HADMÉRNÖK

XII. Évfolyam 2. szám – 2017. június

BLOKKLÁNCOK

BLOCKCHAINS

AMBRUS Éva

(ORCID: 0000-0002-8354-1296)

ambrus.eva.eszter@gmail.com

Absztrakt

A digitalizáció következő lépése a big data után a blokkláncok megjelenése. A blokklánc nyilvános vagy privát (zárt) megosztott főkönyv, melyben minden tranzakció nyomon követhető. Most valóban úgy tűnik, hogy ez új alapokra helyezi az internet alapú szolgáltatásokat és interakciókat, nincs olyan terület, mely ne lenne érintett és ne fejlesztene blokklánc technológiát, legyen szó pénzintézetekről, szolgáltatásokról, egészségügyről, közigazgatásról. A 2008-as pénzügyi világválság következtében egy technológiai forradalom indult el és nem úgy tűnik, hogy lassulna.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: blokklánc, pénzügy, digitalizác, adat

Abstract

The next step regarding digitalization after big data is the introduction of blockchains. As of now it seem to become the new platform of the web 3.0 and every industry - financal institutions, services, healthcare, public administration - is developing its own version of blockchain technology. The shockwaves of the global financial crisis have reached the technology sector and it doesn’t seems to slow down.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the *Ludovika Workshop.*

Keywords: *blockchain, finance, digitalization, data*

A kézirat benyújtásának dátuma (Date of the submission): 2017.03.28.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.05.11.

BEVEZETÉS

Az információs-technológiai forradalom magával hozta a digitalizáció iránti igényt, azaz, hogy a munkafolyamatok, adatbázisok, adatok számítógépen elérhetőek legyenek (azaz analóg adatokból digitálissá váljanak). A GKI Gazdaságkutató Zrt. a Siemens Zrt. számára végzett digitalizációs helyzetkép tanulmány [1] szerint a digitalizáció komoly versenyelőnyt jelent, emiatt a vállalatok egyre intenzívebben foglalkoznak a digitalizációval. Magyarország az Európai Bizottság DESI-index (digitális gazdaság és társadalom index) 2017-es adatai alapján a 21. helyet foglalja el, jól teljesít az összekapcsoltság területén, ami főként a nagy sebességű vezetékes széles sáv (NGA) és a 4G elterjedtségének, valamint a széles sávú internethasználat növekedésének köszönhető. Elsősorban a mobilinternetnek köszönhetően az internetfelhasználók száma nőtt, azonban a digitális készségek Magyarországon továbbra is az EU átlag alatt vannak, a főbb felhasználási területek a közösségi média oldalak, a hírportálok és a videótelefonálás. Mind a felhasználói oldalon, mind az üzleti oldalon nincs kihasználva a digitális gazdaság adta lehetőség, amely versenyhátrányt eredményez, a főbb kihívást változatlanul a vállalkozások csekély mértékű IKT (infokommunikációs technológia) használata és a digitális közszolgáltatások fejlettségi szintje jelentik.

A digitalizáció 5 legfőbb előnyének a nyomon követést, a hatékonyságot, a megbízhatóságot, a gyorsaságot és a rugalmasságot tartják. Ezek a tulajdonságok megegyeznek a blokkláncokról alkotott véleményekkel [2], nem véletlenül lett a big data mellett a blokklánc a legdivatosabb kifejezés a technológiai világban, a digitalizáció egyik legújabb eredménye a blokkláncok megjelenése.

A blokkláncok olyan nyitott vagy privát megosztott főkönyveket jelentenek, melyek blokkokból (azaz adathalmazokból) épülnek fel és ezek időrendben egymásra fűződnek – csak úgy, mint egy lánc. Minden blokklánc egyedileg készül, és a blokklánc előállításában és fenntartásában szerepet vállaló résztvevőjének (más néven adatbányásznak) felelőssége van, mivel az (adat)blokkok szét vannak osztva közöttük (innen a *megosztottság*).[1]

Ennek megfelelően olyan főkönyvről beszélhetünk, ahol minden blokk egy lapnak felel meg, és amely lapok meghatározott sorrendben követik egymást. Ez a sorrend nem módosítható. A felelősség (azaz, hogy a főkönyv minden bányásznál megtalálható) szétosztásával értékekkel (zsetonpénz, adat stb.) kereskedhetünk. Ez kihívást jelent az olyan (központosított), felelős hatóságok és szervezetek felé, akik adatvagyonokat őriznek vagy ellenőrzést gyakorolnak felettük (bankrendszerek, szolgáltatások).

A nagymennyiségű adatok (big data) nagyban terhelik a hálózatot – legyen szó akár az adatátvitelről, akár az adattárolásról, költség-és időigényesek. A blokkláncok megosztottsága és megbízhatósága lehetővé teheti az adatfeldolgozást gyorsítását és költségcsökkentését az adatok tömörítésével és a feldolgozás szétosztásával, mely az emberi internethasználók közötti interakciókon túl a dolgok internetét[2] (Internet of Things, IoT) is befolyásolhatja.

