GAZDASÁG ÉS PÉNZÜGY • 12. ÉVF. 3. SZ. • 2025. SZEPT. • DOI: 10.33926/GP.2025.3.3

A PÉNZÜGYI BLOKKLÁNCALKALMAZÁSOK EGY ÉVTIZEDE

Várakozások, gyakorlat és biztonság

Ambrus Éva[1]

ABSZTRAKT

A tanulmány kritikus szemszögből vizsgálja, javította-e a blokklánc-technológia a pénzügyi biztonságot 2014 és 2024 között, különös tekintettel az Európai Unió és Magyarország szabályozási és technológiai fejleményeire. A blokklánc alapvető jellemzői – a decentralizáció, a megváltoztathatatlanság és a kriptográfiai hitelesség – ösztönözték elterjedését olyan területeken, mint a határon átnyúló fizetések, az eszköztokenizáció, a decentralizált pénzügyek (DeFi) és a digitális identitásrendszerek. Ezek az alkalmazások rámutatnak a blokklánc képességére, hogy javítsa az auditálhatóságot, az átláthatóságot és a működési hatékonyságot, miközben mérsékli a centralizált rendszerek bizonyos sebezhetőségeit. A kutatás azonban megállapítja, hogy a blokklánc nem megszüntette, hanem átalakította a kockázatokat. Az új kihívások – például az okosszerződések sebezhetőségei, az orákulummanipuláció és a kulcskezelés kockázatai – a biztonsági felelősséget az intézményekről a protokolltervezésre és a felhasználókra helyezik át. Irodalmi áttekintés, szakpolitikai elemzés és esettanulmányok segítségével a cikk bemutatja, miként igyekszik az EU szabályozási kerete – például a MiCA, a digitális személyiadat-tárca és a DLT Pilot Regime – egyensúlyt teremteni az innováció, a rendszerbiztonság és a fogyasztóvédelem között. Magyarország óvatos, de egyre aktívabb részvétele betekintést nyújt egy kisebb EU-tagállam blokklánc-stratégiájába. Összességében a blokklánc nem a pénzügyi biztonság végső megoldásaként, hanem a bizalom, az irányítás és a felügyelet újragondolásának katalizátoraként jelenik meg a digitális pénzügyi környezetben.

JEL-kódok: G28, O33, K24

Kulcsszavak: blokklánc, pénzügyi biztonság, okosszerződések, szabályozás, Magyarország, MiCA, DeFi, digitális személyazonosság

1 *Ambrus Éva* Széchényi István Egyetem, PhD hallgató. E-mail: ambrus.eva.eszter@gmail.com.

1. BEVEZETÉS

Az elmúlt évtizedben a blokklánc-technológia, kiindulva a 2008-ban megjelent alapdokumentumban felvázolt elméleti koncepciótól, a kriptovalutákon túlmutató, széles körben alkalmazott technológiai vívmánnyá vált. Alapvető jellemzőinek köszönhetően – decentralizáció, megváltoztathatatlanság és kriptográfiai hitelesség –a blokklánc képes volt gyökeres átalakulást hozni a pénzügyi szektorban, ahol elsődleges a bizalom, az átláthatóság és a tranzakciók biztonsága.

E tanulmány központi kérdése a következő: javította-e a blokklánc-technológia a pénzügyi szektor biztonságát az elmúlt évtizedben? Ahogy sok más esetben, a válasz most sem egyértelmű: bár a megosztott főkönyvi technológia biztosítja az átláthatóságot, a megmásíthatatlanságot és javítja az auditálhatóságot, olyan újfajta kockázatokkal jár, mint az okosszerződésekben, az orákulumoktól való függésben és a kriptográfiai kulcskezelésben rejlő sebezhetőségek.

Tanulmányunk célja a pénzügyi területen alkalmazott blokkláncok biztonsági modelljét jellemző előnyök és korlátok együttes értékelése. A technológia elemzésével, szakpolitikai áttekintéssel, valamint az Európai Unióból és Magyarországról gyűjtött esettanulmányokkal járjuk körbe, hogy a blokklánc hogyan formálta át – ha meg nem is szüntette – a digitális pénzügyek terén jelentkező kockázatokat.

1.1. A blokklánc-technológia áttekintése

A blokklánc-technológia egyik alapvető újítása a digitális eszközök megosztott nyilvántartása és tulajdonlása. A központi szervek, például a bankok vagy pénzügyi szolgáltatók által irányított hagyományos rendszerektől eltérően itt a hálózat résztvevői – más néven csomópontok (node-ok) vagy validátorok – együttesen vezetik a blokklánc főkönyvét. Bár a „blokklánc" kifejezés eredetileg a bitcoinhoz kötődött, mára tágabb jelentést kapott: tulajdonképpen a megosztott főkönyvi technológia szinonimájává vált. Tanulmányunkban is ebben az általánosabb értelemben alkalmazzuk a széles körben használt és szemléletes „blokklánc" kifejezést.

A blokklánc-technológia a 2008-ban, Satoshi Nakamoto álnéven publikált Bitcoin-alapdokumentum megjelenésével kapott komolyabb figyelmet. Lényege egy blokkokból álló, folyamatosan növekvő láncolat, amelyben a blokkok időrendi sorrendben kapcsolódnak egymáshoz, és mindegyik blokk kriptográfiai hashkóddal hivatkozik az előzőre (Nakamoto, 2008). Az így képzett adatlánc megváltoztathatatlan és átlátható, eredménye pedig egy minden tranzakciót tartalmazó, ellenőrizhető és visszakövethető főkönyvi nyilvántartás. Elméleti síkon

a blokklánc egy olyan decentralizált tranzakciós adatbázisként írható le, amely konszenzuson alapuló, hitelesített interakciót tesz lehetővé akár nagy számú résztvevő között (Beck et al., 2018).

A blokkláncon alapuló rendszerek integritását, vagyis hitelességét kriptográfiai mechanizmusok biztosítják. A lánc minden blokkja tartalmazza az előző blokk hashét, azaz a lánc visszamenőleges módosítása észszerűtlenül nagy számítási teljesítményt igényel. A Bitcoin ezt például a SHA-256 hashalgoritmussal biztosítja, míg az olyan platformok, mint a Solana és a Tezos más kriptográfiai szabványokat alkalmaznak (IansitiLakhani, 2017). Bármely korábbi blokk módosítása esetén minden utána következő hasht újra kellene számítani, ami a jelenlegi számítástechnikai ismereteink szerint lehetetlen.

A konszenzusmechanizmusok kulcsfontosságú szerepet játszanak a tranzakciók hitelességének és a főkönyv általános minőségének meghatározásában. A Bitcoin Proof-of-Work (PoW) alapú rendszerében a bányászok egymással versengve oldanak meg bonyolult kriptográfiai feladványokat a lánc továbbfűzéséért. Más rendszerek az energiahatékonyabb Proof-of-Stake (PoS) modellben működnek. Többek között az Ethereum is a PoS-alapú konszenzusra állt át 2022-es átfogó protokollátalakításakor (Houben– Snyers, 2018). A blokkláncon alapuló rendszerekben egy tranzakció akkor válik véglegessé, ha azt a hálózat résztvevőinek többsége hitelesíti a blokkok sorba rendezésének belső logikája és (PoW-konszenzusnál) a kumulált nehézség vagy (PoS-konszenzusnál) a zárolt kriptovaluta-mennyiség (stake) relatív súlya alapján.

A blokkláncrendszerekben elágazás keletkezhet, ha egy időben két hitelesített blokkot hoznak létre, így átmenetileg a főkönyvnek két eltérő verziója létezik. Ezeket az ütközéseket a rendszer úgy oldja meg, hogy a hosszabb vagy a számítástechnikailag bonyolultabb láncot viszi tovább. Az elvetett láncverzió, amelyet „árva láncnak" is neveznek, a rendszer nyilvántartásában megmarad, de további kiegészítéseibe nem kerül bele.

A hálózati dinamikát emellett a nehézségi fok adaptív korrekciója szabályozza. A Bitcoin esetében például a bányászás nehézségét 2016 blokkonként, körülbelül kéthetente újrakalibrálják, hogy a rendszerben stabilan körülbelül tízperces időközzel jöjjön létre új blokk.

A blokklánc technológiai fejlődésével új alkalmazási területek nyíltak meg. Ilyenek többek között a decentralizált pénzügy vagy DeFi, ahol okosszerződésekkel automatizálhatók a pénzügyi műveletek; a fizikai és digitális javak tokenizációja; az önrendelkező identitáskezelésre (self-sovereign identity, SSI) támaszkodó digitális identitásrendszerek; az Európai Unió digitális euro kezdeményezéséhez hasonló központi banki digitális fizetőeszközök (CBDC-k); valamint az olyan adat-

védelmi mechanizmusok, mint a nem feltáró bizonyítás (zero-knowledge proof), amellyel az információk felfedése nélkül ellenőrizhetők a rájuk vonatkozó adatok.

Fontos hangsúlyozni, hogy a blokklánc-kialakítás önmagában nem garantálja a biztonságot. A rendszert jellemző sebezhetőségek között említhető az okosszerződések végrehajtási folyamata, az orákulummanipuláció, a hozzáférés ellenőrzésének hiányosságai, valamint a felhasználói hibák. Ráadásul a most formálódó szabályozási keretrendszer, amelyből kiemelendő az Európai Unió kriptoeszközök piacairól szóló rendelete (MiCA) és általános adatvédelmi rendelete (GDPR), jelentős megfelelőségi és irányítási kihívások elé állítja a decentralizált infrastruktúrákat.

Összefoglalva, a blokklánc gyökeres változást jelent a digitális tranzakciókról, az eszközkezelésről és az adatok sértetlenségének biztosításáról alkotott fogalmak és gyakorlati megoldások terén. Ugyanakkor sikeres alkalmazásához fokozott figyelmet kell fordítani a megfelelő technológiai és a megbízható kriptográfiai kialakításra, valamint a szabályozásnak való megfelelésre, ami a pénzügyi szektorban különösen érvényes.

1.2. A blokklánc 2014 utáni térnyerése a pénzügyi szolgáltatási szektorban

Az elmúlt tíz év során a blokklánc biztonságosságára irányuló kutatások fókusza a protokollszintű kriptográfiai biztosítékokról olyan átfogóbb problémákra irányult, mint az irányítás, a jogszabályi megfelelőség és a rendszerszintű kockázatok. Atzei, Bartoletti és Cimoli (2017) korai alapmunkájukban gyűjtötték össze az Ethereum platform okosszerződéseiben leggyakrabban előforduló sebezhetőségeket, köztük a logikai hibákat, a bemeneti adatok ellenőrzés nélküli hitelesítését és az újrabelépéses támadásokat. E problémák rámutattak, hogy a megváltoztathatatlanság önmagában nem garantálja a biztonságot, és világossá vált, hogy szigorú auditgyakorlatokra és módszeres ellenőrzésre van szükség.

Ezzel egy időben az európai jogtudományban előtérbe került a blokklánc megváltoztathatatlansága és a kialakuló adatvédelmi normák közötti ellentét. Finck (2019) az általános adatvédelmi rendeletben rögzített „elfeledtetéshez való jog" és a blokkláncok főkönyvének visszafordíthatatlan jellege közötti alapvető ellentmondást vizsgálta. Munkájában – amely hozzájárul a szakpolitikai párbeszédhez és az olyan gyakorlati átültetésre irányuló kezdeményezésekhez is, mint az ONTOCHAIN – a személyes adatok védelmét előtérbe helyező módszerekben, például a blokkláncon kívüli adattárolásban és a nem feltáró bizonyításban látja a lehetséges megoldást.

Li et al., (2020) a programszintű biztonságon túlmutató, átfogóbb elemzésben tárgyalták a blokkláncrendszerek támadási felületét. Kutatásukban összesítették

a különböző konszenzusmechanizmusok, hálózati protokollok és a felhasználóoldali alkalmazások sebezhetőségeit, megállapítva, hogy a biztonságos kriptográfiai kialakításnak ökoszisztéma-szintű, holisztikus kockázati modellel kell kiegészülnie. A szerzők felhívják a figyelmet, hogy bár a blokkláncrendszerek alaparchitektúrája biztonságos, több védelmi réteg hiányában a felhasználók kockázati dominóhatásoknak vannak kitéve.

Zetzsche et al., (2020) azt vizsgálták, hogyan találkozik a szabályozás és az innováció, és hogyan kérdőjelezi meg a DeFi a jelenlegi szabályozási kereteket. Munkájukban kiemelik, hogy az okosszerződés-alapú, például hitelezési, eszközkezelési és elszámolási szolgáltatások, jelentős kihívás elé állítják a szabályozókat, és a DeFi irányítását a funkcionális ekvivalencia alapelve mentén érdemes megszervezni. Álláspontjuk visszaköszön a kriptoeszközök piacairól szóló uniós rendeletet (MiCA) övező tárgyalásokban is.

Az ellenőrzés problémájához kapcsolódóan Zhang és Lee (2021) kidolgozták az okosszerződések auditmódszertani taxonómiáját. Az auditeszközöket statikus, dinamikus és hibrid kategóriákba soroló tanulmányukban felvázolják a szerződések biztonságát garantáló legjobb gyakorlatokat, és javasolják, hogy a most kibontakozó szabályozási rendszer, így a MiCA 2.0, tegye kötelezővé a módszeres auditot a magas kockázatú protokollok esetében.

A nemzetközi szakpolitikai elemzések is megerősítik a blokklánc összehangolt szabályozásának hiányát. A Cambridge Centre for Alternative Finance 2022-ben megjelent Global Cryptoasset Benchmarking Study [Globális kriptoeszköz-összehasonlító tanulmány] kiadványa rámutat, hogy az uniós tagországok elköteleződése és szabályozási készültsége terén is jelentősek a különbségek. E különbségek még inkább indokolttá teszik az olyan jogharmonizációs kezdeményezéseket, mint az európai blokklánc-szolgáltatási infrastruktúra (European Blockchain Services Infrastructure, EBSI), amelynek célja az irányítás és a kiberbiztonság joghatóságokon átívelő egységességének biztosítása.

Az MIT digitális pénzek kezdeményezése [Digital Currency Initiative] keretében publikált új tanulmány (Lovejoy et al., 2023) a skálázhatóság és a biztonság közötti kompromisszumot vizsgálja a rendszerarchitektúra szintjén. Ez az elosztott konszenzust és küszöbkriptográfiát tárgyaló munka alapul szolgál az olyan biztonságos, nagy teljesítményű rendszerek létrehozásához, amelyek különösen az Európai Központi Bank digitális eurójához hasonló CBCD-kezdeményezésekhez szükségesek.

