ennek részleteire itt nem térünk ki). Az okos szerződéseket futtatni képes blockchain rendszerek teljes utasításkészlettel (ún. Turing-complete) rendelkezők (például Ethereum rendszer – Ethereum Virtual Machine (EVM)).

A teljesség kedvéért megemlítendő, hogy sok funkció megoldható nem (!) teljes utasítás készlettel rendelkező blockchain rendszerek esetén is (például Bitcoin rendszer), de ennek manapság nem sok értelme van, hiszen a blockchain-t ez esetben fő funkcióként nem fizetési (cryptocoin-t használó) rendszerként, hanem egyéb, specializált szolgáltatások miatt használjuk (a nem teljes utasításkészlettel rendelkező rendszerek leginkább fizetési rendszerek, amelyek más funkcionalitásra alapértelmezésben nem, vagy csak igen korlátozott mértékben alkalmasak).

3.5. Szerzői és szomszédos jogok kezelése

A fentiekhez igen hasonló, amikor az adott, szerzői jogot védő művet megismeri a felhasználó (itt gondolhatunk például filmművészeti alkotásra, színházi előadás felvételére, zeneműre, stb.), amikor is a felhasználás ténye is rögzíthető, a szerzői jog jogosultja pontosan tudni fogja, hogy a művét ki használta fel, és milyen mértékű jogdíj fizetésére köteles (nem mindegy jogdíj szempontjából például, hogy egy zeneművet egyvalaki hallgat meg, vagy egy szórakozó helyen, étteremben, stb. játsszák le nagy közönség számára elérhetővé téve azt). Mindezzel akár a közös jogkezelők feladata (Artisjus, MAHASZ-EJI) is egyszerűsödik, hiszen nem *„átalányra"*, hanem tényleges felhasználásra hagyatkozhatnak a jogdíjak megállapításakor, valamint a felhasználásról pontos statisztikák is készülhetnek akár aggregált, akár pszeudonimizált, vagy teljesen anonimizált módon. Megjegyzendő, hogy a blockchain-ben az adott felhasználót bárki (azaz nem csak az adatkezelő) számára azonosítható módon lennének tárolva a felhasználó tevékenységéről gyűjtött adatok, az csak a felhasználó kifejezett beleegyezésével lehet jogszerű.

3.6. Emelt szintű szolgáltatások ellenértéke

A közgyűjtemények vonatkozásában a blockchain további alkalmazási területe lehet az, ha a felhasználó valamilyen fizetős, emelt szintű szolgáltatást akar igénybe venni[8], szükséges valamilyen token vagy cryptocoin (általánosságban, de tévesen elnevezve: kriptopénz) fizetési eszközként való használata, illetve bevezetése. Ez lehet saját, vagy már meglévő fizetési eszköz. A felhasználó előzetesen vásárol valódi pénzért (fiat) megfelelő számú ilyen cryptocoin-t, vagy token-t, és azt használja fel az adott szolgáltatásért való fizetésre. A fizetés biztosítását pedig az adott közgyűjtemény(ek) által üzemeltetett blockchain-ben a már említett smart contract-ok kezelik, illetve bonyolítják (és kényszerítik ki). Ez a technika lehetővé teszi az adott szolgáltatás igénybevételekor az automatikus fizetést. Mindamellett, ha a felhasználónak nem áll rendelkezésére megfelelő ilyen fizetési eszköz, a smart contract nem engedi neki a szolgáltatás igénybevételét.

A szolgáltatás tényleges igénybevételének és megtörténtének bizonyítéka a smart contract-ok révén így bekerül a blockchain-be, az a továbbiakban nem vitatható, mint ahogyan a fizetés megtörténte sem. A rendszer tehát hasonlóan működik, mint pl. a feltöltő kártyás telefonok. Azaz a felhasználó addig tud emelt szintű szolgáltatást igénybe venni, amíg a tárcájában lévő cryptocoin-ok, illetve token-ek mennyisége ezt megengedi. Ha elfogy ez a fizetési eszköz, a felhasználó újra töltheti a wallet-jét.

3.7. GDPR megfelelés

A felhasználói adatok kezelésével kapcsolatosan azonban felmerül az EU adatvédelmi (szokásos rövidítéssel GDPR) rendeletének való megfelelés kérdése is. Abban az esetben, amikor a blockchain-ben csak a hash kód van, és a tényleges adatok a blockchain-en kívül (off-chain) vannak tárolva, így ezen adatoknak az adatkezelőnél való törlésével a GDPR megfelelés (compiance) biztosítható. Igaz, ez esetben a blockchain-ben tárolt hash kódhoz a továbbiakban nem tartozik adat, de mivel a blockchain az adat tárolása után tovább épült, és ezt a node-ok ellenőrizték (validálták), így az továbbra is látszik, hogy ott volt egy olyan tényleges adat,

[8] Megjegyzendő, hogy csak ezért a funkcióért nem kifizetődő blockchaint bevezetni.

amiből az adott hash kód generálódott. Abban az esetben, amikor a blockchain-ben a felhasználó adatai megtalálhatók, akkor ezen adatok blockchain-ben való elégetése a fentiekben vázoltak szerint megoldható, így ez esetben is biztosított a GDPR megfelelés.

4. Nemzetközi példák

A viszonylag csekély számú nemzetközi irodalomban[9] fellelhető projektek is még kezdeti fázisban találhatók (a blockchain, mint technológia jelenleg is korainak mondható fejlődési szakasza okán), illetve még csak ötlet szinten jelentkeznek[10], vagy pl. csak specializált könyvtárakra vonatkoznak[11]. Továbbá különbség a hazai megvalósítási elképzelésekhez képest az eltérő környezet, illetve a digitalizálás nagyobb fokú előre haladottsága (lásd például OCLC[12]).

