Blokklánc alkalmazási lehetőségek a biztonság területén és bevezetés-tervezésük

Kocsis Imre

Budapesti Műszaki és Gazdaságtudományi Egyetem, Méréstechnika és Információs Rendszerek Tanszék, Budapest

Beérkezett: 2020. szeptember 25. Elfogadva: 2020. november 19.

Összefoglalás

A blokklánc-technológiákat első sikeres alkalmazásuk, a kriptopénzek tették híressé és hírhedtté. Valódi jelentőségük azonban az általuk létrehozott új informatikai rendszerkategóriában, az adatbázis jellegű, több résztvevő által közösen hitelesen tartott elosztott főkönyvekben rejlik. A tanulmány ismerteti ezek alapelveit, jellemző üzleti alkalmazási mintáit és a „blokkláncosítást", mint bevezetési stratégia tervezési elvet. Új eredményként a blokkláncosítás a biztonság területén alkalmazhatóságának megteremtéséhez felállításra kerül egy ismert példákon alapuló érték-modell.

Kulcsszavak: blokklánc, elosztott főkönyvi technológiák, blokkláncosítás, biztonsági alkalmazások

Blockchain application opportunities in security and planning their introduction

Imre Kocsis

Budapest University of Technology and Economics, Department of Measurement and Information Systems, Budapest, Hungary

Summary

Blockchain technologies were made famous – and arguably, infamous – by their first successful application: cryptocurrencies. Their true significance, however, lies in the novel IT system category they established: distributed ledgers, which are electronic systems of records maintained by multiple parties. The paper summarizes the key concepts of distributed ledger technologies, their key business application types and „blockchainification" as an innovation strategy planning methodology. As a novel contribution, the paper proposes the application of „blockchainification" in the complex context of security, and sets up an initial version of the necessary domain-specific value and application type framework.

Distributed Ledger Technologies (DLT) have reached maturity where they can be applied to, and have been demonstrated to be able to, facilitate a very broad range of cross-organizational and client-organization cooperation patterns. For enterprise and industrial usage, DLT key value dimensions, supporting blockchain capbilities and value driver application types have been already collected, facilitating the structured and benefit-based planning of their introduction.

One such approach is what we coined „blockchainification". Blockchainification starts with a decomposition of the business architecture of an organization, to the point where specific cooperations can be characterized, both functionally and by the parties involved. Given such a decomposition, the viability of migrating or replacing the functionality with a DLT-based solution can be assessed, on a cooperation by cooperation basis, including the associated risks and benefits. This way, a blockchain introduction strategy can be formulated for the gradual introduction of DLTs. Additionally, blockchainification suggests – at least in the first phases of an introduction strategy – an emphasis on solutions where a DLT essentially just „replaces" the current information system support of already-digitized cooperations.

While in the enterprise and industrial sphere blockchainification is already facilitated by an example-based understanding of key value dimensions, blockchain capabilities and value driver applications, for many other domains, these prerequisites are missing. Importantly, what is already available is not readily applicable for organizations involved in security activities in the broad sense; in many aspects, the value these organizations seek from IT systems is markedly different from the enterprise world. Thus, the paper proposes an initial key value dimension and supporting blockchain capability model for organizations involved in providing a select set of security services.

Keywords: blockchain, distributed ledger technologies, blockchainification, security applications

Bevezető

Ma már a gyakorlat is bizonyítja, hogy a blokklánc (*blockchain*) alapú, több szereplő által konszenzuálisan karbantartott, elosztott adatbázisok nagyságrendi minőségi javulást tudnak hozni mind az üzleti szervezetközi együttműködésben, mind az üzleti szereplők ügyfeleikkel való együttműködésében. Fő értékük elosztottságuk mellett az, hogy a kooperációs folyamatokat visszakövethetővé és letagadhatatlanná teszik, ezáltal növelve a felek közötti bizalmat és a hatékonyságot is. Bizonyos területeken funkciók „közösségiesítését" is lehetővé teszik (pl. biztosítás, hitelezés), ám ezen alkalmazásokkal szemben ma még jelentős a bizalmatlanság és bizonytalanság.

Az üzleti élet mellett azonban példák széles sora bizonyítja, hogy a blokklánc rendszerek alkalmazása új értéket teremthet számos más területen is, a kormányzati és közigazgatási funkcióktól az oktatáson keresztül a tudományos kollaborációig. A terület jellegéből adódóan sokszor láthatóan visszafogott nyilvánossággal, de megindult a blokkláncok *biztonsági* területeken való alkalmazásának feltérképezése és megvalósítása is. Ilyen területek:

– a kibervédelem és adatbiztonság,
– a kritikus infrastruktúrák védelme,
– a katasztrófavédelem- és elhárítás,
– a rendvédelem,
– a honvédelem és
– a hírszerzés.

Az ezen területeken tevékeny szervezetek más, de legalábbis egészen máshogy súlyozott ösztönző és „büntető" faktorok mentén üzemelnek, mint a profitorientált vállalatok, illetve a pénzügyi alkalmazásokat használó magánszemélyek. A fenti feladatköröket jellemzően állami szervek látják el, illetve az adatbiztonság (*security*) biztosítása egy szervezeten belüli olyan funkció, ami nem szorosan csatolt az „üzletmenet" teljesítménymutatóihoz.

Jelen tanulmány bevezeti a blokkláncok és a blokklánc alapon megvalósított ún. elosztott főkönyvi technológia (*Distributed Ledger Technology*, *DLT*) alapfogalmait és alapvető alkalmazási kategóriáit. A tanulmány röviden tárgyalja a blokklánc bevezetés szisztematikus tervezésének fő kérdéseit és bemutatja az ún. „blokkláncosítás" metodológiáját. Végül a fenti területek kontextusában – példákkal alátámasztva – javasolja a DLT alkalmazások céljainak és előnyeinek egy modelljét, melyek a DLT alkalmazások bevezetésének hajtóerejét adhatják.