2014 óta a blokklánc a kriptovalutákhoz kötődő résterületi technológiából alapvető pénzügyi szolgáltatási infrastruktúrává nőtte ki magát. Kezdetben elsősorban a bitcoinos nemzetközi fizetési tranzakcióknál alkalmazták, majd az első generáci-

ós blokkláncok korlátai nyomán létrejöttek az olyan platformok, mint Ethereum, amelyen újításként megjelent a programozhatóság és az okosszerződések.

E fejlemények az intézményi szereplők érdeklődését is felkeltették. Jelentős pénzügyi szereplők, köztük a JPMorgan, a Goldman Sachs és a Santander, elindították kísérleti blokkláncprojektjeiket, illetve csatlakoztak olyan, az elosztott főkönyvi technológia hagyományos pénzügyekben való alkalmazhatóságát feltérképező konzorciumokhoz, mint az R3 és a Hyperledger. Ezzel egy időben a fintech vállalatok a blokklánc előnyeit szélesebb rétegek számára elérhető, hatékony és átlátható pénzügyi termékek kialakításához használták fel, ami lendületet adott a valós idejű elszámolás, az eszköztokenizáció és a digitális eszközök letéti őrzése fejlődésének is.

A kormányok és szabályozó hatóságok erre reagálva infrastrukturális és kutatási kezdeményezéseket indítottak. Az Európai Unió támogatásával útjára indult az EBSI-projekt, a központi bankok, köztük az EKB és a Banque de France pedig a CBCD-k életképességét felmérő kísérletekbe kezdtek. E kezdeményezésekben is visszatükröződik az egyre szélesebb körű egyetértés arról, hogy a blokklánc javíthatja a globális pénzügyi rendszerek átláthatóságát, kölcsönös átjárhatóságát (interoperabilitását) és ellenálló képességét (rezilienciáját).

A 2020-as évek elejére a DeFi, a CBCD-k és az eszköztokenizáció párhuzamos fejlődésével a blokklánc az új generációs pénzügyek kulcskomponensévé lépett elő. Bár a különböző joghatóságokban még mindig eltérő mértékben alkalmazzák, a technológiai beérése, a szabályozás fejlődése és a piaci kísérletezési hajlandóság együtt megszilárdították a blokklánc helyét a digitális pénzügyi infrastruktúrában.

Ahogy Shukla et al., (2024) összegzi, a blokklánc átalakította a pénzügyi műveleteket, a tőkeképzéstől a határokon átnyúló tranzakciókon át az adatok sértetlenségének rendszerszintű védelméig. A megjelenő újítások közül kiemelendő az elsődleges tokenkibocsátás (Initial Coin Offering, ICO), amellyel az induló vállalkozások saját kriptopénz kibocsátásával juthatnak tőkéhez, megkerülve a hagyományos pénzügyi közvetítőket (Chen–Bellavitis, 2020; Nakamoto, 2008, Tapscott–Tapscott, 2016). A blokkláncon alapuló fizetési rendszerek, amelyekhez nincs szükség központi elszámoló intézményre, gyorsabbak és hozzáférhetőbbek (Chen–Bellavitis, 2020, Sharma et al., 2022). A blokklánc alkalmazásával növelhető az átláthatóság, a működési hatékonyság és a kibertámadásokkal szembeni reziliencia a banki és a kapcsolódó szektorokban (Tian, 2017, Warkentin–Orgeron, 2020). Alaparchitektúrája, melynek lényegi jellemzői a decentralizáció, a megváltoztathatatlanság és a kriptográfiai biztosítékok, megbízható védelmet nyújt a digitális eszközök és tranzakciók számára (Hajian et al., 2023, Tanwar et al., 2020, Yue et al., 2016).

1.3. Kutatási kérdés: Javította-e a blokklánc-technológia a pénzügyi szektor biztonságát az elmúlt évtizedben?

E tanulmány a következő központi kérdést teszi fel: Javította-e a blokklánc-technológia a pénzügyi szektor biztonságát az elmúlt évtizedben? A válasz nem egyértelmű, a kérdést csak a tágabb összefüggéseket megvizsgálva, árnyaltabban válaszolhatjuk meg. Míg a blokkláncalapú rendszereket szerkezeti jellemzőik – megváltoztathatatlanság, kriptográfiai hitelesség és decentralizált konszenzus – egyfelől biztonságossá teszik, gyakorlati alkalmazásuk újfajta kockázatokkal és működésbeli kompromisszumokkal jár.

Elmondható, hogy a blokklánc a hagyományos pénzügyi infrastruktúrák számos, régóta problémát jelentő sebezhetőségét kezelte. Ilyenek a határokon átnyúló tranzakciókkal kapcsolatos csalások, a központilag vezetett nyilvántartások átláthatatlansága és a korlátozott ellenőrizhetőség. Az elosztott főkönyv adatstruktúrája ezzel szemben átlátható, minden módosítása nyilvánvaló, elősegítve a tranzakciók nyomon követését és a szabályozói felügyeletet. Emellett az olyan újítások, mint az előre programozott megfelelés (okosszerződések segítségével) utat nyithatnak az automatikus szabályérvényesítés és a szabályozásnak való megfelelés javítása felé is.

Másfelől viszont a blokkláncok alkalmazásával új biztonsági kihívások jelentek meg. A mostanra a DeFi-re és az eszköztokenizációra épülő ökoszisztémák szerves részét képező okosszerződések visszatérő sebezhetőségeinek bizonyultak a programozási hibák, az elégtelen hivatalos ellenőrzés és a téves gazdasági logika. Az orákulumoktól, azaz a külső adatforrásoktól való függés az okosszerződések végrehajtása során további támadási felületet és hibalehetőségeket kínál. Ezenfelül a decentralizált kulcskezeléssel átkerül a felelősség a végfelhasználókhoz, ami a hozzáférhetőséggel, a károk megtérítésével és a letéti őrzés megbízhatóságával kapcsolatban vet fel kérdéseket.

1.4. Módszertan és tárgy: technológiai fejlődés, alkalmazási példák és biztonsági következmények

A tanulmányban a kvalitatív irodalmi áttekintés módszertanát alkalmazzuk, összegezve a 2014 és 2024 között publikált, lektorált szakirodalom, intézményi alapdokumentumok és dokumentált ágazati esettanulmányok megállapításait. Áttekintésünk három vizsgálati terület köré szerveződik: 1. a blokklánc-infrastruktúra technológiai fejlődése; 2. ágazat-specifikus pénzügyi alkalmazási területek; 3. megfigyelt biztonsági következmények. Különös figyelmet kap a techno-

lógia alkalmazása az Európai Unión belül, amely vezető és proaktív szabályozói szerepet tölt be e területen.

A tanulmány első része a blokklánc-infrastruktúra fejlődését vizsgálja. Ezen belül kitérünk a Proof-of-Work (PoW) modellről a Proof-of-Stake (PoS) modellre történő átállásra, a Layer 2 skálázási megoldások megjelenésére és az olyan személyes adatvédelmi mechanizmusok fejlődésére, mint a nem feltáró bizonyítás. E fejleményeket a tranzakciók, a hálózat és az adatok biztonsága tekintetében értékeljük.

A második rész a blokklánc bevett vagy kísérleti szakaszban lévő pénzügyi alkalmazásait vizsgálja. Ilyenek a határon átnyúló fizetések, a decentralizált hitelezési protokollok, az eszköztokenizációs platformok és a személyazonosság-ellenőrző rendszerek. Hogy kiegyensúlyozottabb képet kapjunk, DeFi ökoszisztémákból és hagyományos pénzügyi intézményektől származó esettanulmányokat is gyűjtöttünk.

Végül a már ismert biztonsági következményeket értékeljük. Fő kérdéseink a következők: Kimutathatóan visszaszorította a blokklánc a pénzügyi tranzakciókkal kapcsolatos csalásokat és visszaéléseket? Javította-e az átláthatóságot, auditálhatóságot és a szabályozásnak való megfelelést? Az ismert gyenge pontokat – például az okosszerződések vagy orákulumok kapcsán – sikerült-e az architektúra, vagy az eljárások szintjén bevezetett újításokkal kezelni?

2. A BLOKKLÁNC-TECHNOLÓGIA FEJLŐDÉSE (2014–2024)

A blokklánc-technológia a decentralizált digitális fizetőeszköz, a bitcoin 2009-es megjelenésével került be a köztudatba. 2014-re a bitcoinon és más hasonló kriptovalutákon keresztül már világméretű figyelem irányult az egyenrangú felek által vezetett, kriptográfiai eszközökkel biztosított digitális főkönyvben rejlő lehetőségekre. Az első generációs blokkláncok legfőbb erényei az átláthatóság, a közvetítők kiiktatása és a cenzúramentesség voltak. Ugyanakkor csak egyszerű parancsok voltak rajtuk futtathatók, és elsősorban pénzmozgások végrehajtására voltak használhatók.

2015-ben gyökeres változást hozott az új Ethereum platform indulása és vele az okosszerződések, azaz a blokkláncban rögzített, önfuttató programok megjelenése. Ezzel az architekturális újdonsággal megjelenhettek a decentralizált alkalmazások (dAppok), és új korszak kezdődött a blokkláncforradalomban. Az okosszerződések lehetővé tették a programozott pénzügyi eszközök, a szabályozási követelményeknek való automatikus megfelelés és a digitális eszközök közötti komplex interakciók létrejöttét, megteremtve az évtized végére kialakuló DeFi ökoszisztéma alapjait (Tapscott–Tapscott, 2016, Yermack, 2017).

Az Európai Unióban tágabb körben, a kriptovalutákon túl a közigazgatás, a határokon átnyúló digitális szolgáltatások és a szabályozott pénzügyi piacok területén is elkezdték vizsgálni a blokklánc-technológia alkalmazhatóságát. Az Európai Bizottság és az EU Blockchain Observatory and Forum (Uniós Blokklánc Megfigyelőközpont és Fórum,2022) is rámutatott, hogy a blokklánccal javítható az átláthatóság, csökkenthetők az adminisztratív terhek és előmozdítható a digitális szuverenitás. Bár Magyarország nem volt a blokklánc-technológiát elsőként alkalmazó országok között, egyre jobban bevonódott a területen zajló fejlesztésekbe a hazai fintech szektor és tudományos kutatóhálózatok révén. A technológia elsőként kriptovaluta-kereskedelmi platformok és személyazonosság-ellenőrző kísérleti projektek formájában jelent meg az országban. A Magyar Nemzeti Bank (MNB) jelentése szerint Magyarország ma több mint 200 fintech vállalat működését támogatja, amelyek közül számos megosztott főkönyvi technológiára alapuló szabályozási technológiával (RegTech), automatikus ügyfél-átvilágítási (know-your-customer, KYC) rendszerekkel, valamint pénzmosás elleni (AML) keretrendszerekkel foglalkozik (MNB, 2023).

A 2010-es évek végére kibővült a blokkláncot övező diskurzus. A technológiát egyre többen fogadták el alapvető digitális infrastrukturális elemként, amely számos különféle területen alkalmazható, beleértve a logisztikát, az energetikai rendszereket, az oktatást és a digitális személyazonosság-kezelést. Olyan, egész Európai Uniót lefedő programok, mint az európai blokklánc-szolgáltatási infrastruktúra jelezték, hogy az intézmények is készek továbblépni a technológia kísérleti alkalmazásától annak módszeres integrációjáig. A Horizon 2020 és a Horizon Europe programok keretében szabályozói tesztkörnyezetek (regulatory sandbox), közszféra-beli konzorciumok és kutatási pályázatok jöttek létre a technológia biztonságos és skálázható gyakorlati alkalmazásának felgyorsítása érdekében (Európai Bizottság, 2023). A magyar intézmények, köztük egyetemek és kkv-k, egyre aktívabban vettek részt e kezdeményezésekben, és jelentős eredményeket értek el az identitáskezelési keretrendszerek és az okosszerződések megfelelését biztosító eszközök fejlesztése terén.

Ezzel párhuzamosan a technológia vállalati alkalmazása is felgyorsult. Európaszerte kezdetét vette a pénzügyi intézmények körében az olyan engedélyköteles blokkláncplatformok tesztelése és bevezetése, mint a Hyperledger Fabric és a R3 Corda, amelyek fokozottan biztonságos, szabályozott környezetet biztosító architektúrák. E platformok hozzájárultak a kereskedelemfinanszírozás, a bankközi elszámolás és a megfelelési jelentések digitalizálásához (EU Blockchain Observatory and Forum, 2022). Az intézményi átvételben a központi bankok is jelentős szerepet játszottak. Az Európai Központi Bank, a Banque de France és a Sveriges Riksbank is kísérleti projektet indított a központi banki digitális fizetőeszközök tesztelésére, melyek közül a digitális euro projekt 2021-re komolyabb

politikai és technikai hátszelet kapott (Európai Központi Bank, 2023). Hazai viszonylatban az MNB egyeztetéseket és kutatásokat kezdeményezett a digitális fizetőeszközök monetáris politikai, pénzügyi stabilitási és fizetési innovációs vetületeinek feltérképezésére (Magyar Nemzeti Bank, 2023).

A magánszektor szereplői, köztük bankok, biztosítók és tőzsdék, szintén elindultak a blokklánc-integráció útján. Különféle pénzügyi szervezetek kezdtek ismerkedni az eszköztokenizáció, a blokkláncalapú elszámolási rétegek és a valós idejű kötelező jelentéstétel lehetőségeivel. Ezt a folyamatot gyakran a magán- és közszektor szereplői közötti együttműködések és európai innovációs programok is támogatták. A magyarországi fintech vállalatok, köztük több budapesti székhelyű cég, aktívan hozzájárultak a blokkláncalapú megoldások fejlesztéséhez olyan alkalmazási területeken, mint a pénzmosás elleni szabályoknak való megfelelés, a letéti őrzés biztonságossága és a digitális pénztárcák tervezése.