Jelen írás felvázolja a jelenlegi helyzetet és bemutatja, hogy blokkláncok miért tekinthetők az internet világát felforgató új technológiának.

[1] Az adatbányászok az adott blokklánc hálózat csomópontjai, annak fenntartásában és a blokkok létrehozásában egyenlően vesznek részt.
[2] hálózatba kötött “okos” eszközök

A BLOKKLÁNCOKRÓL ÁLTALÁBAN

A blokklánc technológia alapvető újítása a „vagyon" birtoklása (megosztottsága), amely ez esetben a tulajdonosoknál (adatbányászok) van, és nem egy adatbázissal rendelkező központi félnél (pl. bank, szolgáltató), aki nyilvántartja a vagyon tulajdonosát. [3] A blokklánc kifejezés először a bitcoin-nal kapcsolatosan jelent meg, de – a fogalmat tágabban használva – megjelenik az *elosztott főkönyv* (distributed ledger) kifejezés, jelen esetben azonban a blokklánc kifejezést alkalmazzuk, mint rövidebb és szemléltethetőbb kifejezést, tekintettel arra, hogy jelenleg nincs teljes egyetértés a fogalmak használatában. [4]

A blokklánc legelőször Satoshi Nakamoto, a bitcoin és rendszerének (bitcoin core) megalkotója (vagy megalkotói)[3] 2008-ban publikussá tett, a bitcoin rendszer hátterét adó elméleti leírásában jelent meg. [5] Egy teljes blokklánc magába foglalja az adott rendszerben valaha létrejött vagy végrehajtott összes műveletet annak (a láncnak) az indulása óta, így ebből pontosan megállapítható, hogy melyik címhez milyen információ tartozott.

A blokklánc hossza fontos, hiszen ez szavatolja az adatok biztonságát. Egy csomóponttal (adatbányásszal) rendelkező blokklánc meg tudná változtatni a tranzakciós adatokat, de mivel a hálózatban több csomópont van – és nekik jóvá kell hagyni az új blokkokat (azaz frissíteni a saját főkönyvüket) –, így egy adatbányász nem tud módosításokat végrehajtani a már létrejött adatokon. Az adott blokklánc hálózaton az adatbányászok legalább 50%-ának el kell fogadnia a változást (új adatokat vagy amennyiben elágazás van a láncon) hogy az „igaz" legyen.

A blokkláncban mindegyik blokk magában foglalja az őt közvetlenül megelőző blokk hash-ét[4]. A bitcoin és a rá épülő rendszerek az SHA-256 algoritmust használják[5], ezek szavatolják egyben a blokkok időrendi sorrendjét, valamint azt is, hogy ezeket a blokkokat utólag szinte lehetetlen módosítani, hiszen újra kellene generálni az összes megváltoztatni kívánt blokk utáni blokkokat is.

A blokklánc hosszát az összefűzött blokkok száma adja meg, azoknak teljes, összesített nehézségi értéke (ez bizonyos támadástípusok esetében lehet jelentős). Egy blokklánc továbbá akkor érvényes (sértetlen), ha az ősblokkal kezdődően az összes tranzakció is érvényes. A láncot alkotó blokkokból egyetlen egyenes út vezet vissza az ősblokkhoz, ellenben onnan elindulva több elágazással találkozhatunk. Ez akkor fordulhat elő, amikor egy időben generálódnak új blokkok, a többiek aszerint folytatják a láncot, hogy melyikről értesültek előbb, és az a lánc fog folytatódni (lesz érvényes) amelyik előbb bővül további blokkal.

Az elágazásnál fel nem használt rövidebb (érvénytelen) láncok blokkjait „árva" blokkoknak is nevezik, ezek adatai ugyanúgy tárolódnak a rendszerben, ám ezekhez nem lehet további blokkokat kapcsolni. Mivel minden blokk csak egyetlen másik blokkot jelölhet meg elődjeként, ezért két blokklánc soha nem fonódhat össze. [7]

Korábban szó esett a blokkláncok nehézségi értékéről. A blokkok létrehozásához meg kell oldani egy feladványt, amelyet a hálózat egy matematikai algoritmus alapján választ ki. Amint ezt a feladványt egy csomópont (adatbányász) megfejti, létrejön az új blokk. Ezeken a csomópontokon történik a hitelesítés is, azaz miután a feladvány megfejtésre került, az új blokkot hitelesíteni kell (ahogy fentebb jeleztem, a hálózatban jelenlévő csomópontok bizonyos százalékának el kell fogadnia azt), ezzel előkészítve azt a felhasználásra.

---

[3] Satoshi Nakamoto egy álnév, melyet egy személy vagy csoport használ. Személyazonossága nem ismert, 2011 óta nem aktív(ak).

[4] A hash kriptográfiában használatos hash függvényekre utal, mely informatikai eljárással bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve *hash/hasító érték*. [6]

[5] SHA – Secure Hash Algorithm, azaz biztonságos hash algoritmus.