A kezdetek: Bitcoin és blokklánc

Az első széles körben sikeres rendszer, melyre mint a „blokklánc" paradigma létrehozója hivatkozunk, a Bitcoin volt. A máig ismeretlen valódi identitású Satoshi Nakamoto 2008 végén publikálta cikkét, melyben számítógépek egy olyan nyílt hálózatát írja le, ahol az egymással az Interneten keresztül kommunikáló gépek közösen tartanak karban egy főkönyv-szerű adatbázist. Az adatbázis tartalmát kriptográfiai címekhez, mint egyfajta álnévhez tartozó pénzmennyiségek adják; a rendszer számítógépeitől az Interneten bárki kérhet címek között "átutalás" jellegű tranzakciókat, aki megfelelő digitális aláírással bizonyítani tudja, hogy a forráscímhez tartozó titkos kriptográfiai kulcs birtokában van.

A Bitcoin hálózat által könyvelt „pénznek", a Bitcoinnak nincs központi kibocsátója; a rendszer működése során jön létre úgy, hogy a rendszerben részt vevő számítógépek üzemeltetői jutnak véletlenszerűen „új" Bitcoinhoz a rendszer üzemeltetése során. A rendszer biztonságát az adja, hogy az elfogadni kívánt tranzakciók következő *blokkjáról* a csomópontok egy protokoll – úgynevezett *konszenzus mechanizmus* – segítségével döntenek. Ez biztosítja a főkönyv integritását egészen addig, amíg a résztvevők – a Bitcoin esetén konkrétan a résztvevő számítási kapacitás – elégséges többsége azonos, „őszinte" döntésre jut. Mivel a főkönyvet karbantartó konszenzus folyamatban való részvétel az Interneten keresztül nyílt, a támadások helyett, az „őszinte" viselkedést egy „gazdasági ösztönzőerő" (*economic incentive*) ösztönzi: az újonnan létrejövő Bitcoinhoz (és az újonnan blokkba foglalt tranzakciók Bitcoinban nominált tranzakciós díjához) jutás reménye, illetve lehetősége.

Digitális pénz sémák már a Bitcoin előtt is léteztek; a Bitcoin egyik áttörés értékű aspektusa, hogy egy nyílt elosztott rendszerrel oldja meg az ún. kétszeres költés (*double spending*) problémáját. A közös, rengeteg számítógép által replikált és karbantartott főkönyv igen nehézzé, kevés számítási és hálózati erőforrással rendelkező támadó számára praktikusan lehetetlenné teszi, hogy már „átutalt" pénzt egy felhasználó újra felhasználjon, vagy akár több résztvevő úgy módosítsa a főkönyvet, hogy a már elfogadott tranzakciókat bármilyen szempontból módosítsa (ideértve a „meg nem történtté" tételt is).

A Bitcoin igazi jelentősége azonban nem csak az első sikeres kriptopénz létrehozatalában keresendő, hanem abban is, hogy bizonyította: megfelelő műszaki konstrukcióval és részvételi ösztönzőkkel létrehozhatóak olyan „főkönyv" jellegű adatszerkezetek, melyekben a főkönyv hitelessége nem egy központi szereplőn múlik. Az e sémát követő rendszereket modern terminológiában *elosztott főkönyvi technológiáknak* (*distributed ledger technologies, DLT*) nevezzük.

A „*blokklánc*" kifejezés valójában „csak" egy megvalósítási részletre utal. A Bitcoin-ban és számos, a Bitcoin alapján létrejött technológiában – amellett, hogy a résztvevők kötegelve, *blokkonként* döntenek a következő elfogadandó tranzakció halmazról – minden blokk magában foglalja az *előző* blokk kriptográfiai ujjlenyomatát, *hash*-ét. DLT rendszer azonban más megközelítésekben is létrehozható (bár többségük ma valóban egyben blokklánc rendszer is).

Elosztott főkönyvi technológiák

A Cambridge Framework-öt segítségül hívva *„a DLT rendszerek olyan elektronikus adatbázisok, melyek lehetővé teszik független szereplők számára, hogy konszenzusra jussanak egy megosztott „főkönyv" tartalmával kapcsolatban – anélkül, hogy egy központi koordinátorra kellene hagyatkozniuk a bejegyzések egy autoritatív változatáért" (Rauchs et al. 2018: 23).*

A DLT-k általános működési elvét az *1. ábra* szemlélteti. Az elosztott főkönyvi rendszer felhasználója létrehoz egy tranzakciójavaslatot, melyet digitálisan aláír egy olyan szoftver vagy hardver megoldással, melyre a szakterület kriptopénz-gyökerei miatt *tárcaként* (*wallet*) szokás hivatkozni, s mely jellemzően a felhasználó titkos kulcsait is kezeli. A létrehozott tranzakciójavaslatot tudatja az elosztott főkönyvi rendszerrel, melynek csomópontjai valamely konszenzusmechanizmus segítségével megállapodnak a tranzakciók sorrendjéről, elfogadhatóságáról és arról, hogy a tranzakció hatására hogyan kell módosítani a főkönyvet.

Az ilyen rendszerek általános, jórészt technológiától független előnyei a következőek.

- Megosztott bejegyzéskövetés
- Többszereplős konszenzus
- Független validáció
- Utólagos módosítási kísérletekkel szemben való ellenállóképesség

Megosztott bejegyzéskövetés alatt azt értjük, hogy a főkönyv jellegű adatbázis bejegyzéseit az üzemeltető felek kollektívan hozzák létre, mindegyikőjüknél másolatot hozva létre. Megjegyzendő, hogy az olyan modern vállalati DLT-k, mint pl. a Hyperledger Fabric *(Androulaki et al. 2018)*, az R3 Corda és a Digital Asset Canton képesek az adatterítés körét a „tudni kell" – *need to know* – elv mentén szűkíteni, illetve az ún. *tudásmentes bizonyítási* kriptográfiai sémák – *Zero-Knowledge Proof*, *ZKP (ZKProof 2019)* – egyre inkább lehetővé teszik, hogy a minden csomóponton replikált adatokat csak az egyes tranzakciók szempontjából illetékes felek tudják értelmezni (mint tranzakciót „ellenőrizni" viszont mindenki).