Az egyre nagyobb teljesítményigény miatt 2020-tól felgyorsult a blokklánc technológiai fejlődése. Az első generációs blokkláncok skálázhatósági és költséghatékonysági problémákba ütköztek, életre hívva a fő blokkláncra épülő Layer 2 skálázási megoldásokat. Ide tartoznak az olyan fizetési csatornák, mint a Lightning Network a Bitcoin platformon, valamint az Ethereum „göngyölítéses" (rollup) mechanizmusai (pl. ZK-rollup, optimista rollup), amelyeknél a tranzakciókat a fő láncon kívül hajtják végre, majd a végrehajtás hitelesített eredményét tömörített formában rögzítik a fő láncon, így növelve a hálózat áteresztőképességét (Gray, 2025; Bakkt, 2022). Ezekkel a technológiákkal létrejöhettek olyan kifinomultabb, nagy sebességű pénzügyi alkalmazások, amelyekben változatlanul érvényesül a decentralizáció alapelve.

Lényeges szemponttá vált az interoperabilitás. A láncok közötti kommunikációs hátteret biztosító Polkadot, Cosmos és más hasonló protokollok lehetővé tették a különböző láncok közötti zökkenőmentes adat- és eszközcserét. A láncon kívüli információkhoz való hozzáférést megkönnyítő, Chainlinkhez hasonló orákulumhálózatok megjelenésével pedig megnyílt az út az összetett DeFi termékek és a valós eszközök (tokenizált fizikai vagy hagyományos eszközök) kifejlesztése előtt (Khan, 2025; Bakkt, 2022). E fejlemények nyomán a blokklánc közelebb került ahhoz, hogy a globális pénzügyi infrastruktúra alapkövévé válhasson.

Válaszul e változásokra az európai szabályozók új keretrendszereket hoztak létre, hogy az innovációt a jogi megfelelőség medrében tartva ösztönözzék. A Digitális Európa Program forrásaiból 2023-ban létrejött a blokkláncon alapuló megoldások szabályozó felügyelet alatti tesztelését lehetővé tevő Európai Blokklánc-szabályozói Tesztkörnyezet. A többek között a Bird & Bird ügyvédi iroda koordinálásával megvalósuló kezdeményezésben magyar szereplők, valamint hazai szabályozó szervek és innovatív pénzügyi szereplők is részt vettek (Európai Bizottság, 2023, StandICT, 2023, BlockStand, 2025).

Magyarország szerepvállalása folyamatosan változott ezen az ökoszisztémán belül. Számos magyar egyetemen indultak kifejezetten a blokklánccal foglalkozó kurzusok, míg az állami szervek, köztük a Nemzeti Adó- és Vámhivatal a csalásmegelőzés és a pénzügyi felügyelet területén kezdték vizsgálni a megosztott főkönyvi technológia alkalmazásának lehetőségeit. E fejleményekből is látható Magyarország megfontolt, de egyre aktívabb részvétele a tágabb európai blokklánckutatási és -megvalósítási törekvésekben (MNB, 2023).

A fent bemutatott technológiai, intézményi és szabályozói előrehaladás mentén kirajzolódik, hogyan vált a blokklánc kísérleti elgondolásból a modern pénzügyi rendszer infrastruktúrájának szerves részévé.

3. A BLOKKLÁNC ALKALMAZÁSI TERÜLETEI A PÉNZÜGYI SZEKTORBAN: A FIZETÉSI TRANZAKCIÓKTÓL A PROGRAMOZHATÓSÁGIG

Az elmúlt évtizedben a blokklánc-technológiát a pénzügyi szolgáltatások széles spektrumán alkalmazták: kezdeti, újszerű elszámolási rétegből a programozott pénzügyi architektúra alappillérévé fejlődött. Felhasználási esetei meglehetősen sokrétűek, a határokon átnyúló fizetésektől, az értékpapír-tokenizáción és a személyazonosság-ellenőrzésen át a decentralizált pénzügyig, területenként eltérő mértékű intézményi szerepvállalással, szabályozói felügyelettel és rendszerszintű kockázatokkal. Ez a fejezet összefoglalja az e területeken bekövetkezett kulcsfontosságú fejleményeket, különös tekintettel az Európai Unió szabályozói álláspontjára és Magyarország lépéseire a technológia integrációja felé.

Határokon átnyúló fizetési tranzakciók és elszámolási infrastruktúra

A blokklánc legkorábbi és vitathatatlanul legkiforrottabb pénzügyi alkalmazása a határokon átnyúló fizetések területe. A közvetítők kiiktatásával és a megosztott konszenzus kiaknázásával a blokkláncprotokollok gyorsabb, átláthatóbb és alacsonyabb költségű elszámolási útvonalakat nyitottak meg. Az olyan platformokon, mint a Ripple és a Stellar, a tranzakciók valós időben hajthatók végre, csökkentve a késedelmet és garantálva a globális átutalások szinte azonnali véglegességét (Shei et al., 2025, Bakkt, 2022, Rapid Innovation, 2024). A stablecoinok, különösen az USDC és az USDT elterjedése tovább bővítette ezt az ökoszisztémát, lehetővé téve az árstabil digitális tranzakciókat a blokkláncházatokon, ami a pénzátutalások és mikrofizetések szempontjából is egyértelműen előnyös (EKB, 2025).

Az Európai Unióban a közszférában és a magánszektorban egyaránt vizsgálják a blokkláncon alapuló fizetési innovációkat. Az EKB egy átfogó blokkláncalapú

elszámolási réteg fejlesztésébe kezdett a digitális euro technikai előfutáraként, amelynek célja a pénzügyi intézmények közötti együttműködési képesség és a működési hatékonyság javítása (CryptoSlate, 2025, CoinSpeaker, 2025). Magyarországon a Magyar Nemzeti Bank is végzett kutatásokat a megosztott elszámolási mechanizmusok és az integrált főkönyvi rendszerek hazai fizetési tranzakciókban való alkalmazására (MNB, 2023). Nemzeti viszonylatban a magyar fintech vállalatok aktívan kísérleteznek a Bitcoin Lightning Network-jét és stablecoinos fizetési pályákat használó mobiltárca-alkalmazásokkal és határokon átnyúló átutalási eszközökkel, ami azt tükrözi, hogy az óvatos szabályozói hozzáállással párhuzamosan a technológia alulról szerveződve egyre inkább teret nyer.

Ennek ellenére szélesebb körű intézményi bevezetése több tartós akadályba ütközik, beleértve a megfelelési szabványok széttagoltságát, a hagyományos rendszerekkel való korlátozott interoperabilitást, valamint a stablecoinok MiCA-rendelet szerinti kezelését övező bizonytalanságot. A PSD2 irányelv ad némi szabályozási támpontot, de a kizárólag a blokkláncból származtatott (natív) pénzügyi instrumentumok szabályozásba ágyazása még folyamatban van.

Értékpapír-tokenizáció és piaci infrastruktúra

A blokklánc másik fontos alkalmazási területe a valós eszközök tokenizálása, azaz digitális tokenné alakítása. A tokenizációval a hagyományosan nem likvid vagy nagy értékű eszközök, például ingatlanok, kötvények vagy művészeti alkotások feldarabolhatók, és blokkláncalapú digitális tokenek formájában reprezentálhatók. Ez az újítás fokozhatja a piaci likviditást, és csökkentheti az átfutási időt, valamint a kibocsátási és letéti őrzési költségeket (DLA Piper, 2022; KPMG Germany, 2025). Intézményi környezetben a tokenizáció javíthatja az átláthatóságot és az auditálhatóságot, különösen a magánpiacok és az összetett származtatott termékek tekintetében.

Az eszköztokenizáció Európai Unió-szerte jelentős figyelmet kapott a tőkepiaci intézményektől. Az Európai Beruházási Bank (EBB), a Deutsche Börse és a francia pénzügyi szabályozó hatóságok blokkláncon alapuló kibocsátási és kereskedési folyamatokat teszteltek. E lépésekhez jelentős támogatást biztosít az EU által 2023-ban elindított, megosztott főkönyvi technológián alapuló piaci infrastruktúrák kísérleti rendszere (DLT Pilot Regime), amely biztonságos környezetet teremt a DLT-alapú kereskedési és kiegyenlítési platformok teszteléséhez (Európai Parlament és a Tanács, 2022; ESMA, 2023). A francia, német és olasz nemzeti szabályozó hatóságok a keretrendszer kibővítését szorgalmazták, hogy az többféle eszközcsoportra kiterjedjen és az intézményi szereplők számára is egyszerűbben hozzáférhető legyen (Ledger Insights, 2025).

Bár még csak felderítő jelleggel, de Magyarország is aktívan vizsgálja ezt az alkalmazási területet. A Budapesti Értéktőzsde érdeklődést mutat a DLT integrálása

iránt a kereskedés utáni munkafolyamatokba, hazai fintech cégek pedig a kkv-kat és az ingatlanpiacot megcélzó tokenizációs platformokat indítottak (Global Legal Insights, 2023). A tudományos életben is megjelentek kutatási témaként a blokkláncon alapuló részvényesi irányítási és szavazási mechanizmusok, kiemelve a tokenalapú jogok és a társasági jog közötti összefüggéseket. Bár a másodlagos piaci likviditás és a jogi érvényesíthetőség továbbra is megoldatlan problémát jelent, a szervezett európai kísérleti környezet elősegíti a tokenalapú pénzügyek óvatos tempójú, de folyamatos fejlődését.

Személyazonosság-ellenőrzés és szabályozási megfelelés

A blokklánc potenciális megoldást jelenthet a digitális személyazonosság és az ügyfél-átvilágítási (KYC) követelményeknek való megfelelés terén is, ahol régóta problémát jelent a hatékonytalanság, az adatsilók és az adatvédelmi kockázatok. Az önrendelkező identitáskezelés (SSI) lehetővé teszi, hogy az egyének kriptográfiai eszközök felhasználásával maguk rendelkezhessenek a személyes adataikkal, kiiktatva a felesleges azonosítási folyamatokat és elősegítve a felhasznált adatmennyiség minimalizálását (Togggle, 2024, Gataca, 2022). Ezt egészítik ki az olyan blokkláncalapú KYC-keretrendszerek, amelyekkel az ellenőrzött azonosító jellemzők biztonságosan oszthatók meg a pénzügyi intézmények közötti kommunikációban, így nyers személyes adatok felfedése nélkül tehetnek eleget együttműködési kötelezettségüknek.

Az Európai Unió élen jár a blokkláncalapú személyazonosság-kezelési innovációban. Az uniós tagállami együttműködés keretében 2018-ban útjára indított EBSI célja a határokon átnyúló digitális azonosításiadat-hitelesítés támogatása és az SSI bevezetése a különböző közszolgáltatásokba (Európai Bizottság és Európai Blokklánc-partnerség, 2018; Capacities, 2023). Az átdolgozott eIDAS 2.0 rendeletbe foglalt uniós digitális személyiadat-tárcát az egyének a GDPR követelményeinek is megfelelő, egységes interfészként használhatják digitális azonosító adataik kezeléséhez, illetve a magán- és közszektorbeli KYC/AML-követelmények teljesítéséhez (Biometric Update, 2024; Európai Bizottság, 2025).

E kezdeményezéseket Magyarország is tevékenyen támogatja. Hazai egyetemeken és kutatási intézményekben zajlanak az EBSI-hez kapcsolódó, gyakorlati alkalmazási lehetőségeket vizsgáló projektek, többek között a felsőoktatási azonosító adatok ellenőrzése és az új hallgatók beléptetése terén. Az MNB és belföldi innovációs csomópontok figyelmét is felkeltették a pénzügyi számlanyitást leegyszerűsítő és a csalások megelőzésére is felhasználható blokkláncalapú személyazonosság-kezelő rendszerek (NM Innováció, 2022; Global Government FinTech, 2023). Bár a technológia alkalmazása még korai szakaszban jár, a magyarországi tágabb digitális pénzügyi ökoszisztémán belül mostanra kiépült a személyazo-

nosság-kezeléshez használt, blokkláncon alapuló rendszerek befogadására alkalmas technológiai és jogi infrastruktúra.

Decentralizált pénzügy: innováció és volatilitás

A blokkláncalapú pénzügyi szolgáltatások talán legforradalmibb formája a decentralizált pénzügy, azaz a központi közvetítők nélkül működő protokollok ökoszisztémája. Az Aava, az Uniswap és a Compund platformokon például a felhasználók nyilvános blokkláncon futó okosszerződéseken keresztül hitelezhetnek vagy vehetnek fel kölcsönt, illetve adhatnak el, vásárolhatnak vagy stakelhetnek (kriptoeszközök zárolása jutalomért cserébe) eszközöket. Ezekben a nem engedélyköteles, széles körben hozzáférhető rendszerekben algoritmusok biztosítják a pénzügyi szabályok érvényesítését. Ahogy Bakare et al. (2024) fogalmaznak: a DeFi lényegileg átalakítja a pénzügyi közvetítést, hiszen az intézmények helyébe programkódok és irányítói tokenek lépnek.

A DeFi térnyerésével azonban újfajta kockázatokkal is kell számolnunk. A protokollszintű gyenge pontok, az irányítás manipulálása és az ellenőrizetlen orákulumokra hagyatkozás miatt nagy léptékű visszaélésekre és átfogó veszteségekre kerülhetett sor. A fogyasztóvédelem hiánya és a névtelen részvétel miatt még problémásabb a jogérvényesítés és az elszámoltathatóság. E kockázatok is igazolják e tanulmány átfogóbb tézisét, miszerint a blokklánc elméletben garantált biztonságosságát kritikusan kell vizsgálni a tényleges alkalmazás tapasztalatai és a felmerülő támadási felületek fényében.

Az uniós szabályozást támogató, de óvatos megközelítés jellemzi. Bár a MiCA-rendelet elsősorban a központi szolgáltatókra összpontosít, az Európai Értékpapírpiaci Hatóság (ESMA) a DeFi-t potenciális rendszerszintű kockázatokat rejtő területként azonosítja, különösen az átláthatatlan fedezeti modellek és a bonyolult irányítási struktúrák miatt (ESMA, 2023; ESMA, 2025). A jövőben a szabályozási keret direktebben is kitérhet majd a DeFi-re, és a hagyományos, szervezethez kötött felügyelet helyett nagyobb hangsúlyt kaphatnak a szerepkörhöz kötött szabályok.

Magyarországnak jelenleg nincs saját DeFi ökoszisztémája, de a kriptovalutafelhasználók aktívan használják a nemzetközi protokollokat. Magyar egyetemek és agytrösztök készítettek elemzéseket az okosszerződések kockázatairól, a likviditás felaprózódásáról és a jogilag szabályozatlan területekről, míg az MNB figyelmeztető ajánlásaiban hívta fel a figyelmet a DeFi piacok szabályozatlanságára és volatilitására.

