Huszár Viktor:

KIBERBIZTONSÁG MINT A HADERŐFEJLESZTÉS KIEMELT TERÜLETE: A DECENTRALIZÁCIÓ ÉS A BLOKKLÁNC-TECHNOLÓGIA LEHETŐSÉGEI A KIBERTÉRBEN

DOI: 10.35926/HSZ.2020.3.1

ÖSSZEFOGLALÓ: *A 21. század haderőfejlesztési stratégiáit meghatározza az organikusan fejlődő, digitális technológiai forradalom. A kiberbiztonságról már nem új fogalomként beszélünk, mert a katonai műszaki tudományok és az informatikai tudományok alaptémájává vált. A hálózatokon új technológiák születnek, amelyek digitális forradalmi csomópontokként viselkedve iparágak sokaságát írják újra. A mesterséges intelligencia, a gépi tanulás és gépi látás gyakran használt szakkifejezések, de a bennük rejlő lehetőségek kiaknázásához az elosztottfőkönyv-technológia és a blokklánc-technológia még feltáratlan. A blokkláncalapú megoldások felhasználási területei szerteágazó, eddig nem ismert tudományos kérdéseket vetnek fel. Katonai felhasználás tekintetében a haderőfejlesztés rákényszerül arra, hogy a hibrid hadviselésre sokkal nagyobb hangsúlyt fektessen, a kutatás-fejlesztésre pedig nagyobb anyagi forrást biztosítson. A blokklánc-technológia lehetővé teszi katonai céllal létrehozott, önkéntes, elosztott hálózatok kriptográfiai eljárással történő együttes fellépését, központi és állami ellenőrzés nélkül. A most zajló digitális paradigmaváltás a decentralizáció, a blokklánc-technológia, a gépi tanulás és a mesterséges intelligencia keresztezéséből indul ki.*

KULCSSZAVAK: *mesterséges intelligencia, gépi tanulás, gépi látás, elosztott főkönyv, blokklánc-technológia*

BEVEZETÉS

Egy „diszruptív” technológia nem forradalmian új megoldást jelent, hanem képes egy meglévő paradigmát szintet léptetni.[1] Adattárolási példával élve: a floppyt a CD, a CD-t az USB-flashtároló, majd azt a felhőalapú tárhely váltja. Az információs hálózaton ilyen paradigmaváltás a blokkláncon *(blockchain)* alapuló technológiának köszönhető.[2] A köznyelv a bitcoin kriptovalutával azonosítja a technológiát,[3] de a máig ismeretlen tervező(k) nem egy új digitális pénzt, hanem egy szinkronizálható erőforrás eloszlásra alapuló lehetőséget alkottak meg. A blokklánc ezért egyértelműen olyan diszruptív innováció, amely a keletkezéséig

[1] Joseph L. Bower – Clayton M. Christensen: Disruptive Technologies: Catching the Wave. Harward Business Review, 01–02. 1995, 43–53.

[2] Konstantinos Christidis – Michael Devetsikiotis: Blockchains and smart contracts for the internet of things. IEEE Access 4, 10. 05. 2016, 2292–2303. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408 (Letöltés időpontja: 2020. 04. 07.) DOI: 10.1109/ACCESS.2016.2566339

[3] Satoshi Nakamoto: Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf (Letöltés időpontja: 2020. 04. 07.)

ismert jogi, gazdasági és műszaki tudományos működési rendet alapjaiban megváltoztatja.[4] A technológia rekordsebességgel újratervezésre kényszerítette a monetáris bankrendszertől kezdve a hagyományos pénzügyi világhoz köthető szerződéses tranzakciókat, de hazai viszonylatban rendkívül kevés blokkláncalapú katonai, védelmi igazgatást és haderőfejlesztést érintő tudományos értekezés foglalkozik a katonai lehetőségekkel és veszélyekkel. Nemzetközi kitekintésben már elindult több kutatás-fejlesztési program. A NATO C4ISR[5] és a Pentagon már saját blokkláncprogramokat indított,[6] SBIR 2016.2 néven már biztonságos, decentralizált üzenetküldési applikációt fejlesztenek a haderő számára.

HIBRID HADVISELÉS A KIBERTÉRBEN

A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program[7] felismerte, hogy az új típusú kihívások kiemelt figyelmet igényelnek, és hogy Magyarországnak fel kell építenie, fenn kell tartania és fejlesztenie kell a kibervédelmi képességeit.[8] 2019 júniusában átadták a Magyar Honvédség Kiber Képzési Központját,[9] amely a hibrid haderőfejlesztési stratégiánk egyik legfontosabb alappilléreként szolgál. A kibervédelmi haderőnemi szemlélőség a megfelelő infrastruktúrára és eszközrendszerre támaszkodik, a szentendrei kiberakadémia alapítása teremtette meg azonban a hibrid hadviseléshez szükséges képességet: folyamatos képzésben részt vevő, felkészült, kiképzett katonákat. Az MH Kiber Képzési Központ kettős célt tud szolgálni, mert a kibervédelmi képességfejlesztés és harmonizálás támogatása mellett közvetlenül egy intézményesített haditechnikai kutatás-fejlesztési centrummá is válhat, ami egy ország védelmét alapvetően meghatározza.[10]

A Nemzetbiztonsági Szakszolgálat által működtetett Nemzeti Kibervédelmi Intézet,[11] az ágazati munkacsoportok,[12] az MHP Infokommunikációs és Információvédelmi Csoportfőnökség, valamint az MH Kiber Képzési Központja egymást támogató és kiszolgáló egységet alkotnak. Korábbi tanulmányok felvetik, hogy Magyarországnak olyan informatikai területeken érdemes specializálódnia, mint az elektronika és a szoftverfejlesztés.[13] Aktua-

[4] David Perkins: Blockchains – The great chain of being sure about things. The Economist, 31. 10. 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (Letöltés időpontja: 2020. 04. 07.)

[5] Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance.

[6] Chris Thatcher: Technology's dilemmas: Are we wired to respond? Vanguard, 11. 05. 2015. https://vanguardcanada.com/2015/05/11/technologys-dilemmas-are-we-wired-to-respond/ (Letöltés időpontja: 2020. 01. 19.)

[7] Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program. https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltés időpontja: 2020. 04. 07.)

[8] Uo. 39.

[9] Átadták a Magyar Honvédség Kiber Kiképzési Központját. 2019. 06. 13. https://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat (Letöltés időpontja: 2020. 03. 31.)