A főkönyv adatmodellje és a támogatott tranzakciók egy kriptopénzt könyvelő DLT esetén jórészt adódnak a rendszer funkciójából: a főkönyv a kriptopénz tulajdonviszonyait követi. Az Ethereum *(Wood 2017)* hálózathoz köthető az az innováció, hogy a felhasználók programkódban fogalmazhatnak meg saját üzleti logikát leíró tranzakciótípusokat. Ezeket a programokat szokásosan okosszerződéseknek (*smart contracts*) nevezzük. Okosszerződésekkel a legkülönbözőbb funkciókat alakították ki a felhasználók az Ethereum hálózaton; automatizált kifizetésű biztosításoktól kezdve, közösségi közlekedési sémákon keresztül, különböző befektetési eszközökig, és algoritmikusan megvalósított vállalatokig.

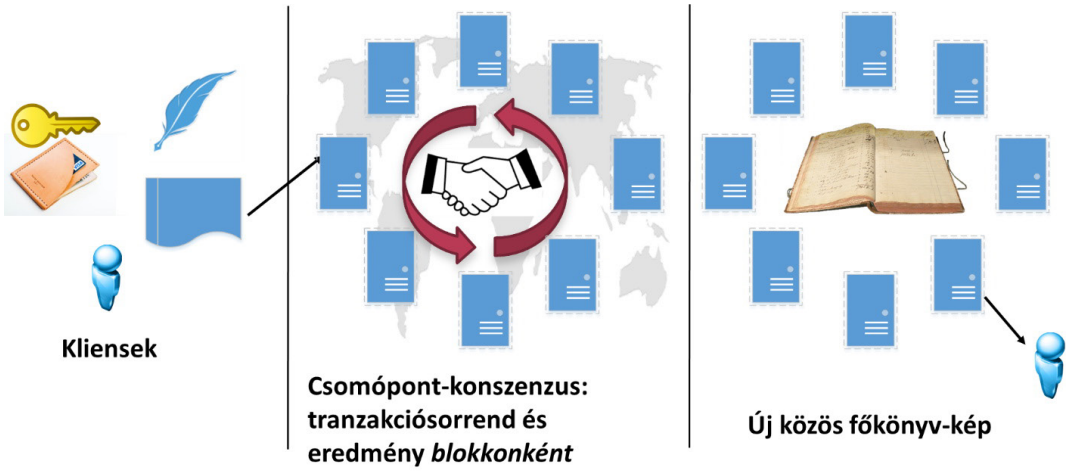
Az okosszerződéseket ma már gyakorlatilag minden – általános üzleti alkalmazást megcélzó – DLT támogatja.

Hálózat-típusok

Bár a DLT rendszerek működési elveikben mind a fent bemutatott sémára illeszkednek, jellemző és lehetséges alkalmazásaikat két fő tulajdonságuk alapvetően határozza meg.

Részvétel jellege a konszenzusfolyamatban. Ha a rendszer üzemeltetésében, azaz a konszenzusfolyamatban való részvétel (az Interneten keresztül) nyílt, akkor *nemjogosultságkezelt* (*unpermissioned*) DLT-ről beszélünk. Ezzel szemben, ha a részvétel jogosultság-ellenőrzéshez kötött – pl. cégek egy konzorciumára korlátozott –, akkor *jogosultságkezelt* (*permissioned*) rendszerről beszélünk.

Hálózathoz hozzáférés jellege. Ha a DLT hálózat (az Interneten keresztül) szabadon hozzáférhető a felhasz-



1. ábra | A DLT rendszerek általános működési elve

nálók számára, akkor *nyílt* (*public*) hálózatról beszélünk; a felhasználói hozzáférést szabályozó hálózatokat pedig *zártnak* (*private*) nevezzük.

E két típus mentén három, a gyakorlat szempontjából is meghatározó hálózattípust különböztetünk meg.

Publikus, nem jogosultságkezelt blokkláncok

E kategóriában mind a részvétel, mind a hozzáférés szabad. Ezek a rendszerek tipikusan nagy, világméretű *peer-to-peer* hálózatok; a kriptopénz-funkció jelenléte törvényszerűnek tekinthető, hiszen a kriptopénzhez jutás reménye az, ami az üzemeltetők minél nagyobb részvételét, és a szabálykövető magatartást ösztönzi. E kategória legismertebb példái olyan közismert hálózatok, mint a Bitcoin, az Ethereum és a kifejezetten privacy-orientációjú ZCash. Áteresztőképességük viszonylag alacsony, a tranzakciók irreverzibilis befogadásának késleltetése pedig tipikusan magas (tíz-másodpercektől egy óráig).

Publikus, jogosultságkezelt blokkláncok

A korlátozott teljesítmény a nem-jogosultságkezelt konszenzus – „akárki beállíthatja a számítógépeit a rendszerbe" – ma alkalmazott megoldásainak alapvető tulajdonságaiból fakad. E problémák kiküszöbölésének egy módja, ha ismert szervezetek egy diverz közössége végzi a konszenzusfolyamat működtetését (hatékonyabb konszenzus-protokollokkal), miközben a szabad hozzáférésű használat lehetőségét fenntartjuk.

Az ilyen jellegű hálózatok viszonylag újak a „klasszikus" DLT-khez képest; közös jellemzőjük, hogy tipikusan iparág-specifikusak. Ide sorolható például az XRP Ledger hálózat nemzetközi átutalások támogatására, vagy az Energy Web Chain az energiaszektorban, illetve a Facebook Libra kezdeményezése.

A publikus hálózatokra tekinthetünk úgy, mint egyfajta „közmű"; saját csomópont futtatása nélkül is használhatóak és szó szerint az „egész világ" látja a főkönyv aktuális és korábbi tartalmát.

Zárt, jogosultságkezelt rendszerek

A harmadik kategóriát azok a hálózatok adják, melyeket szervezetek egy konzorciuma kifejezetten a saját együttműködésük támogatása érdekében hoz létre, s melyhez csak saját rendszereik és alkalmazottaik férhetnek hozzá. Ezek a DLT rendszerek a szervezetközi együttműködés dedikált infrastruktúrái, tervezhető teljesítménnyel és jól kontrollálható információ-megosztással.