E problémák ellenére a DeFi a programozott pénzügyi megoldások tesztelésének elsődleges színtere. A különböző rendszerelemek kombinálhatósága, az algoritmusalapú hitelezés és a decentralizált irányítás terén létrejött újítások lehetnek

a jövő pénzügyi infrastruktúrájának kiindulópontjai, amennyiben ez megfelelő szabályozói biztosítékokkal és intézményesült tervezési elvekkel társul.

4. A BLOKKLÁNC HATÁSA A PÉNZÜGYI RENDSZEREK BIZTONSÁGÁRA

A blokkláncot gyakran szerkezetéből fakadó biztonságossága miatt dicsérik, ami egyértelmű előnyöket kínál a hagyományos pénzügyi rendszerekkel szemben. Architekturális szinten a decentralizált jelleg kiiktatja az egyedi gyenge pontokat, hiszen a bizalom eloszlik a hálózatot alkotó csomópontok között, így az kevésbé van kitéve a jogosulatlan beavatkozásnak és hozzáférésnek. Minden tranzakció kriptográfiai eszközökkel kapcsolódik a korábbi tranzakciókhoz, biztosítva a megváltoztathatatlanságot és az ellenőrzési visszakövethetőséget. E tulajdonságok együttese javítja az adatok sértetlenségét, az elszámoltathatóságot a tranzakciók tekintetében, valamint az átlátható működést.

Ezek az elméleti előnyök jól illeszkednek az Európai Unió digitális bizalmat és szabályozáshoz való alkalmazkodást hangsúlyozó megközelítésébe. Az olyan uniós kezdeményezések, mint az EBSI, határozottan támogatják a hamisításvédett technológiák alkalmazását az érzékeny pénzügyi, személyazonosító és közbeszerzési adatok védelmére. A magyar pénzügyi intézmények és fintech vállalatok is egyre nyitottabbak a blokkláncnak a belső kontrollrendszer, az ellenőrzési nyomvonal sértetlensége és az egyeztetés hatékonysága terén kamatoztatható biztonsági előnyeire (MNB, 2023). Bár alkalmazása még mindig korlátozott, e kísérleti projektek arról árulkodnak, hogy egyre nagyobb a blokklánc mint a pénzügyi műveletek biztonságát és szabályszerűségét biztosító eszköz iránti érdeklődés. Chittoju és Ansari (2024) is hangsúlyozzák, hogy a blokklánc – titkosításra és tartós nyilvántartásra épülő – szerkezetéből fakadóan előmozdítja a biztonságot és az átláthatóságot a banki szolgáltatásokon és a biztosítási szektoron át az eszközkezelés területéig, bár egyelőre korlátot jelent skálázhatósága és a szabályozás kiforratlansága.

Ezeket a megállapításokat a gyakorlati alkalmazási tapasztalatok is megerősítik. A magánszektorban a JPMorgan Onyx (illetve ma már Kinexys néven futó) platformja JPM Coin valutában számolja el biztonságosan és szinte valós időben a bankközi tranzakciókat és repókat, míg a Santander 2019-ben, az Ethereum platformon lebonyolított 20 millió USD értékű kötvénykibocsátási ügyelete bizonyította, hogy kivitelezhető az okosszerződésekre alapuló klíring és elszámolás (Ihnatiuk, 2024, Allison, 2019, Finadium, 2024). E példák jól mutatják, hogy a blokklánccal szinkronizálhatók a különféle üzleti partnerek közötti pénzügyi folyamatok és fokozható a „szállítás fizetés ellenében" elv érvényesülése. Hasonló

eredménnyel zárultak a közszférában indított kísérletek is. Az Európai Beruházási Bank digitáliskötvény-kibocsátásai és a Horizon támogatási program kísérleti projektjei kapcsán a csalások elleni védettség és az adatok auditálhatóságának javulásáról, valamint hatékonyabb folyamatokról számoltak be (Ledger Insights, 2021; Goldman Sachs, 2021). Az ázsiai kontinensen a Szingapúri Pénzügyi Felügyeleti Hatóság vezetésével a blokkláncot határokon átnyúló fizetési tranzakciókhoz és a kereskedelemfinanszírozásban alkalmazták, bizonyítottan javítva a megbízhatóságot és a kockázatcsökkentést (Bangkok Post, 2023).

Magyar viszonylatban az EBSI-hez kapcsolódó projektek és a hazai kutatóintézmények a blokklánc közpénzügyek és csalásellenes rendszerek keretében történő felhasználását vizsgálták (Capacities, 2023; MNB, 2023). Bár kísérleti szakaszban lévő projektekről beszélünk, ezekből is látható, hogy a magyar nemzeti prioritások találkoznak az EU által felvázolt stratégiai irányvonallal. Ezeken túlmenően a magyarországi fintech vállalatok elosztott főkönyvi technológiára alapuló tranzakciófigyelő eszközöket tesztelnek, az állami intézmények pedig a digitális közigazgatás és a pénzmosás elleni jelentések kapcsán vizsgálják a blokklánc alkalmazási lehetőségeit.

Ugyanakkor a blokklánccal összetett és gyakran alulértékelt biztonsági kockázatok jelentek meg, különösen az alkalmazási réteg szintjén. Bár a decentralizált pénzügyi szolgáltatások és a tokenizáció kulcsfontosságú eszközei az okosszerződések, megfelelő működésüket könnyedén alááshatják a programozási és logikai hibák, valamint a váratlan játékelméleti sebezhetőségek. A 2016-os DAO-incidenshez hasonló súlyos visszaélések és a DeFi protokollokat ért újabb keletű támadások rávilágítanak, milyen következményekkel járhat, ha módszeres ellenőrzés nélkül használunk önműködő programokat (Atzei–Bartoletti–Cimoli, 2017, Zhang–Lee, 2021). Ezek a hiányosságok visszafordíthatatlan kárt okozhatnak a felhasználóknak, és rendszerszintű kockázatot jelentenek, különösen az egymással kombinálható protokollok esetében.

Egy másik kritikus sebezhetőség az orákulumokra, azaz a külső adatforrásokra hagyatkozás az okosszerződések végrehajtása céljából. Az orákulumokra nem terjed ki a blokklánc bizalmi modellje, és gyakran centralizált vagy nem biztonságos, ezért manipulálható vagy a rendszerből könnyen kieső szereplőkről beszélünk. Már számos DeFi biztonsági incidenshez, köztük gyorskölcsönökhöz kapcsolódó visszaélésekhez és a fedezet nem megfelelő áron történő értékesítéséhez vezettek az orákulumoktól származó hibás vagy hamis adatok (Li et al., 2020; Zhang–Lee, 2021).

A kulcsok kezelése további kihívást jelent. A blokkláncrendszerekben a biztonsági felelősség a felhasználókra hárul, akiknek intézményi támogatás nélkül kell megóvniuk a privát kulcsokat. A kulcs elvesztése vagy illetéktelen felhasználása az eszközök végleges elvesztését eredményezi, ami jelentős aggályokat vet

fel olyan jogi környezetben, ahol a fogyasztóvédelem és a vitarendezés kiemelt fontosságú. Ezek a kérdések különösen érvényesek a GDPR-hoz és a MiCA-hoz hasonló európai keretrendszerek összefüggésében, amelyekben hangsúlyosak az egyéni jogok és az intézményi elszámoltathatóság. Finck (2019) rávilágít, hogy a blokklánc állandósága miként ütközik a GDPR-ban rögzített „elfeledtetéshez való joggal". Ez a feszültség olyan technikai megoldásokat szült, mint a láncon kívüli adattárolás, az adathashelés és a nem feltáró bizonyítás.

A magyar pénzügyi hatóságok is felismerték a fenti a kockázatokat. A Magyar Nemzeti Bank FinTech és digitalizációs jelentésében (MNB, 2023) fokozódó kiberfenyegetettséget azonosít a hazai pénzügyi szektorban, aggályos területként megjelölve a tranzakciós csalásokat és az adathalászatot. A pénzügyi szereplők számára egyre világosabb, hogy a digitális innovációhoz jól szervezett kiberbiztonsági keretrendszereknek kell társulnia, amit jól szemléltetnek a KiberPajzshoz hasonló kezdeményezések. A szabályozás gyors ütemben alkalmazkodott, de még nem teljes. Az EU 2024 decemberétől hatályos MiCA-rendelete harmonizált rendszert hoz létre a kriptoeszköz-szolgáltatók számára, a működési biztosítékokra, a fogyasztóvédelemre és a kockázati adatközlésre vonatkozó egyértelmű követelményekkel. Bár a MiCA elsősorban a centralizált platformokra fókuszál, a benne foglalt elképzelések iránymutatást adnak az okosszerződések, a főláncot érintő irányítás és az összekapcsolt DeFi rendszerek szabályozásáról szóló eszmecseréhez is (MiCA-rendelet, 2025; ESMA, 2023). Mindeközben a pénzmosás elleni és az ügyfél-átvilágítási kötelezettségek betartatása problémás a közvetlenül nem azonosítható szereplőkkel működő nyilvános láncokon. Az említett ellentmondások feloldását célozzák az EU digitális személyiadat-tárca és EBSI-projektjéhez csatlakozó hibrid személyazonosság-kezelő keretrendszerekkel folyó kísérletek (Biometric Update, 2024; Európai Bizottság, 2025).

A magyar szabályozó hatóságok is az EU álláspontját követik. Az MNB és a Nemzeti Adatvédelmi és Információszabadság Hatóság hangsúlyozza, hogy a blokklánc-alkalmazásoknak nemcsak a MiCA és a GDPR szabályainak, hanem a pénzügyi felügyeletre, a fogyasztói jogokra és az intézményi elszámoltathatóságra vonatkozó hazai szabályoknak is meg kell felelniük (MNB, 2023; ActiveMind, 2024). A hatóságok ösztönzik az innovációt, de nem engednek a jogi megfelelőségből, különösen a személyes adatokat érintő vagy pénzügyi kockázati kitettséggel járó projektek esetében.

Összességében a blokklánc pénzügyi biztonságra gyakorolt hatása nem kétpólusú, biztonságos/nem biztonságos felosztásban, hanem inkább a kockázati környezet átrendeződéseként értelmezhető. Miközben kiküszöböl egyes hagyományos rendszerekre jellemző sebezhetőségeket, például a centralizált adatsilókat és az átláthatatlan elszámolási folyamatokat, új támadási és hibalehetőségeket is működésbe hoz. A blokklánc biztonsági potenciáljának maximális érvényesüléséhez

a kriptográfiai kifinomultság mellett megbízható irányítás, egyértelmű jogi háttér és intézményi szintű integráció szükséges. A szabályozók és a fejlesztők előtt álló kihívás az, hogy ezeket a biztosítékokat a blokkláncon alapuló rendszerek legfőbb értéke, a decentralizáció és a programozhatóság sérelme nélkül építsék be.

5. A BLOKKLÁNC BIZTONSÁGÁNAK ÉS INFRASTRUKTÚRÁJÁNAK ÖSSZEHASONLÍTÓ ELEMZÉSE

A blokklánc pénzügyi biztonsági értékét csak úgy lehet érdemben felmérni, ha a képességeit nem önmagukban, hanem azokkal az infrastruktúrákkal összevetve vizsgáljuk, amelyeket kiegészíteni vagy kiváltani hivatott. A pénzügyi üzenetközvetítés, klíring és elszámolás régóta az olyan hagyományos rendszereken nyugszik, mint a SWIFT, a SEPA és az automata elszámolóházak (ACH-k). Ezeket a rendszereket centralizáltság, kialakult jogszabályi háttér és stabil működés jellemzi, ehhez azonban lassúság, nagy egyeztetési igény és közvetítői részvétel társul.

Ezzel szemben a blokklánccal egy gyökeresen eltérő, megosztott konszenzuson, valós idejű véglegességen és előre programozott elszámoláson alapuló modell jelent meg. Az olyan atomikus átutalási mechanizmusokat megvalósító platformok, mint a RippleNet és a Stellar, csökkentik a partnerkockázatot és lerövidítik a tranzakciós ciklust (Global Radar, 2025). Széles körű elterjedésüket azonban olyan nehezen áthidalható kihívások gátolják, mint a hagyományos pénzügyi rendszerekkel való interoperabilitás, a jogszabályi háttér kiforratlansága és a változó intézményi bizalom. Az Európai Unióban az átfutási idő átfogó infrastrukturális módosítások nélküli lerövidítésére olyan kezdeményezések indultak, mint a TARGET Instant Payment Settlement (TIPS), azaz a pán-európai azonnali elszámolási szolgáltatás, amely ugyancsak az EU lépésenként haladó stratégiáját példázza (EKB, 2018; Modern Treasury, 2025). Magyarország részvétele a SEPA-rendszerben és a blokkláncalapú kísérleti programokban hibrid megközelítést tükröz: a modernizációra való nemzeti törekvés a blokklánc kritikus fontosságú munkafolyamatokba való integrálásának körültekintő értékelésével párosul.

Biztonságökonómiai szempontból a blokkláncot egyaránt jellemzi működési hatékonyság és jelentős tervezési kompromisszumok. A blokklánc főkönyvének megváltoztathatatlansága csökkenti a csalás kockázatát, javítja az auditálhatóságot, és mérsékli az elszámolási kockázatot, különösen, ha ezt az okosszerződések előre programozott szabályrendszerei is segítik (Chan et al., 2022). Az olyan kriptográfiai mechanizmusok, mint a digitális aláírás, a hashfüggvények és a Merkle-fák, segítenek kivédeni az adathamisítási kísérleteket és a személyazonossággal való visszaéléseket (IBM Developer, 2018). A nagy értékű tranzakciókat bonyolító

rendszerek esetében ezek a tulajdonságok jelentősen csökkenthetik a működési kockázatot.