[10] Csák Tamás Károly: A haditechnikai kutatás-fejlesztés múltja, jelene, helye, szerepe a magyar haderő fejlesztésében, jövőbeli kihívásai a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében. Honvédségi Szemle, 2019/3., 125–139. https://honvedelem.hu/files/files/115996/hsz_2019_3_beliv_125_139.pdf (Letöltés időpontja: 2020. 04. 07.)

[11] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.). https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (Letöltés időpontja: 2020. 04. 07.)

[12] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről. https://net.jogtar.hu/jogszabaly?docid=a1300484.kor (Letöltés időpontja: 2020. 04. 07.)

[13] Sticz László: A védelmi ipar helye szerepe a katonai képességfejlesztés folyamatában a HM Rt-k és azok privatizációja bemutatása tükrében. Hadmérnök, 2009/3., 375–388. http://hadmernok.hu/2009_3_sticz.pdf (Letöltés időpontja: 2020. 04. 07.)

litását tekintve kitörési pont lehet az új típusú kihívásokkal kapcsolatos kutatás-fejlesztés, humánerő-képesség. Értékarányosan a legkiválóbb honvédelmi befektetés – egyben talán az egyetlen, amiben katonai dimenzióban világszinten versenyképes lehet Magyarország – a kibervédelmi haderőnemi szürkeállomány, amely kormányzati, polgári és katonai interoperabilitást, valamint oktatási, gazdasági és társadalmi értékteremtést eredményez. A hibrid hadviselés biztonságos harmonizációja ezért nemzeti érdekünk.[14]

A hibrid hadviselés színtere megfoghatatlan, „a kibertér varázslatos",[15] az innovációs és digitális forradalom által folyamatos mozgásban tartott élő, lüktető szervezet. A kibertér katonai meghatározása tágabb, mint a kifejezés szokásos, polgári értelmezése. Kijelenthető, hogy a kiberteret hálózati rendszerek és azok fizikai tulajdonságai jellemzik, ahol az adatokat tárolják, cserélik és módosítják.

A 2013-as Nemzeti Kiberbiztonsági Stratégia globálisan összekapcsolt, decentralizált információs rendszerek együtteseként definiálja a kiberteret.[16] A haderőnemi műveleti tartományok meghatározzák a négy lehetséges fizikai tartományt (földi, légi, tengeri és űr),[17] de a kibertérben történő adat- és információs tevékenység mögött meghúzódó szándék továbbra is kulcsfontosságú kérdés maradt, a katonai műszaki tudományos kutatások fontos témája. Olyan új technológiák jelentek meg a hálózatokon, amelyek katonai iparágakat változtathatnak meg. A blokklánc a kiberteret új környezetbe helyezi: az elosztottfőkönyv-technológia (DLT[18]) olyan új innovációkat képes erőforrás-optimalizáltan hasznosítani, mint a mesterséges intelligencia és a gépi látás kombinációja. Az elosztott főkönyv több földrajzi hely, ország vagy intézmény között eloszló (decentralizált), konszenzusalapon többszörözött, megosztott és szinkronizált digitális adatok adatbázisa.[19] Az ilyen főkönyvön futtatható, mély neurális hálózati tanulási képességek potenciális felhasználása számos katonai tudományos kihívást jelent, következésképpen új platformokat hoz létre a kiberműveletekhez.

ÚJ TÍPUSÚ KIHÍVÁSOK A BLOKKLÁNC-TECHNOLÓGIA KIBERTÉRBEN TÖRTÉNŐ ALKALMAZÁSÁBAN

Az elosztott főkönyv legismertebb típusa a blokklánc, ami transzparens és hatékony digitális interakciók rögzített, biztonságos, jóváhagyott, egymás közt megosztott adatbázisa.[20] Minden blokklánc egy elosztott főkönyv, de nem minden elosztott főkönyv blokklánc. A blokklánc-technológia felhasználási területei új típusú katonai kihívások sokaságát vetik

[14] Pálinkás József: Nemzeti érdek a globális kihívások korában. Nemzeti Érdek, Új folyam, 2015/11–12., 93.

[15] Kovács László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018, 19. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (Letöltés időpontja: 2020. 04. 08.)

[16] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (Letöltés időpontja: 2020. 04. 08.)

[17] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány, 2018/1., 113–131. http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf (Letöltés időpontja: 2020. 04. 08.) DOI: 10.17047/HADTUD.2018.28.1.113

[18] Distributed Ledger Technology.

[19] Mark Peplow (ed.): Distributed Ledger Technology: Beyond block chain. UK Government, Office for Science, 01. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Letöltés időpontja: 2020. 04. 08.)

[20] Sinclair Davidson et al.: Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. 22. 07. 2016. https://ssrn.com/abstract=2811995 (Letöltés időpontja: 2020. 03. 23.) DOI: 10.2139/ssrn.2811995

fel. A technológia ugyanis lehetővé teszi decentralizált, önkéntes, elosztott hálózatok kriptográfiai eljárással történő együttes, robusztus fellépését, katonai és állami ellenőrzés nélkül. A technológiát ismertté tévő virtuális fizetőrendszerek kiegészültek az okos szerződésekkel[21] *(Smart Contract)*, amivel olyan tranzakciók bonyolíthatóak le, mint az ingatlan-adásvétel, vagyontárgyak, ingóságok kereskedelme. A kezdeti katonai felhasználási lehetőségek az adatbiztonságra, a titkosított kommunikációs adatátvitelre fókuszáltak.

A decentralizált, blokkláncalapú katonai felhasználás új típusú kihívás a haderőfejlesztésben. A katonai infrastruktúra hatékony felhasználása az erőforrások korlátozott elérhetősége miatt tudományos kutatás-fejlesztési téma, hogy miként lehet decentralizált, központi adattárolás és katonai felügyelet nélküli védelmi igazgatási rendszert létrehozni, egyáltalán életképes gondolat-e egy ilyen rendszer létezése. Egy ilyen elkülönített rendszer mesterséges környezetben, a mesterséges intelligencia által vezérelve milyen öntudat kialakítására lehet képes? Az automatizált, elosztott főkönyvön alapuló katonai felhasználási környezet adatbiztonsága és integritása, a mesterséges intelligenciával kapcsolatos döntéshozatali környezet izolációja a jogosultsági szintek keretrendszerének meghatározásától függhet. A katonai rendszerek és döntéshozatali mechanizmusok központosítottak. A központi adattárolás az egyik fő eredendő oka, hogy az állam- vagy szolgálati titkokat kezelő szervezetek gyakran célponttá válnak.[22] Ezért javasolt a kutatás-fejlesztési kapacitást részben a decentralizált, elosztott rendszerekbe ágyazható megoldások irányába kijelölni.