A konzorciális hálózatok talán első, igazán sikeres alkalmazási területe a szállítási láncok kezelése (*supply chain management*) volt (lásd pl. a TradeLens konténerhajózási platformot). A globális szállítási láncokban nagyszámú szereplő vesz részt, a teljes folyamat sok lépésből áll, a lépések dokumentáció-igényesek és a vitás kérdések rendezése hosszadalmas és költséges.

A teljes folyamatot lehet digitalizálni egy központosított adatbázissal, ez azonban nem csak a szolgáltatótól függés problémáját veti fel, de törvényi és szabályozói korlátokba is ütközhet (pl. az adatok kezelése történhete adott esetben másik kontinensen). Felmerülnek üzletmenet-folytonossági kockázatok is.

A központosított megoldással szemben a DLT alapú szállítási lánc kezelés esetén minden résztvevő szervezet rendelkezik (legalább) az őt érintő szállítási események, és az azokhoz csatolt dokumentumok digitális aláírásokkal hitelesített kópiáival. A folyamatok felgyorsulnak, és a vitára okot adó helyzetek többsége vagy megszűnik, vagy gyorsan feloldhatóvá válik – a folyamatok úgymond „súrlódásmentessé" (*frictionless*) válnak.

Látható, hogy üzleti szinten a DLT alkalmazásának fő ösztönzője ebben az esetben, a hatékonyság és a bizalom növelésén keresztül, az együttműködés költségének csökkenése. Ma még általánosan igaz az, hogy az üzleti szervezetek számára a DLT alkalmazásának fő ösztönző ereje ez a költségcsökkentési potenciál.

Hálózat-típusok és szoftvertámogatásuk

A DLT-k esetén a *hálózat létrehozására alkalmas szoftvertechnológia,* és az azokkal létrehozott *hálózatok* különböző fogalmak. A (fő) Bitcoin és Ethereum hálózat csomópontjai által használt Bitcoin és Ethereum szoftver alkalmas más típusú, akár konzorciális hálózatok létrehozására is (a Bitcoin vállalati képességekkel kiegészített egy változata, ún. "*fork*"-ja a MultiChain, az Ethereumé pedig a Quorum). A kifejezetten konzorciális alkalmazási esetekhez készült technológiák – mint pl. a Linux Foundation által vezetett Hyperledger projekt DLT-keretrendszereinek többsége – pedig kifejezetten sok, testreszabott, egy-egy üzleti együttműködést támogató hálózat felállításának támogatására jött létre.

DLT-k és blokkláncok jellemző alkalmazásai

A már ma is sikeresnek tekinthető üzleti célú DLT használati esetek természetesen messze nem csak a beszállítói láncokra korlátozódnak. Szakirodalmi és ipari források alapján a DLT által megvalósított funkcionalitás kategorizálható a következőképpen:

- Közhitelesítés-jellegű regiszterek
- Munkafolyamat-követő dinamikus regiszterek
- Piacterek
- Pénzügyi infrastruktúra
- Adatcsere- és hozzáférés támogatása

A jelen cikk szempontjából kiemelt jelentőségű kategóriákat a továbbiakban röviden ismertetem (elhanyagolva a piactereket és a pénzügyi infrastruktúrákat). Már itt érdemes megfigyelni, hogy a kategóriák alá eső konk-

rét alkalmazástípusok – mint például az eszközkövetés – számos szektorban relevánsak lehetnek. Általánosságuk miatt így szokás ezeket (használati eset) mintának (*pattern*) is hívni. A *World Economic Forum* (*WEF*) elemzése *(Warren-Treat 2019)* jó kiindulópont a használati esetek szélesebb körű megismeréséhez.

Közhitelesítés-jellegű regiszterek

Ezen használati esetekben a DLT, mint egyfajta „közösen hitelesített" adatbázis funkcionál. A *Massachusetts Institute of Technology* sikeres blokklánc feletti diplomaregisztráció prototípusa alapján létrejött BlockCerts nyílt keretrendszer segítségével, blokklánc alapú tanúsítványok széles köre hozható létre. Több ország is vizsgálja a földhivatali nyilvántartás DLT-re migrálását. Az identitáskezelést is lehetséges DLT alapokra helyezni; ennek fő előnye, hogy lehetővé teszi az azonosító szervek által kiadott, és egyéb tanúsítványok birtokló általi kezelését (*self-sovereign identity, SSI*), fenntartva azonban a tanúsítványok kibocsátó általi viszavonhatóságát. (Lásd pl. a Hyperledger Indy projektet és a Sovrin hálózatot.)

Munkafolyamat-követő dinamikus regiszterek

A központosított rendszereken alapuló informatika számos alkalmazásának fő célja a munkafolyamatok követésének és végrehajtásának digitalizálása. A munkafolyamatok DLT-kre migrálásának egyik aspektusa a folyamatok egyes lépései közötti adatátadás hitelességének és letagadhatatlanságának biztosítása. Hasonlóan fontos képesség azonban a folyamatvégrehajtás szereplők közötti sorrendjének kikényszerítése, és a folyamatvégrehajtás állapotának követése – hitelesen, letagadhatatlanul, és a kooperáló felek számára követhető módon. A szállítási láncokon túl ezért számos területen állnak alapvetően a sokszereplős munkafolyamatokat támogató DLT megoldások bevezetés alatt. Ezek közé tartozik az eszközkövetés- és kezelés (*asset tracking*), az eredetkövetés (*provenance tracking*), a dokumentumok – sokszor tényleges szerződések – követése, és a különböző kereskedési platformok üzletkötés utáni elszámolási tevékenységei (*settlement*).

Adatcsere és -hozzáférés támogatása

A DLT-k különösen alkalmasak a szervezetközi adatcsere és adathozzáférés követésére és kezelésére. Bár az itt felmerülő használati esetek jó része a munkafolyamat-kategóriába is sorolható lenne, az adatkezelés mégis külön kategóriát igényel annak köszönhetően, hogy a megfelelő erőforráskiépítésű konzorciális DLT-k *közvetlen adattárolásra* is alkalmasak, viszonylag magas áteresztőképességgel. Ez megnyitotta alkalmazásuk lehetőségét olyan használati esetekben, ahol közvetlenül IoT forrásokból származó adatok, illetve azok aggregátumai kerülnek a főkönyvön tárolásra *(Christidis–Devetsikiotis 2016)*. Csak egy példát kiemelve: az önvezető járművek térnyerésével ezek a megoldások fontos szerepet fognak kapni, pl. közigazgatási, szervíztámogatási, biztosítási használati esetekben.