Mindennek azonban megvan a maga hátulütője. Az okosszerződések sebezhetőségei és az orákulumok tévedései továbbra is visszafordíthatatlan pénzügyi veszteséget okozhatnak, aláásva a nem engedélyköteles ökoszisztémákba vetett bizalmat (CEUR Workshop, 2024). A blokkláncon alapuló infrastruktúrák, különösen a proof-of-work modellben működő hálózatok energiaigénye fenntarthatósági aggályokat vet fel, ami szembemegy az EU környezetvédelmi és digitális rezilienciára irányuló célkitűzéseivel (Energy Sustainability Directory, 2023). Emellett a blokklánc széles körű alkalmazása nemcsak technikai beruházásokat igényel, hanem a jogszabályok kiigazítását és a kiberbiztonsági eszköztár átalakítását is. Intézményi szinten ez új szakemberek felvételével, a megfelelőségi modellek korszerűsítésével és a blokklánc többrétegű digitális biztonsági architektúrákba integrálásával jár (Rapid Innovation, 2024; GSCARR, 2022).

A magyar intézményeknél, különösen a kisebb bankoknál és a közszektorbeli szerveknél különösen súlyosak ezek a költség-haszon dilemmák. Míg a blokklánc csökkenthetné a megfelelőségi és egyeztetési többletköltségeket, az integrációjához kapcsolódó beruházási költségek, a szabályozás összetettsége és a képzett munkaerő hiánya továbbra is akadályt jelent. Az EU által finanszírozott programok, mint a Horizon 2020 és a Digital Europe, a kezdeti költségigény enyhítésével kulcsfontosságú támogatást nyújtanak a tagállamok számára, amelyek így aránytalan fiskális kockázat nélkül fedezhetik fel a biztonságos innovációt (Chan et al., 2022).

A technikai előnyökön túl a blokklánc biztonsági potenciálját három alapvető dimenzió kölcsönhatása határozza meg, nevezetesen a kriptográfia, az irányítás és az infrastruktúra. A blokklánc meghamisíthatatlansága és adatvédelmi funkciói az olyan kriptográfiai alapelemekre vagy „primitívek"-re épül, mint a nem feltáró bizonyítási mechanizmusok és a küszöbaláírás (Hagen, 2023). Csakhogy, még a kifogástalan kriptográfiai tervezés sem helyettesítheti a megbízható irányítást. A protokollfrissítésekre, a vitarendezésre és a validátori ösztönzőkre vonatkozó döntésektől függ, hogy egy hálózat képes-e megőrizni elvárt biztonsági profilját. Az elégtelen irányítás aláásható a bizalmat, szétzilálhatja a hálózatot fenntartó közösséget, vagy lehetőséget adhat a rosszindulatú szereplőknek a konszenzusok kimenetelének manipulálására (Kasimatis et al., 2022).

A harmadik pillért az infrastruktúra adja. A blokkláncon alapuló alkalmazások biztonsága nem pusztán a főkönyvön, hanem a kapcsolódó rendszerek tulajdonságain, így a tárcaszoftvereken, a csomópontok megbízhatóságán, a letétkezelői integritáson és az API-végpontokon is múlik. Az ezeken a rétegeken jelentkező gyengeségeket a támadók kihasználhatják, még ha maga a blokkláncprotokoll sértetlen is marad. E kockázatok fokozottabban érvényesülnek a kevésbé fejlett

digitális infrastruktúrájú, vagy egységes kiberbiztonsági normákkal nem rendelkező joghatóságokban. Az európai blokklánc-szolgáltatási infrastruktúra (EBSI) holisztikus választ ad ezekre a kihívásokra. A fejlett kriptográfiát, tagállami szintű irányítást és átjárható infrastruktúrát egyesítő EBSI célja, hogy biztonságos és skálázható alapokat teremtsen a páneurópai blokklánc-szolgáltatások számára (European Blockchain Services Infrastructure, 2024). Magyarország aktív szerepe az EBSI kísérleti programjaiban, különösen az önrendelkező személyazonosság-kezelés területén, igazolja az ország elkötelezettségét a blokklánc egységes jogi és megbízható technikai háttérbe illesztése iránt (Du Seuil et al., 2023, PriFoB Consortium, 2023).

1. táblázat
Összehasonlító táblázat a hagyományos és blokklánc alapú rendszerek között

Tulajdonság	Hagyományos rendszerek (SWIFT/ACH/TIPS)	Blokkláncalapú rendszerek (pl. RippleNet, Stellar)
Elszámolás sebessége	T+1 vagy hosszabb; kötegelt, gyakran több órás vagy napos késéssel (Owolabi et al., 2024).	Néhány perc vagy másodperc; közel valós idejű elszámolás (Global Radar, 2025; Chainspect, idézi: Shei et al., 2025).
Közvetítői részvétel	Erős függés a klíringházaktól és levelező bankoktól.	Minimális vagy hiányzik: az elszámolás a résztvevők között, megosztott konszenzus alapján történik (Finextra, 2025).
Tranzakciós költség	Közepestől magas (határokon átnyúló tranzakciós díjak).	Jellemzően alacsonyabb a közvetítők kiiktatása és a stablecoinok miatt (Rapid Innovation, 2024; EKB, 2025).
Auditálhatóság/ átláthatóság	Központi nyilvántartások; korlátozott betekintési lehetőség a főbb szereplőkön kívül.	Teljes körű, hamisításvédett, azaz átláthatóan visszakövethető nyilvános főkönyv.
Véglegesség és visszafordíthatóság	A véglegesítés késleltetett; adott esetben visszafordítható; egyeztetési hibák lehetősége (Owolabi et al., 2024).	Alacsonyabb partnerkockázat a fizetési tranzakciók szinte azonnali, visszafordíthatatlan elszámolása miatt.
Interoperabilitás	Globális szabványok (pl. SWIFT, SEPA) biztosította magas fokú integráció.	Széttagoltság; az eltérő protokollok gátolják a rendszerek közötti zökkenőmentes integrációt.
Szabályozási és jogbiztonság	Magas fokú: kialakult keretrendszerek szabályozzák.	Kialakulóban: joghatóságonként eltérő jogállás; a MiCA meghatározza a kialakuló szabályozás körvonalait.

Forrás: saját szerkesztés

Az *1. táblázat* összeveti a hagyományos pénzügyi infrastruktúrák (pl. SWIFT, ACH, TIPS) és a RippleNethez és Stellarhoz hasonló, blokkláncon alapuló rendszerek relatív erősségeit és korlátait. A blokklánc előnyei egyértelműek az elszámolás sebessége, az auditálhatóság és az átláthatóság terén, hiszen szinte valós időben véglegesednek a tranzakciók, amelyeket hamisításvédett nyilvántartás rögzít, és közvetítőkre is kevésbé van szükség. E jellemzők jól illeszkednek az EU digitális bizalom növelésére, a szabályozási követelmények észszerűsítésére és a rendszerek széttagoltságának csökkentésére irányuló célkitűzéseibe. A blokklánc előnyeit azonban ellensúlyozza az erősen korlátozott interoperabilitása és kiforratlan jogállása. A hagyományos rendszerek erényét a szabványos protokollok és a kialakult szabályozási keret jelentik, míg a blokklánchálózatok működését egyelőre széttagoltság és formálódó, joghatóságonként változó szabályok jellemzik. Az eltérések miatt problémás átfogóbb alkalmazásuk, különösen a jogilag összehangolt, de működését tekintve sokféle európai pénzügyi környezetben.

A fentiekből következik, hogy a blokklánc nem fog máról holnapra a hagyományos rendszerek helyébe lépni. Ehelyett a legvalószínűbb forgatókönyv a hibrid architektúrák elterjedése, amelyek kiegészítik, nem kiváltják a meglévő infrastruktúrát. Ezzel a modellel is fokozható a hatékonyság és a reziliencia, feltéve, hogy megbízható irányítási keretrendszerben és az intézmények folyamataiba biztonságosan integrálva működik. Magyarország részvétele az uniós kísérleti projektekben és a SEPA-ban éppen ezt az óvatos, de haladó megközelítést tükrözi. Végső soron a tágabb jogi, működési és intézményi ökoszisztémák érettségén és nem csupán kriptográfiai alapjain is múlik, mennyire tudnak érvényesülni a blokklánc biztonsági adottságai. Ebből a szempontból a blokklánc sokkal inkább átcsoportosítja, mint felszámolja az intézményi kockázatokat, ezért az elméleti erősségei csak jól szervezett felügyelet, világos normák és rugalmas szabályozási modellek mellett hajthatnak tényleges biztonsági hasznot.

Az utóbbi években a blokklánc fejlődési pályáját egyre inkább a tágabb monetáris és technológiai paradigmába való beolvadás határozta meg, különös tekintettel a központi banki digitális fizetőeszközök kifejlesztésére, a mesterséges intelligencia (MI) és az adatvédelmi kriptográfia párhuzamos térnyerésére, valamint a RegTech keretrendszerek kialakulására. Az EKB központi szerepet tölt be a lakossági és kereskedelmi banki CBCD-architektúrák kialakításában, amelyek közül a digitális euro kezdeményezés tekinthető az EU első számú válaszának a digitalizációra és pénzügyi stratégiai függetlensége biztosítására. Bár az EKB kifejezetten elhatárolódik a „programozott pénz" kifejezéstől, a kezdeményezés keretében folyó tervezési egyeztetései visszagazolták a feltételes kifizetések, késleltetett pénzmozgások és ismétlődő tranzakciók jelentőségét, amelyek a felhasználói adatok védelme vagy a monetáris semlegesség sérelme nélkül valósítanak meg a programozhatósághoz hasonló funkciókat (Európai Központi Bank, 2024;

EBF, 2023). Ezzel párhuzamosan a magyar jegybank, az MNB, újszerű CBCD-kísérleti projektbe kezdett a Diákszéf applikációval, amely a 8–14 éves gyermekek pénzügyi műveltségét kívánja fejleszteni. Bár kisebb léptékű, a projektben szerepet kapnak olyan programozható összetevők, mint a szülői felügyelet és az előre meghatározott kiadási kategóriák, ami mutatja, hogy Magyarország tevékenyen részt vesz az uniós irányvonalat követő pénzügyi innovációban (Magyar Nemzeti Bank, 2023; Central Banking Publications, 2023).

Mindeközben a blokklánc-ökoszisztéma továbbfejlődésében új lépcsőfokot jelent a kapcsolódó technológiákkal, különösen az MI-vel, a dolgok internetével (Internet of Things, IoT) és a nem feltáró kriptográfiai megoldásokkal való integrációja. Egyre szélesebb körben használnak MI-alapú elemzést a csalások azonosítására, a szabályozás szerinti kötelező jelentéstétel egyszerűsítésére és az okosszerződések működésének javítására (Pasupuleti, 2025, Nguyen et al., 2024). Az MI blokkláncon alapuló megfelelési rendszerekbe illesztésével javítható a tranzakciófigyelés és a döntéshozatal, kizárva az emberi elfogultságot és a késedelmeket. Az IoT és a blokklánc találkozásából megjelentek többek között a biztosítások, a logisztika és az ellátásilánc-finanszírozás területén az adatok sértetlenségét valós időben, szenzorok segítségével biztosító megoldások, amelyek keretében az okoseszközök automatikusan hajtanak végre tranzakciókat az ellenőrzött input alapján (Rapid Innovation, 2024). Magyarországon is számos fintech startup vállalkozás és egyetemi konzorcium kezdte el uniós finanszírozású kezdeményezések keretében feltérképezni e lehetőségeket, köztük az MI-vel támogatott csalásmegelőzési rendszereket és az adatvédelem-központú tranzakció-ellenőrző platformokat.

Az adatvédelem és a jogszabályoknak való megfelelés területén az egyik legjelentősebb fejleményt a nem feltáró bizonyítási (ZKP) módszerek, ezen belül is a zk-SNARK és zk-STARK mechanizmusok jelentik. E mechanizmusokkal az adatok felfedése nélkül végezhetőek el ellenőrizhető módon a számítások, azaz a blokklánc GDPR-nak is megfelelő alkalmazását lehetővé tevő kriptográfiai módszerek. Pénzügyi környezetben a ZKP-módszerek szilárd adatvédelmi garanciát nyújtanak a digitális személyazonosság-kezelés, a magánhitelek és a szelektív adatközlés terén, amely előfeltétele a blokklánc szabályozott célterületeken való megjelenésének. Magyarország részvétele a ZKP-módszereket és blokkláncon alapuló digitális személyazonosság-kezelést is magában foglaló egyetemi és kísérleti projektekben jól mutatja a tágabb nemzeti stratégia összhangját az uniós kiberbiztonsági és adatvédelmi célkitűzésekkel (Volet, 2024, ResearchGate, 2024).

Az összhang különösen látványos a RegTech területén. A blokklánc mára megkerülhetetlen a megfelelés automatizálásában az egyre komplexebb szabályozói követelményekkel szembesülő intézmények számára. Az okosszerződések KYC/AML-szabályokat rögzíthetnek, ellenőrzési nyomvonalat hozhatnak létre és segítik a valós idejű felügyeletet, a szabályozási követelményeket előre programozott

szabályrendszerekké alakítva (EBH, 2021, AML Watcher, 2024). Lendületesen növekvő fintech ökoszisztémájának köszönhetően, amelyben több mint 200, a megfelelés automatizálása és a digitális személyazonosság-kezelés területén tevékenykedő cég vesz részt, Magyarország vezető RegTech szereplővé léphet elő. Az MNB 2018-ban indított saját szabályozói tesztkörnyezete és Innovation Hub-ja felügyelt környezetben teszi lehetővé a blokkláncalapú megfelelési mechanizmusok „éles" tesztelését (Cemla/MNB, 2019). Ez a szabályozói háttér elősegíti a nemzeti digitális átalakulást, miközben biztosítja, hogy az innováció a jogszabályi keretek között maradjon és a közérdeket szolgálja. Az EU digitális személyazonosság-kezelési kezdeményezéseiben is az innováció és a jogi megfelelés egyensúlya érvényesül. Az uniós digitális személyiadat-tárca és a blokklánc-szolgáltatások európai infrastruktúrájának célja, hogy az azonosító adatok mindenhol zökkenőmentesen és az állampolgárok teljes kontrollja alatt áramolhassanak a rendszerek között, a határokon átnyúló közszolgáltatásokon át a magánszektorbeli KYC-követelményekig. Magyarország is részt vesz a jóléti támogatások elosztását, adóügyi szolgáltatásokat és a biztonságos azonosítást érintő tesztprogramokban, amely ugyancsak azt mutatja, hogy a blokkláncon alapuló személyazonosság-kezelési megoldásokkal ma már a pénzügyeken túl az átfogóbb kormányzati szolgáltatásokban is találkozhatunk.