DECENTRALIZÁLT GÉPI LÁTÁS ÉS A MESTERSÉGES INTELLIGENCIA HASZNÁLATA

A blokkláncalapú mesterséges intelligencia (AI[23]) és a gépi látás lehetséges felhasználása számos katonai műszaki tudományos és jogi kérdést vet fel. A decentralizált hálózatból származó adatok mindig a kibertérből származnak, függetlenül a légi, szárazföldi, tengeri és űradatok műveleti forrásától. Tegyük fel, hogy egy AI által vezérelt drón központi döntés nélkül, a gépi látás bemeneti adatainak feldolgozásával önmaga eldönti, hogy mi legyen a saját maga által kijelölt útvonala, és az AI eldönti azt is, hogy milyen adatokat továbbít egy blokkláncalapú, titkosított rendszeren keresztül, mindezt valós időben. A kibertérben ezen az elosztott rendszeren rögzített adatok összekapcsolják a fizikai területeket azokkal a kognitív folyamatokkal, amelyek tárolására, módosítására vagy cseréjére felhasználják az adatokat.[24] A drón feldolgoz olyan adatot, amit felhasznál a tanulási folyamatához, viszont nem továbbítja és nem tárolja ezt az adatot (pl. egy katonai objektum képe). Az így feldolgozott adat egy olyan mély neurális hálózati tanulási folyamat részévé válik, amiből nem feltétlen lehet következtetni a bemeneti adat – jelen esetben egy katonai objektum – teljes körű információira. Bár a kívánt kiberbiztonsági adatvédelem az adatok decentralizált átvitelével és rögzítésével elérhető egy erre tervezett blokkláncon, de létrejött az ismeretlen, hasznosan pazarolt adat fogalma.

---

[21] Nick Szabo: Formalizing and Securing Relationships on public networks. First Monday, vol. 2, no. 9, 01. 09. 1997. https://firstmonday.org/ojs/index.php/fm/article/view/548/469 (Letöltés időpontja: 2020. 04. 08.) DOI: 10.5210/fm.v2i9.548

[22] Folláth János et al.: Informatikai biztonság és kriptográfia. A veszélyeztetettséget befolyásoló tényezők. Kempelen Farkas Hallgatói Információs Központ, Budapest, 2011. https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch03s04.html (Letöltés időpontja: 2020. 04. 08.)

[23] Artificial Intelligence.

[24] David Fahrenkrug: Cyberspace Defined. The Wright Stuff, 2007.

Az AI-rendszereknek folyamatosan elérhető adatokra és adatcsatornákra van szükségük a gyorsabb tanulási görbék eléréséhez. Az adat beszerzése drága, mivel a katonai információk minősítettek és titkosak, ezért az adatok beszerzése a mesterségesintelligencia-rendszerek katonai alkalmazhatóságához egyre nehezebb, jogi szempontból aggályos és összességében egy nagyon költséges folyamat. Intelligens megoldások léteznek, ahol titkosított adatok ellenőrizetlen vagy nyílt forrású formában elérhető[25] forrásokból szerezhetők be, az adatok általában továbbra is emberi hibáknak vannak kitéve, és másodlagos értékelést és megerősítést igényelnek. A katonai alkalmazásokra vonatkozó adatok még érdekesebbek, mivel az adatbiztonságnak prioritást kell élveznie a védelmi adminisztrációban és a hatóságok napi kommunikációjában. A manuálisan beszerzett adatok felhasználása ütközhet a feldolgozott személyes adatok felhasználásával és a kapcsolódó adatfeldolgozási műveletekkel.[26] Az európai általános adatvédelmi rendelet (GDPR) és más szabályozási politikák ezért korlátozzák az adatfelhasználás forrását.[27] Javasolt a kutatás-fejlesztéseket a közeljövőben a szintetikus adatgyártásra koncentrálni, mert adott helyzetben alkalmazható, közvetlen más méréssel ki nem nyerhető adatokra lesz szükség a hatékonyabb AI-algoritmusok fejlesztéséhez.

Az AI használata a polgári és a katonai alkalmazások esetén sok tudományos kérdést vet fel.[28] A valós idejű eredmények számítási műveletei komoly infrastruktúrát igényelnek, mert a szűkös erőforrások költségessé tehetik a számításokat. A tudományos kihívás kiterjed az ilyen rendszer mesterséges elszigeteltségére és a gépi tanulás vagy a programozott AI öntudatra ébredésének katonai kockázataira.

Gyakorlati nemzetközi példák iránymutatóak a Zrínyi 2026 programnak is. Az Amerikai Egyesült Államokban a Maven Project[29] az Algorithmic Warfare Cross-Functional Team (AWCFT) program része, a célja pedig az amerikai haderő versenyelőnyének a megtartása gépi tanulás és gépi látás használatával. A Pentagonnál felismerték, hogy nem képesek emberi kapacitással feldolgozni a beszerzett adatmennyiséget, ezért a gépi tanulás segítségével dolgozzák fel, hasznosítják és osztják el (Process–Exploit–Disseminate)[30] a drónok által közepes magasságból készített digitális fotókat és videókat (Mid-Altitude Full Motion Video). Az AI alkalmazásával adatcímkézés, algoritmikus szelektálás érhető el, ami felgyorsítja a katonai döntési mechanizmust. A rendszer hatékonysága a gépi tanulásnak köszönhetően

---

[25] Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság, 2017/1., 4. http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf (Letöltés időpontja: 2020. 04. 08.)

[26] Péterfalvi Attila: A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban. 2017. 07. 18. https://docplayer.hu/68689343-A-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-allasfoglalasa-a-blokklanc-blockchain-technologia-adatvedelmi-osszefuggeseivel-kapcsolatban.html (Letöltés időpontja: 2020. 04. 08.)

[27] Leigh Cuen: Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report. CoinDesk, 27. 03. 2019. www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report (Letöltés időpontja: 2019. 05. 15.)

[28] Porkoláb Imre – Négyesi Imre: A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben. Honvédségi Szemle, 2019/5., 6. https://honvedelem.hu/wp-content/uploads/2019/09/HSz-2019-5_03-20_Porkol%C3%A1b-Imre_A-mesters%C3%A9ges-intelligencia.pdf (Letöltés időpontja: 2020. 04. 08.)

[29] Berta Sándor: Maven projekt – a Google könnyen pótolható. Sg.hu, 2018. 06. 06. https://sg.hu/cikkek/it-tech/131574/maven-projekt-a-google-konnyen-potolhato (Letöltés időpontja: 2019. 05. 15.)