Blokklánc bevezetés, stratégiák és „blokkláncosítás"

Napjainkban már egyértelmű, hogy a DLT-kben rejlő innovációs potenciál a szervezetközi együttműködésben igen nagy; gazdasági szempontból valószínűleg messze túlmutat a kriptopénzeken. A potenciál mellett azonban, mint minden új technológia, a DLT-k kockázatokat is hordozhatnak (különösen adatvédelmi szempontokból nézve), alkalmazásuk pozitív hatása nem minden üzleti részterületen azonos és egyes területeken műszaki tulajdonságaik (pl. késleltetés-korlátok) miatt nem alkalmazhatóak.

Így annak vizsgálata, hogy új értéket teremt-e egy blokklánc alapú megoldás bevezetése egy adott területen – az esetleges negatívumokat is ellensúlyozva – tudatos elemzést igényel. Ma már számos egyszerű, folyamatábra jellegű döntési modell ismert a „szükséges-e blokklánc" kérdés eldöntésére (lásd pl. *Peck 2017)*, de ezek gyakorlati hátránya pont túlzott egyszerűségük. A szisztematikus elemzés metodológiái ma még kialakulóban vannak és egyelőre jellemzően üzleti fókuszúak.

Blokklánc megoldások érték-modellezése

Előremutató eredményként a WEF elemzése *(Warren–Treat 2019)* felállít egy (üzleti fókuszú) blokklánc-érték keretrendszert, a következő fő elemekkel.

- Kulcs (érték)dimenziók (*key dimensions*): a blokklánc lehetséges üzleti modell szintű hatásai. Az azonosított elemek a „nyereségesség és minőség növelése", a „résztvevők közötti transzparencia növelése" és a „termékek és folyamatok megújítása".
- Képességek (*capabilities*): a blokklánc technológiák azon tulajdonságai, melyek lehetővé teszik az üzleti modell szintű hatások realizálását. (Például: teljes visszakövethetőség, automatizáció okosszerződésekkel, megosztott adatkezelés).
- Értékteremtő funkciók (*value drivers*): a blokklánc alkalmazásának konkrét cél-kategóriái. Ezek között megtalálhatóak azok a jellemző alkalmazások (mint pl. az eszközkövetés- és kezelés, vagy a piacterek létrehozása), amiket a korábban bemutatott modellünk rendszerez, de olyan, tisztán úgynevezett extrafunkcionális (azaz a megvalósított funkcionalitáson túlmutató) célok is, mint az ellenállóképesség (resiliency) vagy az auditálhatóság (auditability).

A WEF által publikált innovációs megközelítés lényege, hogy egy szervezetnek először az egyes kulcs dimen-

ziókban érdemes azonosítania üzleti modell szintű problémáit és a sejtett új lehetőségeket, majd ezekre megvizsgálni, hogy van-e olyan blokklánc képesség, mely új értéket teremthet ezek kontextusában, végül pedig azonosítani a megfelelő blokklánc értékteremtő funkciót. Például: a szállítmányozásban probléma az áruk mozgásának és aktuális helyének nem, vagy elégtelen láthatósága. A blokklánc a teljes, szinte valósidejű visszakövethetőség (*full traceability*) képességével ezt a problémát képes orvosolni, a számos példából ismert, eszközkövetést megvalósító elosztott főkönyv jellegű alkalmazásával.

Blokkláncosítás

A BME Méréstechnika és Információs Rendszerek Tanszékén kialakított, úgynevezett „blokkláncosítási" (*blockhchainification*) paradigma két fő aspektus tekintetében mutat túl a WEF megközelítésén (és más hasonló, kiemelten üzleti fókuszú és „top-down" megközelítéseken, melyek ismertetésére jelen tanulmányban nincs lehetőség).

Dekompozíció és megvalósítás-migráció. Megközelítésünk alapja a szervezeti funkció-dekompozíció, addig a szintig, ahol a szervezet által végzett különböző kooperációkra az ismert blokklánc alkalmazások előnyei és kockázatai már rendre, szisztematikusan vizsgálhatóak (ez a vizsgálat történhet pl. a WEF által javasolt megközelítés alapján is). Az elégségesen finom dekompozíció egyik kiemelt előnye, hogy képes felfedni olyan szervezetközi, vagy szervezet–ügyfél kooperációs eseteket is, ahol a kooperáció már erősen digitalizált és a blokklánc bevezetés megtörténhet egy olyan DLT-migrációval, mely mind a kooperáció folyamatait, mind felhasználó oldali és szervezeten belüli informatikai integrációs támogatását szinte érintetlenül hagyja. (A leegyszerűbb példa: e-mail alapú kommunikáció, vagy egy központosított érkeztetési tárhely „lecserélése" DLT-re.) A javasolt dekompozíció egy jól kidolgozott példáját mutatja be vasútüzleti és vasútüzemi kontextusban *(Kuperberg–Kindler–Jeschke 2019)*.

Fokozatos bevezetési stratégia kialakítása. A szisztematikus vizsgálat felfedi a DLT bevezetési lehetőségek egy körét. Ezek előny és kockázat szempontjából sorrendezhetőek és lehetővé teszik a blokklánc megoldások tervezett, *fokozatos* bevezetését. Blokkláncosítási paradigmánk része, hogy javasoljuk a stratégia kezdeti lépései során a megvalósítás-migráció előnyben részesítését.

Blokklánc alkalmazások és értékük a biztonság területén

A blokklánc bevezetés tervezési metodológiái feltételezik azt, hogy megfelelően azonosítani tudjuk – a WEF keretrendszerének terminológiájában – az adott szervezet számára releváns kulcsdimenziókat, képességeket és értékteremtő funkciókat. Ideális esetben ezeket egy keretrendszer össze is gyűjti, mint teszi azt a WEF üzleti fókuszú modellje is.