A hitelesítés a felhasználástól is függ, a bitcon esetében olyan kérdéseket kell megvizsgálni, miszerint egyik tranzakció sem mutat-e többszörös elköltést-e vagy észlelhető-e bármiféle rendellenesség?

A blokkláncok nehézségi értéke aszerint változik, hogy éppen hányan vannak a hálózatban és csatlakoznak egy-egy blokklánchoz annak bővítéséhez. Értelemszerűen minél többen generálnak új blokkokat, annál nehezebb feladványokat küld a hálózat, ha pedig azt érzékeli a rendszer, hogy túl lassan készülnek az új blokkok, akkor csökkenti a nehézségi szintet.

A bitcoin esetében jelenlegi ismereteink szerint minden 2016. blokknál kerül sor a nehézségi szint felülvizsgálatára és újra beállítására (ez körülbelül kéthetenként felülvizsgálatot jelent, amennyiben figyelembe vesszük a célt, hogy 10 percenként új blokk kerüljön a láncokhoz). [8]

BITCOIN ÉS ETHEREUM

A Bitcoin-t ismereteink szerint 2008-ban, a gazdasági világválság után hozták létre a pénzügyi rendszerek egy elméleti és design kísérleteként. Évekig viszonylag ismeretlenségben fejlődött ez az alternatív pénzügyi rendszer. Az első újsághíradások a bitcoinról 2011-ből származnak, összekötve a rendszert a sötét web Selyemútjával (Dark vagy deep web, az internet illegális tranzakcióit és piacát felöle része). [9] A Bitcoin alapjában véve jelöli ezt a nyíltforrású digitális fizetőeszközt (melynek árfolyama van[6]) – annak létrehozását, tranzakcióját és tárolását – valamint a fizetőeszközt kezelő nyílt forráskódú szoftvert és az azzal létrehozott elosztott hálózatot is.

Az Ethereum létrehozója, Vitalik Buterin ezzel ellentétben nem pénzügyi rendszerként, hanem egy decentralizált applikációs platformként, a web 4.0[7] alapjaként hozta azt létre. [10] Ennek lényege, hogy minden olyan kedvelt web 3.0 applikációt és szolgáltatást decentralizáltan használhatóvá tesz felhasználótól-felhasználóig (peer-to-peer) szerkezeten keresztül a személyi azonosítóddal (pl. uPort, egy Ethereumon alapuló decentralizált személyazonosító rendszer[8]) történő interakció hozzáférési pontként (ezzel kihagyva a közösségi média platformokat).

Ezzel az Ethereum célja, hogy a felhasználók ne passzív szereplői legyenek a nagy közösségi médiacégek centralizált hatalmi struktúráiban, hanem nagyobb átláthatósággal, felelősséggel és hatalommal, aktív szereplőkké lépjenek elő és maguk dönthessenek adataik, online személyiségük, értékük és kommunikációjuk felett.

Az Ethereum saját fizetőeszköze az éter, amelyet a bányászok feladatokért kapnak cserébe. Az étert digitális fizetőeszköz helyett inkább digitális olajként nevezik, mely működteti ezt az ún. bizalomgépet. [11]

Az Ethereum nagy újítása az ún. okos szerződések (smart contract), melyet az Ethereum saját programozási nyelvén, a Solidity-n lehet megírni és amelynek tényleges tere az Ethereum Virtual Machine (EVM). Az EVM-et Turing-teljesre terveztek, azaz minden elméletben algoritmizálható feladat lefutható rajta. Okos szerződés lehet például üzleti szerződés (ezzel kihagyva az üzletkötőt), vagy akár szerencsejáték (ethereumlottó) is.

---

[6] http://www.napiarfolyam.hu/%C3%A1rfolyam/bitcoin/

[7] A web 1.0 csak olvasást tett lehetővé a felhasználók számára, a web 2.0 kifejezés olyan internetes szolgáltatások gyűjtőneve, amelyek elsősorban a közösségre épülnek, azaz a felhasználók közösen készítik a tartalmat vagy megosztják egymás információit. A web 3.0 a szemantikus web, ahol a mesterséges intelligencia / gép képes feldolgozni az adatokat, míg a web 4.0 – mely kialakulóban van – szimbiotikus web lehet, ahol a mesterséges intelligencia / gép végrehajtásra is képes, egyfajta web operációs rendszerként.

[8] https://www.uport.me

Az Ethereum másik nagy felhasználási területe a fentebb említett applikációk és szolgáltatásokban rejlik, hiszen egy vagy több okos szerződéssel, értékzsetonnal (amely szintén létrehozható az okos szerződés keretében) és egy felhasználóbarát weblappal létrehozható az ún. Dapp (decentralized application, azaz decentralizált applikáció) [12], amelynek felhasználási területei sokrétűek lehetnek. Kettőt kiemelve ezek közül: az Augur[9], egy előrejelző-prediktív piaci platform, ahol jövőbeni eseményekre lehet fogadni, pénzneme a REP (reputation, azaz hírnév), jelenleg béta tesztelés alatt áll, 2017 nyarán várható az indulása, valamint a Golem[10], egy nagy számítógép kapacitást igénylő, feladatokat megosztó platform, elődje a Brass Golem, számítógépes grafikai render farmként működik. Pénzneme a Golem Network Token (GNT), jelenleg szintén tesztelés alatt van.