[30] Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven). Department of Defense, USA, 26. 04. 2017. https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf (Letöltés időpontja: 2020. 03. 25.)

egyre jobb lesz a tárgyak felismerésében és osztályozásában (címkézésében). Az AI ebben már évek óta hatékonyabb az embereknél.

Jelenlegi becslések alapján több mint 100 ország rendelkezik katonai drónokkal, ebből 20 ország fegyveres drónokat is használt már – nem feltétlenül államhoz köthető szervezetek által. A pilóta nélküli repülőrendszerek (UAS[31]) a robotika szempontjából sokszor nem túl kifinomultak még, és szinte mind távolról vezéreltek. Az autonómia egyre inkább megjelenik a különböző járművek kezelésében. Ilyen például a G-NIUS vállalat által kifejlesztett Guardium nevű, személyzet nélküli földi jármű (UGV[32]), amelyet a gázai határ mentén alkalmaznak az izraeliek katonai feladatokra. A jármű önvezető, de a rajta található fegyvereket távolról emberek kezelik még. A blokkláncalapú AI-alkalmazásokat a katonai feladatok esetén egyszerűen be lehet építeni fegyverrendszerekbe,[33] de akár civil alkalmazásokba is.[34] Az egészségügyben számos példát láthatunk már erre, például pontosabb EKG-eredmények előrejelzése, elemzése.[35]

Egy bármihez tervezett kamerarendszer működtethető lehet blokkláncalapon, gépi látásra támaszkodó AI bevonásával. Ehhez a gépi látás fejlesztéseit szükséges felhasználni a képfelismerés és képelemzés alkalmazásával, amelyek egyaránt nagy számítási teljesítményt igényelnek.[36] A jelenlegi képanalízis-módszertanok gyakran lassúak és nem működnek valós időben. A gyanús események kiváltó okai könnyen csoportosíthatóak (füst, fegyver stb.), így határsértések, terrorcselekmények vagy más bűncselekmények megelőzése és egyéb nemzetbiztonsági feladatok ellátása is hatékonyabbá válhat. A bűncselekmények és a körözött személyek azonosítása pedig nem igényelne annyi időt és erőforrást.

Az energiaellátás biztosítása még kutatandó terület. A blokkláncalapú rendszerek világszinten kiugró áramfogyasztásra képesek. A bitcoinbányászat erre kiváló példa, az összes bányász számítógép együttes számítási kapacitása 2013-ban meghaladta az akkori 500 legnagyobb szuperszámítógép kapacitásának 250-szeresét,[37] a bányász közösség összesített fogyasztása pedig 2017-ben 159 ország átlagos éves villamos energiaszükségletével egyezett meg.[38] Számos technológia viszont kombinálható a szinergia és a legjobb áramfelvételi teljesítmény érdekében. A versenyképes gépi látáson alapuló megoldások azok lesznek, amelyeknek a jelenlegi drága hardver- és erőforrásigénye csökken. Az önjáró autók fejlesztését segítő elkülönített autópályák és az 5G hálózati tesztek eddig szintén költséges gépi

[31] Unmanned Aerial System.

[32] Unmanned Ground Vehicle.

[33] Paul Scharre: Killer Robots and Autonomous Weapons With Paul Scharre. Council on Foreign Relations, 01. 06. 2018. www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre (Letöltés időpontja: 2020. 03. 12.)

[34] Négyesi Imre: Die Vision der tragbaren Informationstechnologiegerate. Hadmérnök, 2008/4., 173–179. http://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2107/2008_4_negyesi.pdf?sequence=1&isAllowed=y (Letöltés időpontja: 2020. 04. 10.)

[35] Donna Lu: AI can predict if you'll die soon – but we've no idea how it works. New Scientist, 11. 11. 2019. https://www.newscientist.com/article/2222907-ai-can-predict-if-youll-die-soon-but-weve-no-idea-how-it-works/#ixzz64yUWdOkn (Letöltés időpontja: 2020. 03. 12.)

[36] Reuven Cohen: Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined! Forbes, 28. 11. 2013. https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#4a8d4b6b6e5e (Letöltés időpontja: 2020. 04. 10.)

[37] Uo.

[38] Oscar Williams-Grut: The electricity used to mine bitcoin this year is bigger than the annual usage of 159 countries. Business Insider, 26. 11. 2017. https://uk.news.yahoo.com/electricity-used-mine-bitcoin-bigger-080700148.html (Letöltés időpontja: 2020. 03. 29.)

látáson alapuló kutatás-fejlesztési eredményekről számoltak be.[39] A decentralizált és elosztott hálózati megoldások gazdasági szempontok miatt nyernek majd teret, de térhódításukkal új kibervédelmi dimenziók fognak nyílni. A hálózati hadviselés, az elektronikai hadviselés és számítógépes hálózati műveletek a haderőfejlesztés – kiberbiztonsággal kapcsolatos – területeinek főbb kutatás-fejlesztési témái lesznek.[40]

A BLOCKCHAIN LÁNCOLAT

A *blockchain* („blokkok lánca") egy elosztott adattárolási napló, de gyakran elosztott főkönyvként vagy elosztott adatbázisként hivatkoznak rá. Az adatbázis sorba rendezett bejegyzések növekvő blokkokba szervezett listáját tárolja. Az egyes blokkok minden, a blokkláncot tároló csomóponton tartalmaznak egy hivatkozást a megelőző blokkra is. A blokkláncot alkalmazó rendszerek alapvető jellemzője az összes rendezett bejegyzések blokklánc csomópontjainak tárolása, és az aktuális állapotról konszenzusalgoritmus segítségével állapodnak meg.[41] Az elosztott adattárolás ilyen megközelítését a bitcoin elosztott kriptovaluta fizetési rendszere tette közismertté és népszerűvé, ma már azonban számtalan olyan rendszer létezik, illetve áll fejlesztés alatt, amelyek ugyanezt az alapelvet követik, de céljukban és kulcsfontosságú műszaki elemeikben a bitcointól alapvetően különböznek. Ezekre a rendszerekre együtt a DLT-családba tartozó blokklánctípusú technológiaként szoktunk hivatkozni.[42]

Az eddigi adatok alapján okkal jelenthető ki,[43] hogy a blokklánc-technológia lesz a következő technológiai forradalom,[44] amely legalább olyan hatással lesz az életünkre, mint annak idején az internet volt.[45] A blokklánc jelentőségét – elosztott hibatűrő működés, meghamisíthatatlan tranzakciók – szinte minden iparág felismerte, és folyamatban vannak azok a kutatások, hogy esetlegesen hogyan lehet különböző létező rendszereket részben vagy egészben átültetni blokkláncalapra.