A biztonság a bevezetőben kijelölt területein azonban ez a modell nem alkalmazható közvetlenül. A vonatkozó szervezetek – jellemzően közfunkciójukból adódóan – nem nyereségmaximalizálásra törekednek, így legfőbb kulcsdimenzióik és a legrelevánsabb kiemelt blokkláncképességek legalább részben eltérőek.

Így jelen tanulmány példák alapján – és a szerző tudomása szerint ebben a formában újszerű módon – megkísérel felállítani egy olyan kulcsdimenzió- és képességmodellt, mely segítségével rendszerezetten vizsgálhatóvá válik konkrét biztonsági funkciók informatikai támogatása esetén, hogy nyújthat-e előnyt a blokklánc alkalmazása. (Az értékteremtő funkciókra ez nem szükséges; egyrészt azok lehetséges köre nagyon hasonló, mint más területeken, másrészt pedig ezeket a hivatkozott példák is fogják szemléltetni.) A kulcsdimenziók az eredeti WEF modellhez képest jórészt helyettesítő szerepűek, míg a képességek az ott megjelöltek hangsúlyos kiegészítői.

Mint látni fogjuk, a képességek több példa esetén is közvetlenül a blokklánc alkalmazás céljaként szerepelnek. Ezt részben magyarázza a terület sajátos jellege; de az is, hogy a szisztematikus bevezetés-tervezés metodológiái még csak kialakulóban vannak. Így, mint ahogy azt a blokkláncosítás paradigmája is javasolja, „első lépésként" mindenképp követhető út a létező funkciók (viszonylag kézenfekvő) DLT-re implementáció-migrációját vizsgálni.

Kulcsdimenziók a biztonság területén

Felügyeleti és ellenőrzési hatékonyság növelése

Az első lehetséges értékelem egyben kivétel is abból a szempontból, hogy feltételezi, hogy egy műszaki, társadalmi vagy üzleti területen *már megtörtént* a blokklánc bevezetés, a terület saját szempontrendszere alapján értéket teremtve. Ez esetben, a már létrejött blokklánc platformon, egy felügyeleti, illetve szabályozói jogosítványokkal rendelkező szervezet *valós időben* auditálhatja az (üzleti, vagy köz-) szereplők között elosztott adatbázis változásait. A szervezet – megfelelő platformmechanizmusok, illetve megfelelő okosszerződés-támogatás esetén – arra is jogot szerezhet, hogy módosításokat megakadályozzon, vagy visszavonasson. A meglévő megoldás, mint előfeltétel miatt ezen a területen kifejezetten biztonsági példákról még nem számolhatunk be, de a potenciál egyértelmű, pl. a kritikus infrastruktúrák felügyelete területén (pl. villamosenergiaellátás-menedzsment *(Andoni et al. 2019)*), vagy a városi rendvédelem esetén (okos város alapokon *(Xie et al. 2019)*).

Általánosan igaz az, hogy az ipar *(Bodkhe et al. 2020)*, az IoT *(Reyna et al. 2018)*, az energiaszolgáltatás *(Andoni et al. 2019)*, a telekommunikáció (*Praveen et*

al. 2020), az egészségügy *(Shi et al. 2020)* a szállítmányozás *(Petersen–Hackius–von See 2018)* és „az okos város" *(Xie et al. 2019)* olyan területek, ahol a blokklánc rendszerek alkalmazásai megjelenőben vannak. Így az ezekhez kapcsolódó biztonsági tevékenységek potenciálisan kiaknázhatják azt, hogy megfelelő felhatalmazással felügyeleti-ellenőrzési szerep nyerhető a megoldásokban.

Megjegyezzük, hogy egy felügyelő-ellenőrző szerv maga is aktív szerepet vállalhat a „hatékonyan felügyelhető tranzakciós környezet" kialakításában, mint azt pl. a Magyar Nemzeti Bank 11473/2020 iktatószámú, „Lakásbiztosítás nyilvántartás DLT" tárgyú közbeszerzési felhívása szemlélteti hazánkban.

Automatizált szabályalkalmazás és -végrehajtás

Az „okosszerződések" nevének ellentmondása, hogy általános értelemben se nem „okosak", se nem „szerződések". Megfelelően kialakítva őket (és megfelelő jogi környezetet teremtve) azonban sok esetben alkalmasak *szabályalkalmazásra* és *végrehajtásra*; egyszerű példa egy forgalmi sebesség-adatokat fogadó blokkláncban (okos kereszteződések, gépjárműbiztosítás támogatása, szállítmányozás-követés, …) a gyorshajtás felismerésének és büntetésének automatizálása.

„Súrlódásmentes" szervezetközi kooperáció

A biztonsági szervezetek többsége nonprofit jellege mellett *szervezet a klasszikus értelemben* – így a hatékony külső-belső kooperáció annak ellenére fontos számukra, hogy teljesítményüket végső soron nem pénzügyi nyereségben mérik. Így azon blokklánc használati esetek, melyek a szervezetközi, és adott esetben nagy szervezeten belüli folyamatok hatékonyságát növelik, sokszor közvetlenül alkalmazhatóak – kiemelendő példa a fegyveres erők beszállítói és ellátási lánc kezelése *(Barnas, 2016)*. A fizikai világ objektumainak (de ebben a kontextusban akár pl. intézkedés alá vont szubjektumainak) a forrástól való, szervezeteken átívelő eredetkövetése (*provenance*) és az „eszközkezelési" (*asset management*) tevékenység is olyan használati eset minták, melyek számos manifesztációval rendelkeznek a biztonsági kontextusban.

A „súrlódásmentes" szervezetközi kooperáció bevezetése szempontjából érdemes a közfeladatot ellátó biztonsági szervezetek egy olyan különleges tulajdonságát kiemelnünk, mely érdekes módon nagyban elősegítheti a blokkláncosítási stratégia kidolgozását. Ezen szervezetek feladatkörei, jogosítványai, tevékenységük korlátai és felügyelete erősen kodifikáltak (a jogforrási hierarchia számos szintjén). Ennek megfelelően a szervezet tevékenység-szerkezeti feltérképezése, mely a fokozatos blokkláncosítás előfeltétele, esetükben várhatóan kisebb kihívás, mint az üzleti életben.