Jogi szabályozás területén áttörést jelenthet, hogy 2017. február 22-én az arizonai törvényhozás egyhangúlat elfogadta azt a törvényjavaslatot (HB2417), amely az okos szerződéseket, mint érvényes üzleti szerződéstípust legalizálja, ezzel utat engedve további jogalkotói folyamatoknak. [13]

A BIZTONSÁG GARANTÁLÁSA

A blokkláncok amiatt a tulajdonságaik alapján tekinthetően biztonságosnak, amelyek biztosítják, hogy szinte lehetetlen őket újra írni, hiszen egy blokklánc bármelyik blokkjának az újra írásához az összes többit is újra kellene írni, amely nagyon nagy számítókapacitást (és tőkét)[11] feltételez. Ezért is fontos, hogy gyakran jöjjenek létre új blokkok, hiszen minden egyes új hozzáfűzött blokk csökkenti az előtte lévőknek az átírási esélyét. A blokkláncok értelmezését egy szoftver végzi, amely kivonatolja a lényeges információkat. [14] Mivel az adatok decentralizálva vannak, azaz az egész hálózaton elosztva találhatóak meg, így ezzel csökken a központosított rendszerekre jellemző sebezhetőség (melyeket a hackerek esetleg kihasználhatnának), illetve minimalizálódik egy központi hiba miatt létrejövő teljes adatvesztés. További biztonsági eljárást jelent a nyilvános kulcsú titkosítás használata. [15]

Amikor két blokk jön létre közel egyszerre, akkor elágazásokat (ún. forks-okat) hoz létre, ezekből kettőt különböztetünk meg, attól függően, hogy mennyire elő-kompatibilisek, tehát mennyire fogadják el az „erősebb” blokkláncot (értve ezalatt azt a láncot, melyre előbb kapcsolódik egy újabb blokk). Amennyiben konszenzussal módosítás történik a blokkláncnál (azaz melyik blokklánc legyen érvényes), úgy softforknak nevezzük (előremutató, idomuló elágazások). Amennyiben egy elágazásnál a bányászok ¾-e megegyezik egy láncban, a maradék ¼-e továbbra is tud érvényes tranzakciókat végrehajtani az árvaláncon.

A hardforkok (visszatekintő, merev elágazásokat) esetében a hitelesítésnek újra meg kell történnie az elágazást megelőző összes blokknál, minden résztvevő bányásznak frissítenie kell azt. Hardforknak tekinthetünk minden blokkmódosítást, hashmódosítást[12], nehézségi szint módosítás vagy érvényestranzakció módosítást. [16]

---

[9] https://augur.net/

[10] https://golem.network/

[11] Ez az értékzseton, a bitcoin, amiért létrehoznak blokkokat. Maga a blokk létrehozás is pénzbe kerül (de bitcoin-ban térítik vissza). A Bitcoint erre kiépített, speciális számítógépek bányásszák (melyek alapértéke is igen magas, az áramfogyasztásuk mellett – ezt honorálják bitcoinnal).

[12] A hash tulajdonképpen olyasmi, mint az adat újlenyomata, és az algoritmus, amely az adatokból „újlenyomatot” csinál többek között az SHA-256, melyet pl. a bitcoin használ, ám amennyiben más algoritmusra váltanának, úgy minden adatbányásznak el kellene azt fogadnia és visszamenőleg is érvényesíteni kellene újra a blokkokat, hogy érvényes maradjon.

NYILVÁNOS, KONZORCIUM, PRIVÁT BLOKKLÁNCOK

A nyilvános (szabadfelhasználású) blokkláncok felhasználó-barátabbak és mindegyik korai blokklánc rendszer engedély nélküli volt (lásd Bitcoin, Ethereum). Azzal, hogy megjelentek privát rendszerek – központi hatóságok által meghatalmazott hitelesítőkkel (pl. pénzügyi szektor) –, ez a definíció újra értelmezését igényelheti a szakterület képviselőitől. [17] Ahogyan létezik publikus internet hozzáférés és privát intranet (illetve ezek kombinációja), ugyanúgy van legitimitása és akadálya mindkét típusú blokkláncnak is.

A nyilvános blokkláncok esetében bárki elolvashatja azokat, küldhet és fogadhat tranzakciókat, és részt vehet a konszenzus-folyamatban (abban a folyamatban, amely eldönti, hogy mely blokkokat adják a lánchoz és mi a lánc aktuális állapota). A központosított felelősséggel/felügyelettel (pl. bankfiók) rendelkező szervezeteknél a jogosultságok szintjeit a központ határozza meg, a nyilvános blokkláncok esetében ezt a kriptográfiai hitelesítések biztosítják. Ezeket a blokkláncokat tekintjük teljesen decentralizáltnak, ilyenek voltak a korábban bemutatott Bitcoin és Ethereum.