---

[39] Mintegy 40 milliárd forintból épül járműipari tesztpálya Zalaegerszegen. Autószektor, 2016. 05. 12. www.autoszektor.hu/hu/content/mintegy-40-milliard-forintbol-epul-jarmuipari-tesztpalya-zalaegerszegen (Letöltés időpontja: 2019. 01. 15.)

[40] Victoria Adams: Why Military Blockchain is Critical in the Age of Cyber Warfare. ConsenSys Media, 05. 05. 2019. https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619 (Letöltés időpontja: 2019. 12. 13.)

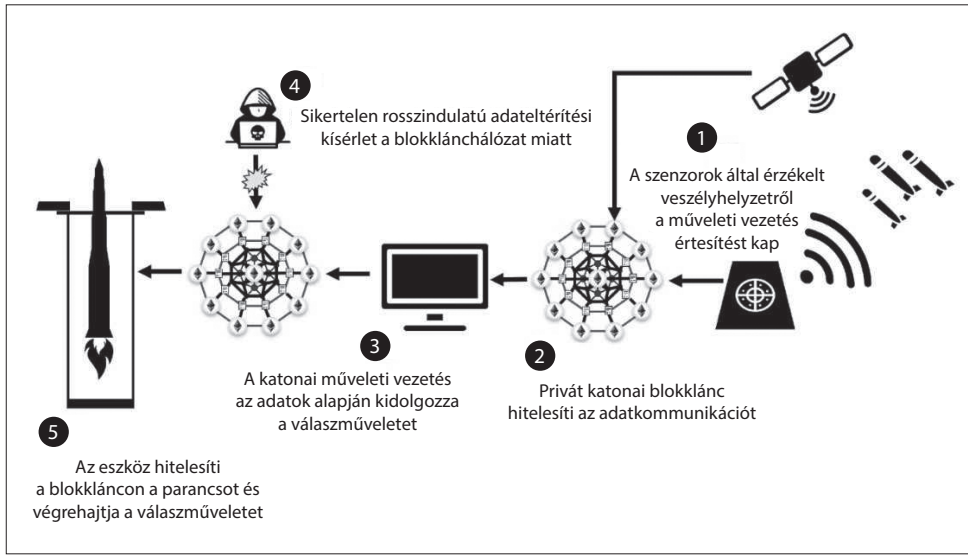
[41] Nir Kshetri: Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy 41 (10), 11. 2017, 1027–1038. https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483 (Letöltés időpontja: 2020. 04. 10.) DOI: 10.1016/j.telpol.2017.09.003

[42] Tareq Ahram et al.: Blockchain technology innovations. 2017 IEEE Technology and Engineering Management Society Conference. Temscon, 06. 2017, 137–141. https://www.researchgate.net/publication/318894127_Blockchain_technology_innovations (Letöltés időpontja: 2020. 04. 10.) DOI: 10.1109/TEMSCON.2017.7998367

[43] Jong-Hyouk Lee – Marc Pilkington: How the blockchain revolution will reshape the consumer electronics industry. IEEE Consumer Electr, Mag. 6 (3), 07. 2017, 19–23. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7948864 (Letöltés időpontja: 2020. 04. 10.)

[44] Don Tapscott – Alex Tapscott: Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin Random House, New York, 2016.

[45] Négyesi Imre: Changing Role of the Internet in the Light of an International Conference. Hadmérnök, 2008/3., 147–153. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2106/2008_3_negyesi.pdf?sequence=1&isAllowed=y (Letöltés időpontja: 2020. 04. 10.)



1. ábra *Blokkláncalapú védelmi mechanizmus*[46]

Érdemes a blokkláncalapú technológiákra úgy tekintenünk, mint amelyek egy elosztott *„ledger"*-t, magyarul főkönyvet valósítanak meg.[47] A blokklánc-technológiák kontextusában a főkönyv egy bejegyzéstároló, ahol a bejegyzések bármit tárolhatnak, és nem lehet őket módosítani, miután a tárolóba kerültek. Ennek a főkönyvnek egyébként lehet szűken vett „főkönyv" szemantikája is a blokklánc-technológiáktól, illetve annak alkalmazásától függően, de ez közel sem törvényszerű. A blokklánc-technológiák oly módon valósítanak meg elosztott főkönyvet, hogy azt szinkronban tartják az elosztott hálózat csomópontjai között – melyek között akár jelentős geográfiai távolság is lehet, illetve különböző vállalatok birtokában is lehetnek, ezáltal mindegyik csomópontnak megvan a saját egyenértékű másolata a főkönyvről. Bármilyen változtatás, ami a főkönyvön történik, és amiben a hálózat fennmaradó csomópontjai is megegyeznek, a többi csomópont főkönyvében is perceken, sőt egyes megoldásokban másodperceken belül megjelenik, és rajtuk keresztül a bejegyzésekben tárolt információkhoz hozzá lehet férni bármilyen megbízható központi felügyeleti szerv és annak belső folyamatai, szabályai bevonása nélkül.[48]

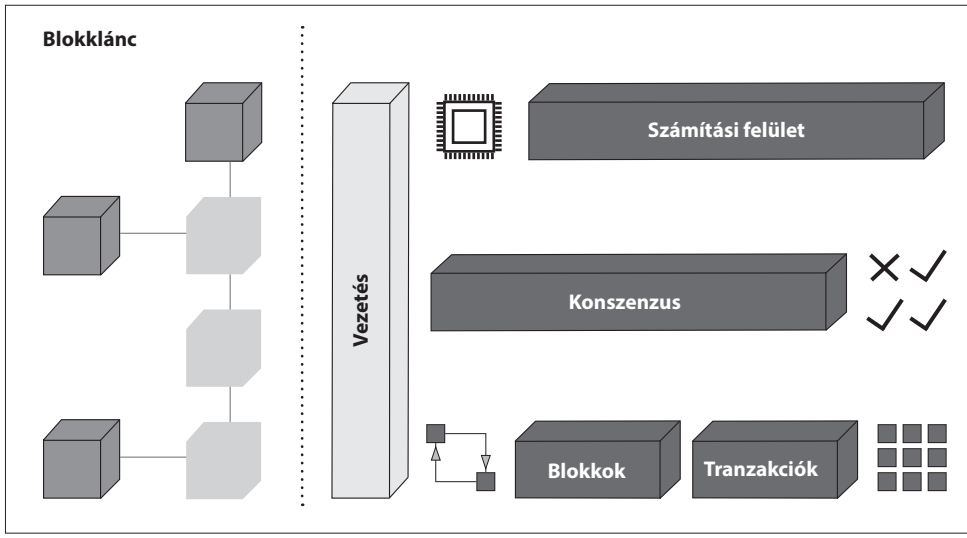
A főkönyv karbantartását valamilyen megegyezési algoritmus (konszenzus) alapján az elosztott hálózat csomópontjai végzik, amelyek a tároláshoz és a tranzakciók ellenőrzéséhez erősen használják a kriptográfiát. Így a hálózat még nagyszámú hibás csomópont esetén is működőképes maradhat, feltéve, ha a hibás csomópontok száma nem éri el a maximálisan

[46] Wendel Minnick: Computer Attacks Form China Leave Many Questions. Defense News, 13. 08. 2017., 13. http://minnickarticles.blogspot.com/2009/09/computer-attacks-from-china-leave-many.html (Letöltés időpontja: 2020. 04. 10.)