Társadalmi transzparencia

A blokkláncok alapvetően újszerű lehetőségeket teremthetnek a biztonság területén működő szervezetek működési transzparenciájával kapcsolatban is. A nyílt hozzáférésű hálózatok főkönyvének változásait a széles publikum nyomon követheti. (Ez a folyamatos és nem korlátozott betekintési modell persze merőben más, mint a közérdekű adatigénylések ma is alkalmazott modellje; egyébiránt annak blokklánc alapú megvalósítása is hozhat önmagában hatékonyságnövekedést.) Így itt fel kell oldani azt az ellentmondást, hogy a biztonsági szervezetek belső működésének és egymás közötti együttműködésének számos érzékeny részlete rejtve kell, hogy maradjon az illetéktelen felek elől. Erre ma már számos, részben műszaki, részben kriptográfiai megközelítés ismert – lásd pl. *(ZKProof 2019)*.

A szerző ismeretei szerint a blokkláncok a szűkebben értelmezett biztonsági transzparencia szolgálatába állítása összességében még nyílt kérdésnek tekinthető. A *kormányzati transzparencia* támogatása azonban jó ideje aktívan és nyilvánosan vizsgált terület, melyről a WEF publikált áttekintő elemzést *(World Economic Forum 2020)*. A tágabban értelmezett biztonság szempontjából az elemzésben bemutatott transzparens blokklánc alapú kormányzati megoldások közvetlenül relevánsak: ilyen például vészhelyzetben az áruk és szolgáltatások gyorsított közbeszerzése.

Képességek

Ellenállóképesség és adatintegritás

Különösen a nagy, „értékes" kriptopénzek forgalmát könyvelő, publikus blokklánc hálózatokra igaz, hogy folyamatos támadási kísérleteknek vannak kitéve. Ennek köszönhetően kódbázisukban napjainkban már jellemzően csak csekély számú és korlátozott hatású szoftverhibára derül fény. A hálózatok által futtatott okosszerződésekre ez jóval kevésbé igaz, de köszönhetően néhány különösen nagy publicitást kapott, okosszerződésen keresztüli „kriptopénz-lopási" esetnek (lásd pl. az Ethereum hálózat feletti úgynevezett DAO-támadást *(Atzei–Bartoletti–Cimoli 2017)*), az ellenálló, bizonyítottan helyes okosszerződések fejlesztésének módszertanai különösen erősen fejlődnek. Hozzá kell azonban tennünk, hogy a konzorciális hálózatok blokklánc technológiái esetén kevésbé igaz, hogy folyamatos és különösen alapos biztonsági elemzésnek lennének kitéve (akár támadás, akár védelem céljából).

Ha azonban a közös módusú szoftverhibáktól eltekinthetünk, akkor a blokklánc hálózatok, mint elosztott adatbázisok jellemzően különösen ellenállóak más hibák hatásaival szemben (mint például egyes csomópontok meghibásodása, vagy éppen megsemmisülése). Hibák és támadások széles körével és aktivációs forgatókönyveivel szembeni ellenállóképességük abban mutatkozik meg,

hogy az elosztott főkönyv, mint adatbázis integritása ezek bekövetkezte esetén sem sérül, illetve a hálózat által megvalósított „adatbázis-szolgáltatás" ezek esetén sem esik ki.

Ennek megfelelően a blokkláncok alkalmazásának előnye és célja *önmagában* is lehet az, hogy egy erősen hiba- és támadástűrő köztesréteg (*middleware*) funkciót valósítsanak meg (kifejezetten katonai kontextusban lásd pl. *(Barnas 2016)*). A köztesréteg-jelleget itt az adja, hogy a blokkláncra, mint funkcionálisan a szokványoshoz erősen hasonlító *adattároló*, illetve *üzenetközvetítő* komponensre tekintünk, amely azonban különleges *extrafunkcionális* (pl. hibatűrés) tulajdonságokkal rendelkezik. A katonai alkalmazások mellett így ismert felvetés alkalmazásuk kritikus rendszerek (nem kemény valósidejű, azaz nem *hard real time*) felügyeletében és irányításában is, ahol ráadásul a teljes és letagadhatatlan visszakövethetőség további előnyként jelenik meg (pl. blokklánc alapú „fekete dobozok").

Letagadhatatlanság és visszakövethetőség

Az elosztott tárolás letagadhatatlansága és visszakövethetősége a kiber- és adatbiztonság területén várhatóan a blokkláncok egyik elsődleges értéke lesz *(Banerjee–Lee–Choo 2018)*. A blokklánc alapokra migrált SIEM (*Security Information and Event Management*; biztonsági információ és eseménykezelés) megoldások kizárják annak lehetőségét, hogy egy tárolt biztonsági esemény egy belső vagy külső támadó által utólagosan módosításra, vagy törlésre kerüljön. Emellett szükségszerűen a biztonsági események és információk egy teljes, letagadhatatlan és visszakövethető audit láncát (*audit trail*) is tartalmazzák. Kiberbiztonsági szempontból különösen izgalmas lehetőség, hogy a blokklánc segítségével egymással kapcsolatba hozott szervezetenkénti SIEM-ek megteremtik a kollaboratív és koordinált védekezés lehetőségét is (pl. a hálózati támadásokkal szemben védekezés szintjén), ez az aspektus azonban a szervezetközi kooperáció támogatásának kategóriájába illeszkedik inkább.

Anonimitás

A kriptográfia és különösen a ZKP-k területének újszerű eredményei segítségével nem csak a főkönyvi tranzakciók tartalma tehető értelmezhetetlenné egy blokklánc rendszer „széles nyilvánossága" számára, hanem maguk a tranzaktáló felek is „elrejthetőek".