Konzorciumos blokkláncnak tekinthetjük azt a blokkláncot, ahol a konszenzusos folyamatot egy előre kiválasztott csomópontok (node, a hálózat által tárolt elosztott adatbázisokat osztják el) végzik, például 15 pénzügyi szervezet, mely mind irányítanak egy-egy csomópontot. Konszenzussal például minden blokk létrejöttéhez legalább 10 csomópontnak hitelesítenie kell azt, hogy érvényes legyen. Eldönthető továbbá, hogy a blokkláncok olvasása nyilvános legyen, vagy korlátozott a résztvevők részére. Ezeket a blokkláncokat hívhatjuk részlegesen decentralizáltnak.

A pénzügyi szektorban a legnagyobb blokklánc-technológiára épülő konzorcium az R3CEV, mely több mint 70 pénzintézetet számlál és a blokklánc adatbázis kutatás-fejlesztésével foglalkozik. [19] A pénzügyi szektor a blokklánc helyett a megosztott főkönyvelést (*shared ledger*) használja terminológiaként, az R3CEV által használt platform neve Corda, melyet kifejezetten erre a pénzügyi szektorra fejlesztettek. Összetettebb műveletek és tranzakciókat is képes végrehajtani, mindamellett, hogy korlátozza az ezekhez való hozzáférést. [20] A Corda kódjai 2016 végén nyilvánossá váltak, hogy ezzel is hozzájárulhassanak a Linux Foundation HyperLedger projektjéhez.[13] [21] Az R3CEV tagjai többek között a Barclays, BBVA, Credit Suisse, J.P. Morgan, Citi, Deutsche Bank, HSBC.

Privát blokkláncok azok, ahol a blokkírás egy központi szervezethez van kizárólagosan rendelve, annak olvasása lehet nyilvános vagy korlátozott. Felhasználási területei lehetnek az adott (központ) szervezet adatbázis menedzsmentje, auditálása. [18] Leginkább az intranethez hasonlítható. Egy példa: a Nasdaq amerikai részvénypiac saját fejlesztésű Linq blokkláncra épülő technológiát felhasználva 2015 vége óta lehetővé teszi a zártkörű értékpapírkereskedést [22]

A blokkláncok további fejlesztése és szélesebb körű alkalmazása a pénzügyi világon túl a közigazgatást is érintheti a jövőben. Az Egyesült Arab Emírségek 2016 végén bejelentette, hogy a 2020 Jövő Projektje keretében 2020-ig a blokklánc technológia segítségével el akarják érni a papírmentes közigazgatást. Ehhez 2017 elején Dubai város meghirdette a Blockchain Challenge-t, annak megvalósítására, hogy Dubai legyen az első blokkláncokon alapuló okosváros, fejlesztve ezzel a régiót, valamint vezető szerepet betöltve a blokklánc technológia területén. [23] [24]

[13] A projekt célja horizontálisan összekötni a technológiai, pénzügyi, valamint a beszállítói világpiaci szereplőket a blokklánc technológia segítsével. A projekt tajgai többek közöett az R3, Cisco, Fujitsu, IBM, Intel, Data, J.P. Morgan, Deutsche Börse Group)

Az egészségügy egy további terület, ahol ígéretes kezdeményezések vannak a blokklánc technológia alkalmazása területén. Ilyen többek között a MedRec, amely a páciensek adatkezelését könnyítené meg az egészségügyi rendszerekben. A rendszer az Ethereumra épül, azzal az újítással, hogy az adatbányászatot az orvostani és egészségügyi kutatók végeznék, „fizetségért" az anonimizált orvosi metaadatokért. [25] Magyarországon 2017 februárjában megkezdődött az Elektronikus Egészségügyi Szolgáltató Tér (EESZT) éles próbaüzemet [26]. Az Állami Egészségügyi Ellátó Központ (ÁEEK) irányításával kifejlesztett, felhőalapú elektronikus rendszer összekapcsolja egymással a kórházi, a járóbeteg- és a háziorvosi ellátást, a gyógyszertárakat, a mentőszolgálatot, az ágazatirányítást és a lakosságot.

A BLOKKLÁNCOK TOVÁBBI LEHETSÉGES FELHASZNÁLÁSI TERÜLETEI [27]

A teljesség igénye nélkül, felsorolás jelleggel megadjuk azokat a területeket, ahol a blokkláncok a jövőben hatékonyan felhasználhatóak lesznek.