A blokklánc hosszú távú fenntarthatósága és biztonsága végső soron az ösztönzési alapelvének fejlődésén múlik. A Targeted Nakamoto protokoll újfajta konszenzusos megközelítést képvisel, amely az energiaigényes biztonsági alapvetések helyett jutalomközpontú dinamikára épül. Azáltal, hogy a protokoll a nehézség helyett a hálózat számítási teljesítményét mérő hashráta alapján ösztönzi a bányászokat, olyan visszacsatolási mechanizmust vezet be, amellyel a környezeti hatás minimalizálása mellett tartható optimális szinten a biztonság (Aronoff, 2024). Az ehhez hasonló innovációk közvetlenül hatnak a blokklánc közszektorbeli alkalmazására is, ahol egyre fokozottabban érvényesülnek az EU ESG-célkitűzései és a MiCA fenntarthatósági előírásai. A jövőben az ösztönzővezérelt konszenzus alapján valósulhat meg az energiahatékonyság, a hálózat ellenálló képessége és a gazdasági kiszámíthatóság közötti egyensúly a CBCD-k, a tokenizált eszközök platformjai, illetve a szabályozott nyilvános főkönyvek esetében.

Mindezek a fejlemények azt mutatják, hogy a blokklánc felfutó kísérleti technológiából intézményesült infrastruktúrává emelkedett. A programozott pénzügy, a kriptográfiára épülő adatvédelem, az automatizált szabályozás és a fenntartható protokolltervezés kölcsönhatása formálja Európa új generációs pénzügyi ökoszisztémáját. Magyarország szerepvállalása – a kísérleti programokon, valamint a szabályozói és tudományos részvételen keresztül – megmutatja, hogy a kisebb tagállamok is tevékenyen hozzájárulhatnak az átalakuláshoz, feltéve, hogy nem-

zeti politikájuk összhangban van a biztonságra, innovációra és digitális szuverenitásra vonatkozó uniós szabványokkal.

Az elmúlt évtizedben a blokklánc-technológia gyökeresen átalakította a pénzügyi szektort a vele megjelenő új biztonsági paradigmával, amely a decentralizáció, a megváltoztathatatlanság és az algoritmusokba vetett bizalom köré szerveződik. Alapvető tulajdonságai mérhető eredményeket hoztak az adatok sértetlensége, az auditálhatóság és a tranzakciók nyomonkövethetősége terén, különösen a határokon átnyúló fizetések, az eszköztokenizáció és a digitális személyazonosság-ellenőrzés területén. Ezek az alkalmazási példák is igazolják, hogy a blokklánc meghamisíthatatlan és automatizált jellege képes visszaszorítani a csalást, növelni az átláthatóságot és észszerűsíteni a működési folyamatokat.

Mindazonáltal ezek az előnyök újszerű kockázatokkal is járnak. Azzal, hogy a blokklánc a bizalmat a hatóságilag szabályozott közvetítőkről a programkódra, a konszenzusprotokollokra és a felhasználóoldali kulcskezelésre helyezi át, a hagyományos pénzügyekben ismeretlen sebezhetőségeket hoz mozgásba. Az okosszerződések sebezhetőségei, az orákulummanipuláció és a kulcsok visszafordíthatatlan elvesztésének következményei megerősítik a gondos technikai tervezés, a módszeres ellenőrzés és a biztonságos infrastruktúra fontosságát. A blokklánc tehát ahelyett, hogy megszüntetné a kockázatokat, inkább átcsoportosítja azokat, és nagyobb felelősséget ró a rendszerarchitektúrára, az irányítási modellekre és a felhasználói magatartásra.

Ebből az elmozdulásból következően újra kell értékelni a pénzügyi biztonság jelentőségét decentralizált környezetben. A biztonságot itt ugyanis már nem pusztán az intézményi felügyelet garantálja, hanem a protokollszintű irányítás megbízhatósága, a kriptográfiai eszközök integritása és a jogi átjárhatóság. A szabályozók feladata ezért a végrehajtáson túl kiterjed a biztonságos innovációt támogató keretrendszerek kialakítására. Ezt a megközelítést képviseli az Európai Unió MiCA-rendelete és digitális személyiadat-tárca kezdeményezése, amelyek harmonizált szabványokat mozdítanak elő anélkül, hogy gátat szabnának a kísérletezésnek.

Magyarország tevékenysége is ebbe a tágabb dinamikába illeszkedik. A tudományos kutatásokban, fintech innovációban és az uniós blokkláncalapú kezdeményezésekben való aktív részvétel révén Magyarországon kiépült a blokklánc alkalmazásához szükséges alapvető ökoszisztéma. Magyarország ugyanakkor megfontoltan közelít a nemzeti szintű blokklánc-implementációhoz, óvatosan igazodva a kialakuló szabályozói és kiberbiztonsági előírásokhoz. Ez a hibrid álláspont, azaz az innováció felkarolása a megfelelést előtérbe helyező keretrendszerben mozogva, lehetővé teszi a blokklánc gyakorlati alkalmazásainak felelős és biztonságos skálázását Magyarországon.

A blokklánc tehát összességében egyértelműen nem javította, inkább átalakította a pénzügyi biztonságot. Nem az abszolút bizonyosság, hanem a programozott bizalom a legígéretesebb jellemzője. Ennek kiaknázásához egyaránt szükséges a gondos technikai tervezés, az átlátható irányítás és a proaktív szabályozás. Elengedhetetlenül szükséges a folyamatos tudományközi együttműködés ahhoz, hogy az átmeneti jelenségből infrastruktúrává érő blokklánc elméleti előnyeiből tartós biztonsági hasznot kovácsolhasson a pénzügyi szektor.

6. BEFEJEZÉS

Az elmúlt egy évtizedben a blokklánc-technológia a főként a bitcoinhoz társított résterületi innovációból a digitális pénzügyek alapelemévé vált. Alapvető tulajdonságai – a decentralizáció, a megváltoztathatatlanság és a kriptográfiai biztonság – miatt épülhetett be a fizetési és értékpapírpiaci folyamatokba, a decentralizált pénzügybe és a személyazonosság-kezelő rendszerekbe. E fejlődés mögött a technológia fejlődése mellett az intézményi érdeklődés áll: a pénzügyi szereplők és szabályozó szervek Európán belül és kívül elkezdték feltérképezni a blokklánc átláthatóságát, auditálhatóságát és hatékonyságnövelő potenciálját. A tanulmány ugyanakkor hangsúlyozza, hogy a blokklánc nem abszolút garancia a biztonságra. Beépülése a pénzügyi infrastruktúrába ehelyett inkább átformálta, átcsoportosította, és bizonyos esetekben erősítette a kockázatokat.

A kutatás egyik fő megállapítása, hogy a blokklánc kiválóan teljesít olyan területeken, ahol a központosított pénzügyi rendszerek régóta sebezhetőek. A nyomtalanul nem módosítható, ezért hamisításvédett főkönyvet megvalósító blokklánc növeli a nyomonkövethetőséget és csökkenti a manipulációs és csalási lehetőségeket. A határokon átnyúló fizetések, a valós idejű elszámolás és az eszköztokenizáció területén megvalósított alkalmazásai bizonyítják, milyen jelentős mértékben képes növelni a működési rezilienciát. Ezeket az eredményeket felismerték a jegybankok, kereskedelmi szervezetek és a szabályozó hatóságok is, így olyan kísérleti programok indulhattak el, mint az EBSI, a digitális euro kezdeményezés és a többek között Magyarországon végzett nemzeti kísérleti projektek. A szabályozási megfelelés automatizálásának és a protokollszintű auditfunkciók kialakításának lehetősége a blokkláncot a pénzügyi felügyelet és RegTech forradalmi eszközévé teszi.

A fenti előnyöket azonban eddig ismeretlen biztonsági kockázatok kísérik. Azzal, hogy a biztonság az intézményekről áttevődik a kriptográfiai biztosítékokra, a rendszer sértetlenségéért szoftverek, irányítási protokollok és a felhasználók felelnek. Az okosszerződések gyenge pontjai, az orákulumokra mint külső adatforrásokra való hagyatkozás és a személyes kulcsok kezelésének problematikája a hagyományos pénzügyekben látottaktól eltérő, de nem kevésbé súlyos kockáza-

tokkal jár. A DeFi ökoszisztémák kombinálhatósága súlyos visszaélésekre, visszafordíthatatlan károkra és rendszerszintű kockázatokra ad lehetőséget, ami jól mutatja, milyen veszélyeket rejt az automata programok megfelelő biztosítékok nélküli alkalmazása. Ebben a megközelítésben a blokkláncban az intézményi hibalehetőségeket egy elosztott, de így is sérülékeny technológiai bizalmi modell váltja fel.

Az Európai Unió technológiára adott válaszában központi hangsúlyt kap a megfelelő jogi és szabályozási környezet kialakítása. A MiCA-rendelet harmonizált keretrendszert biztosít a kriptoeszköz-szolgáltatásokhoz, lefektetve a vonatkozó kockázatkezelési és fogyasztóvédelmi alapkövetelményeket. A DLT Pilot Regime szabályozott környezetet biztosít a blokkláncon alapuló piaci infrastruktúrák teszteléséhez, míg az eIDAS 2.0 és a digitális személyiadat-tárca úttörő megoldásoknak számítanak a decentralizált, adatvédelem-központú személyazonosság-kezelés terén. Ezek a kezdeményezések jól szemléltetik az óvatos, de kezdeményező európai innovációirányítási szemléletmódot, amelynek súlypontja a felügyelt kísérletezés. Magyarország – tudományos kutatások, fintech vállalatok és az uniós szabályozói tesztkörnyezet részvevőjeként kifejtett – tevékenysége jól példázza, hogyan tud egy kisebb tagállam ehhez a stabilitást és szabályozásnak való megfelelést előtérbe helyező blokklánc-bevezetési stratégiát felvázoló, tágabb keretrendszerhez hozzájárulni.

A tanulmány egyik általános megállapítása, hogy a blokklánc biztonsága csak az azt befogadó ökoszisztéma fényében értékelhető. Az infrastruktúra különböző rétegei, az irányítási struktúrák és a felhasználói interfészek mind kulcsfontosságú összetevők a blokklánc gyakorlati alkalmazásainak biztonsági profiljában. A technológia kriptográfiai alapjainak megbízhatósága elválaszthatatlan a tágabb működési gyakorlatok megbízhatóságától, a pénztárcák, a csomópontok vagy a letéti őrzési szolgáltatások gyenge pontjain pedig akár a legszilárdabb protokoll védelme is áttörhető. Ebből az összefonódottságból következően a biztonság valójában szocio-technikai probléma. Áthidalásához a számítástechnikai, pénzügyi, jogi és viselkedés-közgazdaságtani tudást egyesítő, tudományközi válasz szükséges.

Elméleti síkon a blokklánc átformálta a pénzügyi biztonságról alkotott fogalmakat. A hagyományos rendszerek alappillérei a központi felügyelet, a jogorvoslat és az intézményi garanciák. A blokkláncban ezeket felváltják a megosztott konszenzus, a megmásíthatatlan nyilvántartás és a programozható irányítás mechanizmusai. Ez az átalakulás újraértelmezi, és a társadalmi és jogi szerződések helyett a programkódra és a kriptográfiai bizonyításra alapozza a bizalom fogalmát. Bár a modell vitathatatlan előnye az alacsonyabb partnerkockázat, az elszámoltathatóság szempontjából bonyolultabb, és a rendszer általános ellenálló képessége is kérdéseket vet fel. A jogszabályi háttér még nem zárkózott fel ezekhez az új fej-

leményekhez, és a jövőben kialakuló szabályozásban ugyanolyan nagy figyelmet kell fordítani az irányítási modellekre, mint a technológiai alapokra.

A blokklánc a jövőben feltételezhetően inkább beépül a meglévő pénzügyi megoldásokba, mintsem kiváltja azokat. A technológia valószínűleg olyan hibrid rendszerek formájában terjedhet el általánosan, amelyekben a jelenlegi infrastruktúrára épül rá a megosztott könyvelés. A digitális euróhoz és a bankközi elszámolásban alkalmazott engedélyköteles blokklánc-megoldásokhoz hasonló kezdeményezések is ebbe az irányba mutatnak. A nem feltáró bizonyítás, az MI-alapú megfelelés és az adatvédelem-központú számítástechnika fejlődéséből arra következtethetünk, hogy a blokklánc biztonsága a jövőben tovább erősödik más technológiák bevonásával. Magyarország és a hozzá hasonló országok az uniós kísérleti projektekben való részvétellel és a kutatási kapacitások bővítésével tudják megőrizni versenyképességüket és tevőlegesen alakítani a szabályozási környezetet.

Összegezve, nem mondható ki egyértelműen, hogy a blokklánc javította vagy éppen aláásta volna a pénzügyi rendszer biztonságát. Sokkal inkább újrarendezte a viszonyokat. Leginkább katalizátornak vagy olyan erőnek tekinthető, amely a szabályozókat, a technikai szakembereket és a pénzügyi intézményeket a bizalom, a biztonság és a reziliencia működési alapjainak újraértelmezésére sarkallta az egyre digitálisabbá váló gazdasági környezetben. A programkódba épített biztonság bevezetésével és ezzel párhuzamos újfajta gyenge pontok felfedésével a blokklánc felgyorsította a pénzügyi felügyelet és a kiberbiztonság fejlődését. A következő évtizedben dől el, hogy a fejlődés egy megbízható rendszer kialakulása vagy az elaprózódás felé halad-e tovább. Előbbihez gondos technikai tervezés, szabályozói rátermettség és együttműködésre építő megközelítés szükséges. Csak így aknázhatók ki a blokklánc programozhatóságában rejlő lehetőségek a hozzá társuló kockázatok megfelelő kezelése mellett.

HIVATKOZÁSOK

ActiveMind (2024): Are blockchain and GDPR unintelligible? [Valóban érthetetlen a blokklánc és a GDPR?] *ActiveMind.Legal*. https://www.activemind.legal/guides/blockchain/.

Allison, I. (2019.09.12.): Santander settles both sides of a $20 million bond trade on Ethereum. [Az Ethereumon végrehajtott 20 millió dolláros kötvényvásárlási ügylet minden oldalát a Santander bonyolítja.] CoinDesk. https://www.coindesk.com/markets/2019/09/12/santander-settles-both-sides-of-a-20-million-bond-trade-on-ethereum.