[47] Hossein Kakavand et al.: The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 (Letöltés időpontja: 2020. 04. 10.) DOI: 10.2139/ssrn.2849251

[48] Andrea Pinna – Wiebe Ruttenberg: Distributed ledger technologies in securities post-trading revolution or evolution? ECB Occasional Paper, no. 172., 28. 04. 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770340 (Letöltés időpontja: 2020. 04. 10.)

megengedett hibás csomópontok számát. Elosztott konszenzusalgoritmusból, általánosabb értelemben elosztott konszenzusprotokollból az informatika rengeteget ismer és alkalmaz. Egy adott alkalmazási kontextusban a konszenzusprotokoll kiválasztását olyan faktorok befolyásolják, mint például a feltételezett hibamódok, a rendszer maximális mérete, a konszenzussal kapcsolatos válaszidő és szinkronitási követelmények. Ennek megfelelően nem meglepő, hogy a különböző blokklánc-technológiák is számos különböző konszenzusprotokollt alkalmaznak. Közös azonban a blokklánc-technológiákban, hogy az elosztott konszenzus problémáját valamilyen protokoll segítségével kezelik.



2. ábra *A blokklánc-architektúra felépítése*[49]

A blokklánc egy tranzakciónapló, egy elosztott főkönyv (de szokták *journal*nak is hívni), bejegyzéseit szigorúan időrendi sorrendben, tömbösítve tároljuk a blokkokban. Ezeket a blokkokat időbélyeggel látják el, és egy, a protokollból választott titkosítási eljárással azonosítjuk. Minden blokk tartalmaz egy referenciát, amely az őt megelőző blokkra mutat. Így a blokkok egy visszafelé láncolt szekvenciába, láncolatba, azaz valójában egy listába szerveződnek, amelyet legrosszabb esetben az első blokktól feldolgozva egyértelműen meghatározható az elosztott adatbázis mindenkori állapota – természetesen abban az esetben, amikor a csomópontok között konszenzus áll fenn a blokklánccal kapcsolatban. Ha a konszenzusprotokoll „elég erős", úgy egy korábbi művelet megváltoztatására, törlésére nincs lehetőség úgy, hogy a rendszer elég sok csomópontjával kapcsolatban álló kliens ezt ne vegye észre.

A blokklánc-technológia decentralizált jellege (2. ábra) azt jelenti, hogy nem támaszkodik központi entitásra, ellenőrzési pontra. A hatóság hiánya tisztességesebbé és biztonságosabbá teszi a rendszert. Az adatok blokkláncra történő rögzítésének módja tükrözi

[49] Fran Casino et al.: A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, Volume 36, 03. 2019, 55–81. https://www.sciencedirect.com/science/article/pii/S0736585318306324 (Letöltés időpontja: 2020. 04. 10.)

a decentralizáció értékét.[50] Ahelyett, hogy egy központi hatóságra támaszkodnánk, hogy biztonságosan tranzakcióba lépjen a többi felhasználóval, a blokklánc innovatív konszenzusprotokollokat használ a csomópontok hálózatán, hogy hitelesítse a tranzakciókat, és megvesztegethetetlen módon rögzítse az adatokat. Így a blokkláncot nem egy központi adatkezelő tárolja, hanem azt gyakorlatilag valamennyi felhasználó tárolja saját számítógépén.

INTEGRITÁS A KIBERBIZTONSÁGBAN

A kiberbiztonság a blokklánc-technológia alacsony költségű, de magas hozzáadott értékkel rendelkező lehetséges alkalmazási területe. A blokklánc-technológia olyan szabad erőforrásokat képes valós idejű számítási teljesítménnyé konvertálni, amelyek jelenleg kihasználatlanok. A technológia alapja, hogy a titkosított, digitális tranzakciók a blokkláncháló zat más csomópontjaiba eljutnak. Konszenzusalgoritmus alapján a tranzakciók, digitális események olyan elosztott adatbázisokba kerülnek, amelyeket külső fél soha nem változtathat meg. Ezáltal a tranzakció hiteles marad, a minőségi és hitelesített adat következménye a logikai adatintegritás.

A blokklánc megalapozhatja egy számítógépes védelem perimetrikus biztonsági stratégiáját (BDP[51]).[52] A szoftveresen felhúzott védelmi fal (SDP[53]) kombinálható a blokklánccal, így nemcsak maga a védelmi vonal, hanem minden érintett eszköz, felhasználó és információ folyamatosan megfigyelhető és hitelesíthető. A blokklánc kiberbiztonsági gyűrű digitális aláírást tud alkalmazni minden hálózati tagnál, ezáltal a sima szoftveres megoldásnál biztonságosabb, akár katonai alkalmazásra alkalmas rendszer alapjaként is bevethető.

A modern fegyverrendszerek elosztott és decentralizált hálózati adminisztrációval fognak rendelkezni, leváltva a hagyományos, központilag vezérelt katonai rendszereket.[54] A különböző típusú fegyvernemek közötti harmonizációhoz jelenleg rendszerintegrált, katonai központi irányítórendszereket alkalmaznak. A központosítás a rendszer sérülékenységi pontja, mert ha a központi agyat kikapcsolják vagy lekapcsolják a rendszerről, a vezérlés megszűnik. A blokklánc előnye, hogy decentralizált, nincs központi agy, megfelelően felépített blokklánc esetén nincs sérülékenységi pont. Arról lehet hallani, hogy a kriptovalutát (bitcoin) ellopták emberi mulasztás miatt, de arról nem, hogy feltörték volna a blokklánc elliptikus görbén (ECDSA[55]) alapuló titkosított aláírását.[56]

---

[50] Vitalik Buterin: A next-generation smart contract and decentralized application platform. Ethereum White Paper, 2014, 6. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (Letöltés időpontja: 2020. 04. 10.)

[51] Blockchain Defined Perimeter.