1. Digitális valuta, E-kereskedelem: ezen a téren megoldás a bitpay[14], amelyet használva a kiskereskedelemben, e-kereskedelemben, a számlázásban a vásárlók a világon bárhonnan elérhetik az adott felhasználót (eladót), és ő a kifizetéseket és elszámolásokat közvetlenül a saját bankszámlájára kapja meg a kért valutanemben.
    a) Globális kifizetések és átutalások: többek között az Abra15 lehetővé teszi a valuták átutalását és kifizetését akár saját bankszámlára, akár bankszámla nélkül az applikácón keresztül.
2) Okos szerződések a digitális jogok, (sport)fogadások, vagy azonosítás területén: a ShoCard cég többek között a felhasználó személyes adatai feletti ellenőrzést segíti elő, azáltal, hogy azokat csak engedéllyel lehet megosztani a másik féllel és egyen kérni kell a másik fél azonosítóját. [16]
3) Részvénykereskedelem (magánpiacok, adósságkezelés, finanszírozás, származékok kifizetése) területén a fentebb említett Nasdaq Linq.
4) Nyilvántartás:
    a) Egészségügy területén a fentebb említett MedRec;
    a) Gyémántok, drágakövek, műalkotások: a Barclays brit bank által fejlesztett Everledger [17] segítségvel nyomonkövethetővé és ellenőrízhetővé válnak ezek a vagyontárgyak.
    b) Cím nyilvántartás
    c) Tulajdonjog, szellemi tulajdon
    d) Szavazás, e-állampolgárok
    e) Közjegyzői feladatok: 2015 decembere óta a Bitnation cég az Észt kormánnyal együttműködve az e-polgárai számára közjegyzői szolgáltatást tesz elérhetővé. A blokkláncon keresztül képesek hitelesíteni például a házasságot, születési anyakönyvi kivonatot, az üzleti szerződéseket. [18]

[14] https://bitpay.com/
[15] https://www.goabra.com/
[16] https://shocard.com/shocards-use-cases/
[17] https://www.everledger.io/
[18] https://bitnation.co/blog/pressrelease-estonia-bitnation-public-notary-partnership/

A BLOKKLÁNCOK KATONAI FELHASZNÁLÁSA

2016. májusában mind az Egyesült Államok Nemzetvédelmi Minisztériuma, mind a NATO felhívást tett közzé a blokkláncok katonai alkalmazásának fejlesztésére. [28] [29] Az Egyesült Államok elsősorban kommunikációs céllal kívánja hasznosítani a blokklánc technológiát, azon belül is a titkosított üzenetküldés fejlesztésesét tűzték ki célul, amely során a műveleti támogató részlegeket decentralizálni lehet.

A kommunikáció mellett az „okos" szerződésekkel és dokumentumokkal remélhetőleg csökkentik kiberbiztonsági kitettségüket. A cél eléréséhez három fázist jelöltek meg, melyek magukba foglalják egy olyan üzenetküldési rendszert, mely a decentralizált elosztott főkönyvelésen és blokklánc technológián alapul, mely lehetővé teszi az üzenetek törölhetőségét és tagadását, titkosítást mindkét irányba (üzenetküldő felé és üzenetcímzett felé), élő és ön megsemmisítő üzenetek küldését, valamint egyszeri olvasásra („eyes-only") szóló üzenetek küldését és fogadását. Az első fázisban létező blokklánc technológiát használnának fel, míg a második fázisban saját fejlesztésekbe kezdenek és a harmadik fázisban válna elérhetővé szélesebb körben. Az első fázisban kiemelten a Linux Hyperledger Projektére koncentrálnak.

A NATO felhívása a 2016 Innovation Challenge-re a C4ISR[19] és kiberképességek fejlesztésére helyezi a hangsúlyt.

Négy területen tettek felhívást, ezek a következők:

- kibervédelem (azon belül belső elhárítás, helyzetfelismerés, többszintű biztosítás)
- Dolgok Internete (annak alkalmazása a katonai környezetben, okos bázisok létrehozása – kórházak, logisztikai központok, energiaellátás, adatsértetlenség, adatelemzés)
- Katonai alkalmazása (blokkláncok alkalmazása a katonai logisztikában, a beszerzésben, a pénzügyekben, egyéb területek)
- Számítógépes tanulás és kognitív számítástechnika (automatizált dokumentum minősítés, autonóm támogatás a kibertámadások elleni védelemben, autonóm rendszerek a call center-ek helyettesítésére, egyéb felhasználási területek).

Ahogyan a Big Data[20] megváltoztatta a mesterséges intelligenciát (MI), úgy a blokkláncok is hatással lesznek rá, három tényező miatt: decentralizált / megosztott ellenőrzés (felelősség), (2) állandóság / ellenőrzési nyomvonal és értékzsetonok kereskedése.