AML Watcher (2024): Four ways RegTech will transform AML/KYC controls in 2024. [Négyféle mód, ahogyan a RegTech átalakítja az AML/KYC-ellenőrzést 2024-ben.] *AML Watcher*. https://amlwatcher.com/blog/4-ways-regtech-will-transform-aml-kyc-controls-2024/ beaumont-capitalmarkets.co.uk+5amlwatcher.com+5eba.europa.eu+5cemla.org.

Aronoff, D. (2025): Targeted Nakamoto: A Bitcoin Protocol to Balance Network Security and Energy Consumption. [A hálózat biztonságát és az energiafelhasználást kiegyensúlyozó bitcoin protokoll: a Targeted Nakamoto.] https://medium.com/coinmonks/targeted-nakamoto-6933e9a9ec79.

Atzei, N. – Bartoletti, M. – Cimoli, T. (2017): A survey of attacks on Ethereum smart contracts [Az Ethereumot ért támadások áttekintése]. International Conference on Principles of Security and Trust: 15th International Conference [Nemzetközi konferencia a biztonság és bizalom alapelveiről. 15. nemzetközi konferencia]. *POST 2017*, 164–186.

Bakare, A.F. – Omojola, J. – Chibuzor, A.I. (2024): Blockchain and decentralized finance (DEFI): Disrupting traditional banking and financial systems. [Blokklánc és decentralizált pénzügy (DeFi): felfordulás a hagyományos banki szolgáltatások és pénzügyi rendszerek világában]. https://wjarr.com/sites/default/files/WJARR-2024-2968.pdf.

Bakkt (2022): Understanding the Lightning Network: Real-World Use Cases. [Ismerjük meg a Lightning Networköt. Valós alkalmazási példák.] *Bakkt Blog*. https://www.bakkt.com/blog/understanding-the-lightning-network-real-world-use-cases.

Bangkok Post (2023. 07.15.): MAS expands blockchain trade finance initiative. [A Szingapúri Pénzügyi Felügyeleti Hatóság kibővíti blokkláncalapú kereskedelemfinanszírozási kezdeményezését.] Bangkok Post. https://www.bangkokpost.com/business/mas-expands-blockchain-trade-finance-initiative.

Beaumont Capital (2025): AML/KYC tech in European fintech: Legal shifts ahead. [AML/KYC-technológia az európai fintech szektorban: jogi változások a láthatáron.] *Beaumont Capital Markets*. beaumont-capitalmarkets.co.uk.

Beck et al., (2018): Governance in the blockchain economy: A framework and research agenda. [Irányítás a blokkláncalapú gazdaságban: keretrendszer és kutatási terv.] Journal of the Association for Information Systems, 19 (2018),1-40.

Belen-Sağlam, R. – Altuncu, E. – Lu, Y. – Li, S. (2022): A systematic literature review of the tension between the GDPR and public blockchain systems. [Szisztematikus irodalmi áttekintés a GDPR és a nyilvános blokkláncrendszerek közötti ellentmondásokról.] arXiv. https://doi.org/10.48550/arXiv.2210.04541.

Biometric Update (2024.03.07.): EU digital ID wallet trials expand across member states. [Tagállami határokon átívelő kísérleti projektek indulnak az uniós digitális személyiadat-tárcával.] Biometric Update. https://www.biometricupdate.com/2024/03/eu-digital-id-wallet-trials-expand-across-member-states.

BlockStand (2025): Second Cohort of the European Blockchain Regulatory Sandbox Announced. [Elindul az Európai Blokklánc-szabályozói Tesztkörnyezet második kohortja.] https://blockstand.eu/second-cohort-eu-blockchain-regulatory-sandbox.

Capacities (2023): EBSI : European Blockchain Services Infrastructure. [Az EBSI, azaz az európai blokklánc-szolgáltatási infrastruktúra.] https://capacities.ec.europa.eu/project/ebsi.

Central Banking (2023): Hungary's gamified CBDC pilot designed for children. [Gyerekeknek szóló, játékos CBDC kísérleti projekt indul Magyarországon.] *Central Banking*. https://www.centralbanking.com/fintech/cbdc/7959600/hungarys-gamified-cbdc-pilot-designed-for-children.

CEUR Workshop Proceedings (2024.05.14–15.): Analysis of Blockchain Sustainability through the Comparison of Different Smart Contracts Programming Languages. [A blokklánc fenntarthatóságának elemzése az okosszerződésekhez használt különböző programozási nyelvek összehasonlításával.] *Sixth Distributed Ledger Technology Workshop*, Turin, Italy. [Hatodik elosztott főkönyvi technológiai szakmai műhely, Torinó, Olaszország.] https://ceur-ws.org/Vol-3791/paper29.pdf.

Chan, N. – Chen, X.– Smith, J. (2022): Quantifying blockchain's impact on banking transaction costs. [A blokklánc banki tranzakciós költségekre gyakorolt hatásának számszerűsítése.] Frontiers in Blockchain.

https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1551970.

CoinSpeaker (2025.02.20.): ECB unveils blockchain payment system to counter US stablecoin dominance. [Az EKB bemutatta az amerikai stablecoin-dominanciát ellensúlyozni hivatott blokklláncalapú fizetési rendszerét.] *CoinSpeaker*. https://www.coinspeaker.com/ecb-unveils-blockchain-payment-system-to-counter-us-stablecoin-dominance.

CryptoSlate (2025.02.20.): ECB eyes blockchain-based payment settlement layer. [Blokkláncon alapuló fizetési elszámolási réteg bevezetése felé kacsingat az EKB.] *CryptoSlate*. https://cryptoslate.com/ecb-eyes-blockchain-based-payment-settlement-layer/.

Demertzis, M. – Martins, C. (2023): Progress with the digital euro. [Előrehaladás a digitális euro bevezetése felé.] Intereconomics, 58(4). https://www.intereconomics.eu/contents/year/2023/number/4/article/progress-with-the-digital-euro.html.

DLA Piper (2022): Tokenized securities and blockchain: Opportunities of the DLT Pilot Regime. [Tokenizált értékpapírok és a blokklánc: a DLT Pilot Regime kínálta lehetőségek.] https://www.dlapiper.com.

Du Seuil, D. – Lerouge, E. – Tan, E. – Du Caju, J. (2023): Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action research in a cross-border use case between Belgium and Italy. [Az oktatási azonosító adatok ellenőrzése az európai blokklánc-szolgáltatási infrastruktúra (EBSI) segítségével: akciókutatás egy határokon átnyúló felhasználási eset keretében, Belgium és Olaszország részvételével.] Big Data and Cognitive Computing, 7(2)79. https://doi.org/10.3390/bdcc7020079.

EBH (2021): Analysis of RegTech in the EU financial sector. [A RegTech használatának elemzése az európai pénzügyi szektorban.] *European Banking Authority*. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf.

EBF (2023): Vision on a digital euro ecosystem. [Jövőkép a digitális euro ökoszisztémájáról.] European Banking Federation. https://www.ebf.eu/wp-content/uploads/2023/03/EBF-Digital-Euro-paper-2023_final.pdf.

EKB (2018): TARGET Instant Payment Settlement (TIPS) [A TARGET azonnali elszámolási (TIPS) szolgáltatás.] *Európai Központi Bank*. https://www.ecb.europa.eu/paym/target/tips/html/index.en.html.

EKB (2025.05.): Stablecoins market share on trading platforms. [A stablecoinok piaci részesedése a kereskedelmi platformokon.] *Financial Stability Report*. [Pénzügyi stabilitási jelentés.] *Európai Központi Bank*.

Energy Sustainability Directory (2023): Challenges of blockchain energy and the shift to *proof of stake*. [A blokklánc energiaellátási kihívásai és a proof of stake-re való átállás.] *Energy Sustainability Directory*. [Fenntartható energiaellátási címtár.] https://energy.sustainability-directory.com/question/what-are-the-challenges-of-blockchain-energy/.

Európai Bankhatóság és Európai Értékpapírpiaci Hatóság (2025.01): EBA–ESMA DeFi factsheet. [EBH-ESMA DeFi tájékoztató.] https://www.esma.europa.eu/sites/default/files/2025-01/EBA-ESMA_DeFi_factsheet.pdf.

Európai Bizottság (2020): Shaping Europe's Digital Future. [Európa digitális jövőjének alakítása.] Brüsszel: Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága. https://digital-strategy.ec.europa.eu/en/library/shaping-europes-digital-future.

Európai Bizottság (2023.12.19.): MiCA will support innovation by providing proportionate regulatory and supervisory treatment of issuers of cryptoassets. [A MiCA-rendelet támogatja az innovációt azáltal, hogy biztosítja a kriptoeszköz-kibocsátók és a kriptoeszköz-szolgáltatók arányos

szabályozási és felügyeleti kezelését.]. *Digital Finance News.* [Digitális pénzügyi hírek.] https://finance.ec.europa.eu/news/digital-finance-2024-12-19_en.

Európai Bizottság (2023): Digital Finance Strategy for the EU. [Az Európai Unió digitális pénzügyi stratégiája.] Brüsszel: A Pénzügyi Stabilitás, a Pénzügyi Szolgáltatások és a Tőkepiaci Unió Főigazgatósága. https://finance.ec.europa.eu/publications/digital-finance-strategy_en.

Európai Bizottság (2023): European Blockchain Regulatory Sandbox Launches for Cross-Border Blockchain Projects. [Az Európai Blokklánc-szabályozói Tesztkörnyezet határokon átnyúló blokkláncalapú projektekre készül.] *Digital Europe Programme*. [Digitális Európa program.] https://digital-strategy.ec.europa.eu/en/news/european-blockchain-regulatory-sandbox-launches.

Európai Bizottság (2025): European Digital Identity Framework (eIDAS 2.0). [Az európai digitális személyazonossági keret (eIDAS 2.0).] Brüsszel: *Digitális Szolgáltatások Főigazgatósága*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12903-European-Digital-Identity-framework_en.

Európai Bizottság és Európai Blokklánc-partnerség (2018): Declaration on the establishment of a European Blockchain Partnership. [Az Európai Blokklánc-partnerség létrehozásáról szóló nyilatkozat.] Brüsszel: *Európai Bizottság.* https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-partnership.

Európai Értékpapírpiaci Hatóság (2023.10.11.): Decentralised finance in the EU: Developments and risks. [Decentralizált pénzügy az Európai Unióban: fejlemények és kockázatok.] https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf.

Európai Értékpapírpiaci Hatóság (2023): DLT Pilot Regime. [A megosztott főkönyvi technológia kísérleti rendszere.] https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/dlt-pilot-regime.

Európai Központi Bank (2024.04.): Progress on the investigation phase of a digital euro – Second report (May–Oct 2024). [A digitális euro vizsgálati szakaszának előrehaladása. Második jelentés (2024. május–október).] Frankfurt: *EKB*. https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.deprp202412.en.pdf.

Európai Parlament és a Tanács (2022): (EU) 2022/858 rendelet a megosztott főkönyvi technológián alapuló piaci infrastruktúrák kísérleti rendszeréről. Az *Európai Unió Hivatalos Lapja*, L151.

EU Blockchain Observatory and Forum (2022): The European Union Blockchain Landscape. [Európai Uniós blokklánckörkép.] https://www.eublockchainforum.eu/reports.

European Blockchain Services Infrastructure (2024): EBSI core network overview. [Az EBSI alaphálózatának áttekintése.] *European Commission Digital Strategy.* [Az Európai Bizottság digitális stratégiája.] https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.

Finadium (2024.11.14.). J.P. Morgan to move FX settlement to DLT and rebrands Onyx platform as Kinexys. [A J.P. Morgan a megosztott főkönyvi technológián alapuló devizaelszámolásra áll át és Onyx platformját átnevezi Kinexsysre.] Finadium. https://www.finadium.com/j-p-morgan-to-move-fx-settlement-to-dlt-and-rebrands-onyx-platform-as-kinexys/.

Finck, M. (2019): Blockchain Regulation and Governance in Europe. [A blokklánc szabályozása és irányítása Európában.] Cambridge: *Cambridge University.*

Finextra (2025.05.08.): Fluency to test offline and programmable payments for ECB's digital euro project. [A Fluency teszteli az offline és a programozott fizetéseket az EKB digitális euro projektje keretében.] *Finextra*. https://www.finextra.com/newsarticle/45947/fluency-to-test-offline-and-programmable-payments-for-ecbs-digital-euro-project.

Fireblocks (n.d.): What is Markets in CryptoAssets (MiCA)? Features & Benefits. [Mi a kriptoeszközök piacairól szóló rendelet (MiCA)? Jellemzők és előnyök.] https://www.fireblocks.com/glossary/markets-in-crypto-assets/.

Gataca (2022): Blockchain and Self-Sovereign Identity: How SSI Is Shaping the Future of Digital Identity. [A blokklánc és az az önrendelkező személyazonosság-kezelés: hogyan alakítja az SSI a digitális személyazonosság jövőjét.] https://gataca.io/blog/self-sovereign-identity-and-blockchain/.

Global Government FinTech (2023.04.27.): Hungary's MNB eyes digital identity for financial services innovation. [Magyarország jegybankja, az MNB a digitális személyazonosság terén kacsingat a pénzügyi szolgáltatások innovációja felé.]

https://www.globalgovernmentfintech.com/hungary-digital-identity-financial-services/.

Global Legal Insights (2023): Hungary: DLT Market Infrastructure and Tokenization Regime. [Magyarország: megosztott főkönyvi technológián alapuló piaci infrastruktúra és tokenizációs rendszer.] In: Initial Public Offering Regulations 2024.

Global Radar (2025.01.24.): The future of cross-border payments: A comparative analysis of SWIFT and XRP. [A határokon átnyúló fizetési tranzakciók jövője: a SWIFT és az XRP összehasonlító elemzése.] *GlobalRadar.* https://globalradar.com/the-future-of-cross-border-payments-a-comparative-analysis-of-swift-and-xrp/.

Goldman Sachs (2021.06.10.): Digitizing bonds on the blockchain. [Kötvénydigitalizálás a blokkláncon.] Goldman Sachs Insights. https://www.goldmansachs.com/insights/articles/from_briefings_10-june-2021.

Gray, D. (2025): The Lightning Network: Expanding Bitcoin Use Cases. [A Lightning Network: a bitcoin alkalmazási területeinek kiterjesztése.] *Fidelity Digital Assets*. https://www.fidelitydigitalassets.com/articles/lightning-network-expanding-bitcoin.