Biztonsági szempontból a blokkláncok feletti anonimitás nyilvánvalóan kétélű fegyver. Egyrészről a ténylegesen anonim és nem visszakövethető kriptopénz-blokkláncok, mint pl. a ZCash és a Monero, bár szándékukban privacy fókuszúak, illegális tevékenységekhez kapcsolódó kriptopénz-cserére is alkalmasak. Másrészről azonban az ellenálló és az utólagosan módosításokat kizáró platform felett végzett titkos kommunikáció komoly nemzetbiztonsági alkalmazások lehetőségét is magában rejti (lásd pl. *(Jakobson 2019)*).

Összefoglaló

A blokkláncok és blokklánc alapú elosztott főkönyvi technológiák alkalmazásai messze túlmutatnak a kriptopénzeken, és az azokat könyvelő világméretű hálózatokon. A szervezetközi együttműködésben a blokkláncok tipikus alkalmazási esetei és alkalmazásuk okai ma már egyre inkább leírhatóak általánosított módon. Ennek ellenére az egyes szervezetek számára továbbra is komoly kihívást jelenthet, hogy milyen funkciók támogatására és hogyan vezessenek be működésükben blokklánc alapú megoldásokat.

Jelen cikk alapgondolata, hogy a kialakulóban lévő bevezetés-tervezési metodológiák, köztük a „blokkláncosítás" megközelítése, adaptálható a biztonság kontextusára is. Ehhez azonban szükséges a szisztematikus érvelést megalapozó hármas – az „üzleti" kulcsdimenziók, a blokklánc képességek és az értékteremtő funkciók figyelembe vett készletének – adaptálása. A cikk erre ad egy kezdeti javaslatot, példákkal alátámasztva.

Bár a diszciplínát útjára indító Bitcoin már több, mint 10 éves, a blokkláncok általános célú alkalmazása még új területnek tekinthető. A technológia is változóban van még; egyrészt várható a titkosítási megoldások további erősödése, másrészt az olyan, elosztott főkönyvet megvalósító, de műszakilag nem blokklánc alapú rendszerek megjelenése, melyek a kifejezetten *terepi* alkalmazást is célul tűzik ki. A blokkláncok jelenleg sokszor csekély áteresztőképessége is erőteljesen növekszik. Így ma még korai lenne véglegesnek tekinteni a biztonság szempontjából releváns alkalmazási mintákat és illeszkedésüket az egyes alterületekhez – mint az infrastruktúra-védelem, rendvédelem, honvédelem stb. – összehasonlító elemzés alá vetni; ez az elkövetkező évek kutatásainak feladata.

Irodalomjegyzék

Andoni, E. et al. (2019) Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, vol 100., pp 143–174. doi: 10.1016/j.rser.2018.10.014.

Androulaki, E. et al. (2018) Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, New York, NY, USA. pp. 30:1–30:15, doi: 10.1145/3190508.3190538.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017) A survey of attacks on Ethereum Smart Contracts (SoK). In: *Principles of Security and Trust*, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.

Banerjee, M., Lee, J. & Choo, K.-K. R. (2018) A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160. doi: 10.1016/j.dcan.2017.10.006.

Barnas, N. B. (2016) *Blockchains in national defense: Trustworthy systems in a trustless world*. Research report, Blue Horizons Fellows-

hip, USAF Center for Strategy and Technology. https://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf [Letöltve: 2020.08.20.]

Bodkhe, U. et al. (2020) Blockchain for industry 4.0: A comprehensive review. *IEEE Access*, vol. 8, pp. 79764–79800. doi: 10.1109/ACCESS.2020.2988579.

Christidis, K. & Devetsikiotis, M. (2016) Blockchains and smart contracts for the internet of things. *IEEE Access*, vol 4., pp. 2292–2303. doi: 10.1109/ACCESS.2016.2566339.

Jakobson, L. (2019). Defense Department turns to blockchain to secure communications. *Modern Consensus*, https://modernconsensus.com/technology/defense-department-turns-to-blockchain-to-secure-communications/ [Letöltve: 2020.08.20.]

Kuperberg, M., Kindler, D., Jeschke, S. (2019) *Are smart contracts and blockchains suitable for decentralized railway control?*, https://arxiv.org/abs/1901.06236 [Letöltve: 2020.08.20.]

Peck, M. E. (2017) Blockchain world – Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum*, vol. 54, no. 10, pp. 38–60, doi: 10.1109/MSPEC.2017.8048838.

Petersen, M., Hackius, M. & von See, B. (2018) Mapping the sea of opportunities: Blockchain in supply chain and logistics. *it – Information Technology*, vol. 60, no. 5–6, pp. 263–271. doi: 10.1515/itit-2017–0031.

Praveen, G., Chamola, V., Hassija, V. & Kumar, N. Blockchain for 5G: A prelude to future telecommunication. *IEEE Network*, Early Access, pp. 1–8. doi: 10.1109/MNET.001.2000005.

Rauchs, M., Glidden, A., Gordon, B. Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K. & Zhang, B. Z. (2018). Distributed ledger technology systems: A conceptual framework. SSRN Electronic Journal, DOI:10.2139/ssrn.3230013

Reyna, A. et al. (2018) On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, vol. 88, pp. 173–190. doi: 10.1016/j.future.2018.05.046.

Satoshi N. (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf [Letöltve: 2020.05.30.]

Shi, S. et al. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, vol. 97, p. 101966. doi: 10.1016/j.cose.2020.101966.

Subramanian, H. (2018) Decentralized blockchain-based electronic marketplaces. *Communications of the ACM*, Vol 61., No. 1.(2018) pp. 78-84.

ZKProof (2019) ZKProof Community Reference, Version 0.2. https://docs.zkproof.org/pages/reference/reference.pdf [Letöltve: 2020.05.30.]

Warren, S. & Treat, D. (2019) Building value with blockchain technology: How to evaluate blockchain's benefits. World Economic Forum. http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf [Letöltve: 2020.05.30.]

Wood, G. (2017) Ethereum: a secure decentralised generalised transaction ledger (EIP-150 revision). https://gavwood.com/paper.pdf [Letöltve: 2020.05.30.]

World Economic Forum (2020). *Exploring blockchain technology for government transparency: Blockchain-based public procurement to reduce corruption*. http://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf [Letöltve: 2020.08.20.]

Xie, J. et al. (2019) A Survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830. doi: 10.1109/COMST.2019.2899617.