Trent McConaghy előadásában [30] kifejti, hogy a decentralizált ellenőrzés elősegíti az adatmegosztást, amelynek következtében jobb modellek készíthetők, függetlenül attól, hogy privát, konzorciumos vagy nyilvános blokkláncokat használnak. Másik előnye, hogy az adatmegosztással több adat lesz elérhető, ezzel nagyobb pontosságú modellek hozhatók létre. Az adatokat jelenleg birtokolni akarják a vállalatok (közösségi média, keresőszoftver cégek), ezért az adatmegosztásnak haszonnal kell párosulni számukra. Mivel a blokkláncok nagyfokú állandóságot mutatnak (hiszen majdhogynem lehetetlen őket módosítani). A decentralizált adatmegosztás felveti a világméretű adatmegosztást, amely sokkal nagyobb betekintést és elemzési lehetőségek rejt magában. Összeségében ez egy egészen új skálája lehet az adatállományoknak, melyek egyben minőségi adatok. Figyelembe kell azt is venni, hogy alapvetően feltételezzük, hogy ezeket az adatokat emberek fogják felhasználni, de a dolgok

[19] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissange – Vezetés, irányítás, híradás, informatika, hírszerzés, megfigyelés, felderítés.
[20] Nagy mennyiségű adat

internete és a mesterséges intelligencia nagy adatfelhasználó, miért ne lehetnének a felhasználói gépek? Az ellenőrzési nyomvonal lehetővé teszi, hogy megbizonyosodjanak egy adat minőségéről, megbízhatóságáról, hiszen a kiindulási adattól (blokk) az összes módosítás nyomon követhetővé válik. Az adatok értékesítésére megint lehetőséget biztosítanak a blokkláncok, hiszen a hozzáférést értékként kezeli. Mivel az adatok nincsenek egy központi cégnél (hozzáférési licenc, adattárolás, stb.), így saját döntés, hogy milyen adatot milyen szinten és kivel oszt meg a felhasználó (ingyenes vagy zsetonpénzért), beleérve a MI adatokat és modelleket.

KÖVETKEZTETÉSEK

Annak ellenére, hogy a blokkláncok fiatal technológiának számítanak, és alkalmazását egyfajta misztikum övezi, felhasználásának *sokrétűsége és megbízhatósága* új szintre emeli a peer-to-peer[21] és business-to-consumer (B2C)[22] interakciókat, mivel kiiktatja belőlük a közbenső technológiai – pénzügyi – egyéb központosított vállalatokat, ugyanakkor nagyobb kontrollt enged saját személyes digitalizált adataink felett.

Ez a technológia egyben lehetőséget teremt az M2M (machine-to-machine), azaz gépek közötti kommunikáció fejlesztéséhez a korábban említett biztonságossága révén. Jelenleg a dolgok internetének egyik kihívása az okos eszközök védelme, azok egymással való kommunikációjuk sebezehetősége. A blokklánc technológia erre nyújt megoldást és egyben csökkentheti a gépek által okozott (kommunikációs, internet) hálózatterhelést.

Kérdéses, hogy hogyan fognak átalakulni a „fékek és egyensúlyok”, a technológiák feletti ellenőrzés és szabályozás hogyan fog megoszlani a vállalatok, a nemzetek és a nemzetközi szervezetek között?

A blokkláncok decentralizáltsága felvet hatásköri problémákat az elszámoltathatóság és jogi felelősség területén, így egy nemzetközileg összehangolt jogi szabályozás létrehozása lenne célszerű egy regionális vagy nemzeti szintűvel szemben. E mellette a megosztott főkönyvek nem rendelkeznek jogi személyiséggel, így pl. az okos szerződéseknek sincs érvényesítő erejük.

A blokklánc technológia platformot biztosít jó és rossz tevékenységek, műveletek számára, azonban nem jelenti azt, hogy semleges technológia lenne (hiszen nem csupán a felhasználó szándékától függ, hanem magától a rendszertől, a többi adatbányásztól is). Mindazonáltal a legtisztább formájában a blokklánc elősegíti a hatalom újraelosztását a központi szereplőkön túl egy szélesebb társközösség között.

A jelenlegi technológia még nem igazán „felhasználóbarát” – ahogyan az első weboldalak is archaikusnak hatnak mai szemmel –, de az internet korszak kezdetéhez hasonló felfokozott várakozással tekintenek rá. Hamarosan kiderül, hogy a gyorsuló fejlesztések következtében a blokklánc technológia egy újabb lépcsőfokot jelent, vagy valóban új platformja lesz a web 4.0 korszakának.

[21] egyenrangú felek közötti kommunikáció
[22] e-kereskedelem és vásárló közötti közvetlen kapcsolat

FELHASZNÁLT IRODALOM

[1] *GKI Digital Zrt.: Digitalizációs helyzetkép a Magyar vállalatok körében* – felmérés 2016. március http://w5.siemens.com/web/hu/hu/digitalizacio/Documents/GKID_Siemens_digitalizacio_sajto2.pdf (A letöltés dátuma: 2017. február 18.)

[2] *Deloitte Insights: Blockchain technology: 9 benefits & 7 challenges*. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html (A letöltés dátuma: 2017. február 17.)

[3] MOUGAYAR, W.: *Why The Blockchain Is The New Website.* http://www.forbes.com/sites/valleyvoices/2015/12/21/why-the-blockchain-is-the-new-website/#3c1a9d2dac2e (A letöltés dátuma 2017. február 17.)