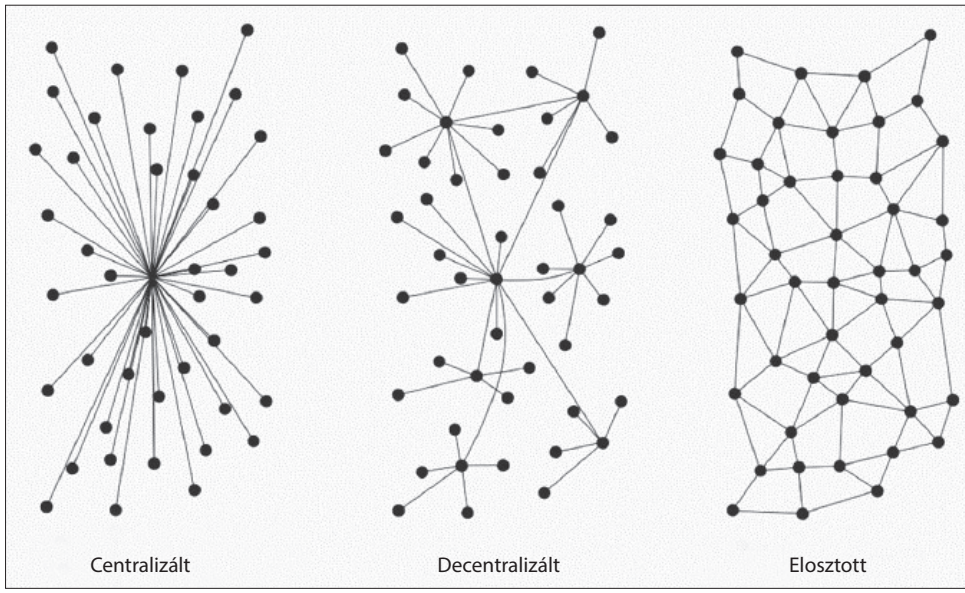
[52] Floyd D. Costa – Narayan Neelakantan: Blockchain Defined Perimeter. https://www.academia.edu/32818182/Blockchain_Defined_Perimeter (Letöltés időpontja: 2020. 03. 08.)

[53] Software Defined Perimeter.

[54] MaidSafe: Evolving Terminology with Evolved Technology: Decentralized versus Distributed. Medium, 05. 02. 2015. https://medium.com/safenetwork/evolving-terminology-with-evolved-technology-decentralized-versus-distributed-7f8b4c9eacb (Letöltés időpontja: 2020. 03. 20.)

[55] Elliptic Curve Digital Signature Algorithm.

[56] Benjamin K. Kikwai: Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions. International Journal of Scientific and Research Publications, Volume 7, Issue 11, 11. 2017, 135. http://www.ijsrp.org/research-paper-1117/ijsrp-p7117.pdf (Letöltés időpontja: 2020. 04. 10.)



3. ábra *A központi, decentralizált és elosztott rendszer logikai felépítése*[57]

A haderőfejlesztés kutatás-fejlesztési iránya a kiberbiztonságot meghatározó új típusú kihívások kezelése lesz. A blokklánc adatbázis-architektúráját alkalmazva a következő generációs harci rendszerek a decentralizált döntési mechanizmusokon alapulhatnak. Az emberi hozzáadott érték nem a végső döntéshozatal, hanem a döntési képességre való tanítás mélysége lesz. Egy decentralizált rendszer gyorsabban tud dönteni a tűzszabályozásról, javítva a túlélési esélyt. A hibázási lehetőség kiszűrhető, ha a különféle fegyverrendszerekbe betöltött mesterséges intelligenciával dolgozó processzorok összehangolhatják tevékenységüket és ellenőrizhetik az adatok hitelességét. A 20. századi haderő még drága számítási teljesítménynyel, de olcsón beszerezhető adatokkal dolgozott. A központosított döntéshozatal indokolt volt. Az új kihívások azért jelentek meg, mert a feldolgozási teljesítmény költséghatékony lett, de maga az adat sokkal drágább. A 21. századi haderőnemek blokklánc-technológiát fognak használni.[58]

ÖSSZEGZÉS

Az elosztottfőkönyv-technológia (DLT) és a blokklánc-technológia a haderőfejlesztés kiemelt területei lesznek. Nemzetközi példák bizonyítják, hogy a decentralizált katonai megoldások felelősek a kiberbiztonsági paradigmaváltásért. Új kiberműveleti dimenziók, katonai műszaki fogalmak születnek a decentralizált digitális interakciók következményeként. Az elosztott főkönyv megbízható, transzparens, titkosított, típusától függően konszenzus alakul ki a hálózaton a használók között. A DLT átlátható, ezért biztonságos, a kriptográfiai megoldások biztosítják, hogy hálózati manipuláció nem lehetséges. A DLT legismertebb típusa

[57] Paul Baran: On Distributed Communications. Memorandum, 1964. RM-3420-PR.

[58] Arleigh Burke-Class (Aegis) Destroyer. Naval Technology. www.naval-technology.com/projects/burke/ (Letöltés időpontja: 2020. 02. 07.)

a blokklánc. A blokklánchálózatok hibatűrők, a megbízható csomópontokat összehangolják, míg a megbízhatatlanokat eldobják. A Zrínyi 2026 kutatás-fejlesztési programjait érdemes speciális képességek kifejlesztésére összpontosítani, mert Magyarország ebben nemzetközileg is versenyképes lehet. A haderőfejlesztés elengedhetetlen és egyik legjobb befektetése lehet az új típusú kibervédelmi kihívások kutatás-fejlesztési támogatása.

Az értekezésemben ismertetett intézményi háttér képes biztosítani a kiberműveleti szellemi képesség fejlesztését, fenntartását és képzését magas szinten lehetővé tevő infrastruktúrát és eszközrendszert. Annak ellenben kevés az esélye, hogy Magyarország fegyver- vagy katonai járműgyártással világviszonylatban az élvonalba tudjon jutni és maradni: ehhez rengeteg pénz és szakértelem, továbbá zárt adatokhoz való hozzáférés lenne szükséges. Aránytalan megterhelést jelentene a haderőfejlesztési reformnak, és nem eredményezne különleges specializálódási lehetőséget globálisan.

A decentralizáció és a blokklánc katonai fejlesztési lehetőségei további komoly és mélyebb kutatást igényelnek. A technológia teljes felhasználási köre folyamatosan változik, ezért javasolt a szerves szakértelem fejlesztése, a nemzetközi eredmények monitorozása és feldolgozása. A mesterséges intelligencia és a gépi látás a polgári-katonai partnerkapcsolati lehetőségeket összekötheti, eredményeként szakmai együttműködések alakulhatnak ki a DLT és blokkláncalapú technológiák fejlesztése érdekében. Magyarország már most is az egyik vezető ország a gépi tanulás, a gépi látás és a mesterséges intelligencia alkalmazásában. A Zrínyi 2026 sikertörténete lehet a kiberbiztonsággal kapcsolatos katonai képesség specializálódása.