5. Megvalósítási alternatívák

A fentiek megvalósításhoz már készen lévő keretrendszerek állnak rendelkezésre, amelyek közül olyat érdemes választani, amelynek a kódja megfelelő módon auditált. Ezeknek az informatikai megoldásoknak, illetve keretrendszereknek a forráskódja általában nyílt, de komoly szaktudás kell ahhoz, hogy a nem kifejezetten ezzel a témával foglalkozó szakember is megértse azt, hogy ténylegesen melyik funkció melyik, és a funkcionalitás megfelelő-e, nincsenek-e a kódban elrejtett csapdák (ún. back-door-ok). A legismertebb ilyen, auditált, nyílt forráskódú rendszer a Linux Foundation által létrehozott és felügyelt Hyperledger nevű, megfelelően testre szabható, programozható, továbbfejleszthető keretrendszer. A Hyperledger rendszer létrehozásában és karbantartásában, támogatásában több alapító cég is közreműködik, például az IBM és az Intel. A Hyperledger felhasználására már most is sok projekt épül, illetve van már működő stádiumban. Ezért a feladat megoldásához szükséges rendszer kiválasztásakor érdemes megfontolni, hogy esetlegesen már kész rendszer további testre szabása, vagy a Hyperledger keretrendszeren nyugvó új projekt eredményeként létrejövő egyedi rendszer kifejlesztése a célszerűbb.

Egy másik megoldás például az OCI által fejlesztett, nyílt forráskódú, de nem monolit, hanem moduláris felépítésű blockchain rendszer, a Graphene alkalmazása, illetve a rendszer előre gyártott egyes moduljainak, könyvtárainak megfelelő összekapcsolásán alapuló rendszer kifejlesztése, saját, testre szabott rendszer kialakítása. Ez az előre gyártott elemek és könyvtárak miatt nem igényel különösebben nagy erőforrás ráfordítású fejlesztést, testre szabást. Mindamellett, a nyílt forráskód ellenére ez a rendszer jelenleg nincs olyan módon auditálva, mint a Hyperledger. Megjegyzendő, hogy a későbbiekben a legnagyobb és legelterjedtebb, smart contract-okat végrehajtani képes publikus blockchain, az Ethereum rendszer fejlesztői is tervbe vették a Graphene alapú fejlesztést.

Harmadik megoldás lehet olyan blockchain keretrendszer választása, amely önmagában is nagy cégek által fejlesztett, illetve támogatott. Ilyen lehet például a Microsoft Coco platformja[13], az SAP Leonardo alapú blockchain megoldása[14], illetve az Oracle Blockchain Cloud Service[15].

Negyedik megoldás lehet a blockchain fejlesztő cégek (általában start-up-ok) projektjei között olyan keresése, amely viszonylag kis energiaráfordítással megfelelővé tehető a fenti funkcionalitás kialakítására.

A blockchain alkalmazása mindazonáltal teljes mértékben összefér a közgyűjteményekben esetlegesen már meglévő, vagy fejlesztés alatt álló egyéb, hitelességet biztosító rendszereivel, azokra semmilyen hatással nincs, sőt azoktól teljesen függetlenül működhet. A blockchain fentiekben vázolt funkcionalitása mindemellett messze túlmutat ezen rendszerek alkalmazhatóságán, hiszen a blockchain nem csak a digitalizált közgyűjteményi adatok hitelességének ellenőrzésére használható.

6. A megvalósításhoz választható blockchain keretredszerek

Természetesen a fent vázolt projektek tetszőleges sorrendben bevezethetők, azonban gazdaságossági és továbbfejleszthetőségi elveket figyelembe véve célszerű annak a rendszer elemnek az első körben való megvalósítása, ami a leginkább kihasználja a blockchain előnyeit. Ez pedig a hitelesség bizonyíthatósága, mindenki felé való igazolása. Ez a projekt azonban már előfeltételezi egy adott blockchain rendszer mellett való döntést és annak bevezetését. Például a Github-ról ingyenesen letölthető és felhasználható, nyílt forráskódú rendszerek támogatás nélküli igénybe vételéhez közbeszerzés egyáltalán nem szükséges, csupán megfelelő mélységű előkészítés alapján való szakmai döntés. A közbeszerzés akkor válik szükségessé, ha valamiféle, fizetős szakmai támogatás (support, maintenance) igénybevételére, vagy licence vásárlására kerül sor a választott keretrendszer vonatkozásában. Megvizsgálandó, hogy egyáltalán van-e valamilyen támogató szervezet a választott keretrendszer mögött, bár mindenképpen érdemes hosszú távon is támogatott rendszert választani az esetleges protokoll/kódhibák javítására, illetve fejlesztési támogatáshoz.

---

[9] Lásd pl. https://ischoolblogs.sjsu.edu/blockchains/blockchains-applied/applications/, https://www.oclc.org/en/home.html

[10] Lásd pl: https://www.tandfonline.com/doi/full/10.1080/02763869.2017.1332261,
http://www.ala.org/tools/future/trends/blockchain,
https://www.edsurge.com/news/2018-02-01-blockchain-in-the-library-researchers-explore-potential-applications,
https://ischoolblogs.sjsu.edu/blockchains/public-libraries-and-blockchain-by-m-ryan-hess/, http://www.stevehargadon.com/2018/05/blockchain-and-libraries-yes-mini.html, https://americanlibrariesmagazine.org/blogs/the-scoop/blockchain-in-a-flash/

[11] http://blog.cssis.org/2017/09/08/blockchain-for-law-libraries/

[12] https://en.wikipedia.org/wiki/OCLC

[13] https://azure.microsoft.com/en-us/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks/

[14] https://www.sap.com/products/leonardo/blockchain.html

15 https://www.oracle.com/cloud/blockchain/