[4] Deloitte: *Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality.* https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf (A letöltés dátuma: 2017. február 17.)

[5] NAKAMOTO S.: *Bitcoin: A peer-to-peer electronic cash system* https://bitcoin.org/bitcoin.pdf (A letöltés dátuma: 2017. Január 30.)

[6] KNUTH, D. *Sorting and Searching.* In: The Art of Computer Programming, 3. Kötet, New Jersey, USA, 1973. pp.506-542.

[7] European Union Agency for Network and Information Security (ENISA): *Blockchain in Bitcoin cryptocurreny.* https://www.enisa.europa.eu/topics/national-csirt-network/glossary/blockchain (A letöltés dátuma: 2017. február 19.)

[8] *Blockchain Glossary, "Difficulty"*, https://support.blockchain.com/hc/en-us/articles/213276463-Bitcoin-terms-glossary (A letöltés dátuma: 2017. február 21.)

[9] PAGLIERY, J.: *Bitcoin fallacy lead to Silk Road foundator conviction. CNN Money* http://money.cnn.com/2015/02/05/technology/security/bitcoin-silk-road/index.html (A letöltés dátuma: 2017. február 20.)

[10] SHANNON, V.: *"A 'more revolutionary' Web". International Herald Tribune.* http://www.nytimes.com/2006/05/23/technology/23iht-web.html (A telöltés dátuma: 2017. Február 4.)

[11] *Ethereum:* https://www.ethereum-price.com/ (A letöltés dátuma: 2017. február 22.)

[12] *Ethereum blog: How to build serverless applications*, https://blog.ethereum.org/2016/07/12/build-server-less-applications-mist/ (A letöltés dátuma: 2017. február 23.)

[13] *Coindesk:* http://www.coindesk.com/unanimous-vote-blockchain-bill-arizona/ (A letöltés dátuma: 2017. Február 24.)

[14] FRANCO, P.: *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons. 2014. p. 95.

[15] BRITO, J.; CASTILLO, A.: *"Bitcoin: A Primer for Policymakers"* (PDF). Fairfax, VA: Mercatus Center, George Mason University. https://www.mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf (A telöltés dátuma: 2017. Február 2.)

[16] *Bitcoin Glossary:* https://bitcoin.org/en/glossary/hard-fork (A letöltés dátuma: 2017. február 20.)

[17] REUTZEL, B.: *"A Very Public Conflict Over Private Blockchains"*. *PaymentsSource*. New York, NY: SourceMedia, Inc. https://www.paymentssource.com/news/a-very-public-conflict-over-private-blockchains

[18] Ethereum blog: *On Public and Private blockchains.* https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (A letöltés dátuma: 2017. február 20.)

[19] KELLY, J.:*"Exclusive: Blockchain platform developed by banks to be open-source"* http://uk.reuters.com/article/us-banks-blockchain-r3-exclusive-idUKKCN12K17E (A letöltés dátuma: 2017. február 21.)

[20] *R3 :* https://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services (A letöltés dátuma: 2017. február 22.)

[21] *Hyperledger.org*: https://www.hyperledger.org/ (A letöltés dátuma: 2017. február 22.)

[22] *Nasdaq:* http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326 (A letöltés dátuma: 2017. Február 22.)

[23] *Gulf News:* http://gulfnews.com/news/uae/government/dubai-launches-blockchain-strategy-to-become-paperless-by-2020-1.1907790 (A letöltés dátuma 2017. Február 23.)

[24] *Cointelegraph*: https://cointelegraph.com/news/suddenly-dubai-aims-to-become-first-blockchain-powered-city-by-2020 (A letöltés dátuma: 2017. Február 23.)

[25] EKBLAW, A., AZARIA A.: MedRec: Medical Data Management on the Blockchain. https://www.pubpub.org/pub/medrec (A letöltés dátuma: 2017. Február 23.)

[26] eGov hírlevél: *Megkezdődött az elektronikus egészségügyi szolgáltatási tér próbaüzeme.* http://hirlevel.egov.hu/2017/02/18/megkezdodott-az-elektronikus-egeszsegugyi-szolgaltatasi-ter-probauzeme/ (A letöltés dátuma 2017 március 16.)

[27] *BTCS.com:* http://btcs.com/index.php#merger-modal (A letöltés dátuma: 2017. Február 23.)

[28] Projekt felhívás: http://www.acq.osd.mil/osbp/sbir/solicitations/sbir20162/preface162.pdf (A letöltés dátuma: 2017. Február 23.)

[29] NATO felhívás: https://www.ncia.nato.int/NewsRoom/Pages/160425_Innovation.aspx (A letöltés dátuma: 2017. Február 23.)

[30] MCONAGHY, T.: *How blockchains could transform artificial intelligence, Dataconomy.* http://dataconomy.com/2016/12/blockchains-for-artificial-intelligence/ (A letöltés dátuma: 2017. Február 24.)