Hagen, R. (2023.08.12.): Cryptographic hash algorithms and digital signatures in blockchain. [Kriptográfiai hashalgoritmusok és digitális aláírás a blokkláncon.] LinkedIn Pulse. https://www.linkedin.com/pulse/cryptography-hash-algorithms-digital-signatures/.

Iansiti, M. – Lakhani, K.R. (2017): The Truth About Blockchain. [Mi várható valójában a blokklánctól?] *Harvard Business Review*. https://hbr.org/2017/01/the-truth-about-blockchain.

IBM Developer (2018): Blockchain basics: Introduction to distributed ledgers. [A blokklánc alapjai: bevezetés a megosztott könyvelésbe.] *IBM Developer* https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/.

Ihnatiuk, V. (2024.08.25.): Review of JPMorgan's Onyx blockchain platform. [Áttekintés a JPMorgan blokkláncalapú Onyx platformjáról.] Boosty Labs. https://boostylabs.com/blog/onyx.

InnReg (2025): MiCA regulation guide. [Útmutató a MiCA-rendelethez.] *InnReg.* https://www.innreg.com/blog/mica-regulation-guide.

Jongerius, S. (2019.08.13.): GDPR's Right to Be Forgotten in Blockchain: It's not black and white. [A GDPR elfeledtetéshez való joga a blokklánc összefüggésében: nem fekete vagy fehér.] TechGDPR. https://techgdpr.com/blog/gdpr-right-to-be-forgotten-blockchain/.

Kasimatis, D. – Buchanan, W.J. – Abubakar, M. – Lo, O. – Chrysoulas, C. – Pitropakis, N. – Papadopoulos, P. – Sayeed, S. (2022): Transforming EU governance: The digital integration through EBSI and GLASS. [Az uniós irányítás átalakulása: digitális integráció az EBSI és a GLASS projekteken keresztül.] arXiv. https://doi.org/10.48550/arXiv.2212.03218.

Khan, F. (2025): Bitcoin vs Lightning Network: Speed and Cost Comparisons. [A Bitcoin és a Lightning Network sebesség- és költségalapú összehasonlítása.] *Crypto Research Weekly*. https://cryptoresearchweekly.com/bitcoin-vs-lightning-network.

KPMG Germany (2025.02.): Maturity analysis of the DLT-based capital markets. [A DLT-alapú tőkepiacok érettségének elemzése.] https://kpmg.com.

Ledger Insights (2019.09.12.): Santander issues end-to-end bond on public Ethereum blockchain. [A Santander teljes körű kötvénykibocsátási folyamatot bonyolított le az Ethereum blokkláncán.] Ledger Insights. https://www.ledgerinsights.com/santander-blockchain-bond-ethereum/.

Ledger Insights (2021.04.27.): Goldman, Santander, SocGen help European Investment Bank on public blockchain bond issue. [A Goldman, a Santander és a SocGen segíti az Európai Beruházási Bank nyílt blokkláncon lebonyolítandó kötvénykibocsátását.] Ledger Insights. https://www.ledgerinsights.com/goldman-santander-socgen-european-investment-bank-eib-public-blockchain-bond-issue/.

Ledger Insights (2024.05.01.): EU stock exchanges trial blockchain for post-trade services. [Az uniós tőzsdék a blokklánc felhasználását tesztelik az értékesítés utáni szolgáltatások terén.] Ledger Insights. https://www.ledgerinsights.com/eu-stock-exchanges-trial-blockchain-post-trade/.

Ledger Insights (2025.04.14.): French, Italian regulators propose changes to DLT Pilot Regime. [A francia és olasz szabályozó hatóságok a megosztott főkönyvi technológia kísérleti rendszerének módosítását javasolják.] https://www.ledgerinsights.com.

LegalNodes (2025): The EU Markets in Crypto-Assets Regulation (MiCA) Explained. [Az Európai Unió kriptoeszközök piacairól szóló (MiCA) rendeletének ismertetése.] *LegalNodes*. https://legalnodes.com/article/mica-regulation-explained.

Li, X. – Jiang, P. – Chen, T. – Luo, X. – Wen, Q. (2020): A survey on the security of blockchain systems. [A blokkláncalapú rendszerek biztonságának vizsgálata.] Future Generation Computer Systems, 107, 841–853. https://doi.org/10.1016/j.future.2020.02.009.

Lovejoy, J. – Brownworth, A. – Virza, M. – Narula N.: Parallelized Architecture for Scalably Executing Smart Contracts (PArSEC). [Skálázható okosszerződés-végrehajtó párhuzamos architektúra (ParSEC).] MIT Digital Currency Initiative (2023). Security and Scalability in Blockchain Systems. [A blokkláncon alapuló rendszerek biztonsága és skálázhatósága.] https://www.dci.mit.edu/projects/parallelized-architecture-for-scalably-executing-smart-contracts-parsec.

Magyar Nemzeti Bank (2023): Diákszéf: a Magyar Nemzeti Bank lakossági digitális jegybankpénz pilot projektje. Budapest: *MNB*. https://www.mnb.hu/letoltes/diakszef-white-paper-final-20250303.pdf.

Mainelli, M. – Milne, A. (2016): The impact and potential of blockchain on the securities transaction lifecycle. [A blokklánc hatása az értékpapír-tranzakciós életciklusra és a kiaknázható lehetőségek.] *The Swift Institute*. https://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL-1.pdf.

MNB (2023): FinTech és digitalizációs jelentés 2023. https://www.mnb.hu/letoltes/final-hu-fintech-e-s-digitaliza-cio-s-jelente-s-2023.pdf.

MNB (2019): FinTech-related regulatory initiatives in Hungary. [Magyarországi szabályozói FinTech kezdeményezések.] *Magyar Nemzeti Bank & CEMLA*. https://www.cemla.org/actividades/2019-final/2019-04-fintech/2019-04-fintech-magyar.pdf

Modern Treasury (2025): What is TARGET Instant Payment Settlement (TIPS)? [Mi a TARGET azonnali elszámolási (TIPS) szolgáltatás?] *Modern Treasury*. https://www.moderntreasury.com/learn/target-instant-payment-settlement.

Nakamoto, S. (2008): Bitcoin: A peer-to-peer electronic cash system. [Bitcoin: a közvetlen elektronikuspénz-forgalmi rendszer.] https://bitcoin.org/bitcoin.pdf.

Nguyen, C.T. – Liu, Y. – Du, H. – Hoang, D.T. – Niyato, D. – Nguyen, D.N. – Mao, S. (2024): Generative AI-enabled blockchain networks: Fundamentals, applications, and case study. [Generatív MI-vel támogatott blokklánchálózatok: alapok, gyakorlati alkalmazás és esettanulmány.] arXiv. https://arxiv.org/abs/2401.15625rapidinnovation.iod197for5662m48.cloudfront.netarxiv.org.

NM Innováció (2022): Blockchain Pilot Projects in Hungary. [Magyarországi kísérleti blokkláncprojektek.] *Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal*. https://nkfih.gov.hu.

Owolabi, O. – Hinneh, E. – Uche, P. – Adeniken, N. – Ohaegbulem, J. – Attakorah, S. – Emi-Johnson, O.G. – Belolisa, C.S. – Nwariaku, H. (2024): Blockchainbased system for secure and efficient cross-border remittances: A potential alternative to SWIFT. [Biztonságos és hatékony határokon átnyúló pénzátutalás blokkláncon alapuló rendszerekkel: kiváltható a SWIFT?] Journal of Software Engineering and Applications, 17, 664–712. https://doi.org/10.4236/jsea.2024.178036.

Pasupuleti, M.K. (2025): Automated smart contracts: AIpowered blockchain technologies for secure and intelligent decentralized governance. [MI-vel vezérelt blokklánc-technológia a biztonságos és intelligens decentralizált irányításban.] ResearchGate. https://www.researchgate.net/publication/390055978_Automated_Smart_Contracts_AIpowered_Blockchain_Technologies_for_Secure_and_Intelligent_Decentralized_Governanceresearchgate.net.

PriFoB Consortium (2023): PriFoB: A privacy-aware fog-enhanced blockchain system for global accreditation and credential verification. [Adatvédelem-központú, ködszámítással kiegészített blokkláncalapú globális akkreditációs és azonosítóadat-ellenőrző rendszer.] arXiv. https://doi.org/10.36227/techrxiv.18319322.v1.

Rapid Innovation (2024.08): Cost-benefit analysis of blockchain for banking: fraud prevention and audit compliance. [Banki blokkláncok költség-haszon elemzése: csalásmegelőzés és auditkövetelményeknek való megfelelés.] *Rapid Innovation*. https://www.rapidinnovation.io/post/blockchain-in-finance-enhancing-security-and-efficiency.

Rapid Innovation (2024): Stellar Blockchain: Cross-Border Payments in 2024. [A Stellar blokklánc: határokon átnyúló fizetés 2024-ben.] *Rapid Innovation*. https://www.rapidinnovation.io/post/cross-border-payments-on-stellar-blockchain.

Rapid Innovation (2024.07.): Top 10 blockchain use cases of zero-knowledge proof: Realtime tracking and regulatory compliance. [10 példa a nem feltáró bizonyítás alkalmazására a blokkláncokban: valós idejű nyomon követés és szabályozási megfelelés.] *Rapid Innovation*. https://www.rapidinnovation.io/post/top-10-blockchain-use-cases-of-zero-knowledge-proofaztec.network.

ResearchGate (2024): Promise of zero-knowledge proofs (ZKPs) for blockchain privacy and security: Opportunities, challenges, and future directions. [A nem feltáró bizonyítási mechanizmusok (ZKP-k) blokkláncon belüli adatvédelmet és biztonságot javító potenciálja: lehetőségek, kihívások és további fejlődési irány.] *ResearchGate*. https://www.researchgate.net/publication/384056745_Promise_of_Zero-Knowledge_Proofs_ZKPs_for_Blockchain_Privacy_and_Security_Opportunities_Challenges_and_Future_Directions.

Reuters (2025.02.06.): Reuters interview with ECB board member Cipollone–digital euro updates. [A Reuters interjúja az EKB igazgatósági tagjával, Piero Cipollonéval – friss hírek a digitális euróról.] *Reuters*. https://www.reuters.com/markets/europe/reuters-interview-with-ecb-board-member-cipollone-2025-02-06/.

Sanction Scanner (2023): Maintaining KYC, AML & CTF compliance across multiple jurisdictions for crypto firms. [A kriptovállalatokra vonatkozó KYC-, AML- és CTF-követelményeknek való megfelelés joghatóságokon átívelő biztosítása.] *Sanction Scanner*. https://kyc-chain.com/maintaining-kyc-aml-amp-ctf-compliance-across-multiple-jurisdictions-for-crypto-firms/ amlwatcher.com+4kyc-chain.com+4sanctionscanner.com+4.

SecurePrivacy (2025.06.): When blockchain meets the right to be forgotten. [A blokklánc és az elfeledtetéshez való jog találkozása.] *SecurePrivacy*. https://secureprivacy.ai/blog/blockchain-immutability-vs-gdpr.

Shei, C. (2025.05.24.). Revolutionizing Cross-Border Payments with Ripple. [A határokon átnyúló fizetést forradalmasító Ripple.] *OneSafe Blog*.https://www.onesafe.io/blog/revolutionizing-cross-border-payments-ripple-stellar.

Shukla, A. – Jirlib, P. – Mishra, A. – Singh, A.K. (2024): An overview of blockchain research and future agenda: Insights from structural topic modelling. [A blokkláncokkal kapcsolatos kutatások és jövőbeli tervek áttekintése: strukturált topikmodellezés alapján levont következtetések.] Journal of Innovation & Knowledge 9(4) (2024. 12.). https://www.elsevier.es/en-

revista-journal-innovation-knowledge-376-articulo-an-overview-blockchain-research-future-S2444569X24001446#:~:text=Blockchain%20is%20a%20disruptive%20technology,on%20various%20aspects%20of%20blockchain.

StandICT.eu (2023): Overview of the European Blockchain Regulatory Sandbox. [Az Európai Blokklánc-szabályozói Tesztkörnyezet áttekintése.] https://www.standict.eu/news/eu-blockchain-regulatory-sandbox-overview.

Sustainability Directory (2023): Smart contract vulnerabilities and resource exhaustion. [Az okosszerződések sebezhetőségei és az erőforrás-kimerítő támadások.] *Energy Sustainability Directory*. https://energy.sustainability-directory.com/term/sustainable-blockchain-security/.

Tapscott, D. – Tapscott, A. (2016): Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. [Blokkláncforradalom: hogyan változtatja meg a bitcoin alaptechnológiája a pénzt, az üzletet és általában a világot.] New York: *Penguin*.

Togggle (2024): How Blockchain Is Transforming KYC Compliance through SSI. [Hogyan formálja át a blokklánc a KYC-követelményeknek való megfelelést az SSI-n keresztül?] https://togggle.io/blog/blockchain-kyc-ssi.

TradeMagazin (2024.06.26.): Bővülő FinTech szektor Magyarországon: tovább javul a digitális fejlettség. *TradeMagazin*. https://trademagazin.hu/hu/bovulo-fintech-szektor-magyarorszagon-tovabb-javul-a-digitalis-fejlettseg/.

Volet (2024): Zero-knowledge proofs: Enhancing blockchain privacy. [Nem feltáró bizonyítás: magasabb szintű adatvédelem a blokkláncon belül.] https://volet.com/blog/post/zero-knowledge-proofs-enhancing-blockchain-privacy-01j7ng5htxtyskdecsyb9k39a7.

Yermack, D. (2017): Corporate governance and blockchains. [Vállalati irányítás és a blokklánc.] Review of Finance, 21(1), 7–31. https://doi.org/10.1093/rof/rfw074.

Zetzsche, D.A. – Buckley, R.P. – Arner, D.W. – Barberis, J.N. (2020): Decentralized Finance (DeFi): Fairness, Efficiency, and Regulation. [Decentralizált pénzügy (DeFi): tisztességeség, hatékonyság és szabályozás.] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194.

Zhang, Y. – Lee, J.H. (2021): A survey on smart contract security: issues, challenges, and solutions. [Az okosszerződések biztonságának vizsgálata: problémák, kihívások és megoldások.] IEEE Access, 9, 1640–1660. https://doi.org/10.1109/ACCESS.2020.3041039.