A blokklánc hatékony katonai alkalmazása további kutatások témája lesz. Az állami informatikai apparátusok jelenlegi kihasználtsága, bekapcsolhatósága egy elosztott főkönyvi infrastruktúrába technikai és kiberbiztonsági kérdéseket vet fel. Nemzetközi gyakorlati példák mutatják, hogy az emberi kapacitást próbára tevő adatelemzési feladatoknál a gépi tanulás, az AI hálózatalapú alkalmazása a kijelölt kutatási irány. Magyarország a hibrid hadviselésben regionális versenyelőnyre tehet szert, kibervédelmi és támadóképességeket fejleszthet, valamint nemzetközileg is jelentősen mérhető tudástőkét, tudományos, intézményesített informatikai kutatói műhelyeket hozhat létre. A kormányzati szabad informatikai számítási kapacitásokat erőforrás szempontjából hatékony módon decentralizált rendszerekbe lehet csoportosítani. Egy ilyen decentralizált, céljaiban definiált rendszer biztonságos működés mellett képes lehet arra, amire az ember nem: hogy pontosan, gyorsan, hibamentesen hozzon döntéseket és készítsen elő megalapozott, tárgyilagos katonai vezetői döntési pontokat.

FELHASZNÁLT IRODALOM

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. https://20102014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf

2013. évi L. törvény (Ibtv.) az állami és önkormányzati szervek elektronikus információbiztonságáról. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről. https://net.jogtar.hu/jogszabaly?docid=a1300484.kor

Adams, Victoria: *Why Military Blockchain is Critical in the Age of Cyber Warfare*. ConsenSys Media, 05. 05. 2019. https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

Ahram, Tareq – Sargolzaei, Arman – Sargolzaei, Saman – Daniels, Jeff: *Blockchain technology innovations*. 2017 IEEE Technology and Engineering Management Society Conference. Temscon, 06. 2017, 137–141. https://www.researchgate.net/publication/318894127_Blockchain_technology_innovations DOI: 10.1109/TEMSCON.2017.7998367

Arleigh Burke-Class (Aegis) Destroyer. Naval Technology. www.naval-technology.com/projects/burke/

Átadták a Magyar Honvédség Kiber Kiképzési Központját. 2019. 06. 13. https://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat

Berta Sándor: *Maven projekt – a Google könnyen pótolható.* Sg.hu, 2018. 06. 06. https://sg.hu/cikkek/it-tech/131574/maven-projekt-a-google-konnyen-potolhato

Bower, Joseph L. – Christensen, Clayton M.: *Disruptive Technologies: Catching the Wave*. Harward Business Review, 01–02. 1995, 43–53.

Buterin, Vitalik: *A next-generation smart contract and decentralized application platform*. Ethereum White Paper, 2014. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Casino, Fran – Dasaklis, Thomas K. – Patsakis, Constantinos: *A systematic literature review of blockchain-based applications: Current status, classification and open issues.* Telematics and Informatics, Volume 36, 03. 2019, 55–81. https://www.sciencedirect.com/science/article/pii/S0736585318306324 DOI: 10.1016/j.tele.2018.11.006

Christidis, Konstantinos – Devetsikiotis, Michael: *Blockchains and smart contracts for the internet of things.* IEEE Access 4, 10. 05. 2016., 2292–2303. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408 DOI: 10.1109/ACCESS.2016.2566339

Cohen, Reuven: Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined! Forbes, 28. 11. 2013. https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#4a8d4b6b6e5e

Costa, Floyd D. – Neelakantan, Narayan: *Blockchain Defined Perimeter.* https://www.academia.edu/32818182/Blockchain_Defined_Perimeter

Cuen, Leigh: *Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report*. CoinDesk, 27. 03. 2019. www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report

Csák Tamás Károly: *A haditechnikai kutatás-fejlesztés múltja, jelene, helye, szerepe a magyar haderő fejlesztésében, jövőbeli kihívásai a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében.* Honvédségi Szemle, 2019/3., 125–139. https://honvedelem.hu/files/files/115996/hsz_2019_3_beliv_125_139.pdf

Davidson, Sinclair – De Filippi, Primavera – Potts, Jason: *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology*. 22. 07. 2016. https://ssrn.com/abstract=2811995 DOI: 10.2139/ssrn.2811995

Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven). Department of Defense, USA, 26. 04. 2017. https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf

David Fahrenkrug: *Cyberspace Defined*. The Wright Stuff, 2007.

Folláth János – Huszti Andrea – Pethő Attila: *Informatikai biztonság és kriptográfia. A veszélyeztetettséget befolyásoló tényezők.* Kempelen Farkas Hallgatói Információs Központ, Budapest, 2011. https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch03s04.html

Kakavand, Hossein – Kost De Sevres, Nicolette – Chilton, Bart: *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 DOI: 10.2139/ssrn.2849251

Kikwai, Benjamin K.: *Elliptic Curve Digital Signatures and Their Application in the Bitcoin Cryptocurrency Transactions*. International Journal of Scientific and Research Publications, Volume 7, Issue 11, 11. 2017. http://www.ijsrp.org/research-paper-1117/ijsrp-p7117.pdf

Kovács László: *A kibertér védelme*. Dialóg Campus Kiadó, Budapest, 2018. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf

Kovács László – Krasznay Csaba: *Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint.* Nemzet és Biztonság, 2017/1. http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf

Kshetri, Nir: *Blockchain's roles in strengthening cybersecurity and protecting privacy*. Telecommun. Policy 41 (10), 11. 2017, 1027–1038. https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483 DOI: https://doi.org/10.1016/j.telpol.2017.09.003

Lee, Jong-Hyouk – Pilkington, Marc: *How the blockchain revolution will reshape the consumer electronics industry.* IEEE Consumer Electr, Mag. 6 (3), 07. 2017, 19–23. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7948864

Lu, Donna: *AI can predict if you'll die soon – but we've no idea how it works*. New Scientist, 11. 11. 2019. https://www.newscientist.com/article/2222907-ai-can-predict-if-youll-die-soon-but-weve-no-idea-how-it-works/#ixzz64yUWdOkn

MaidSafe: Evolving Terminology with Evolved Technology: Decentralized versus Distributed. Medium, 05. 02. 2015. https://medium.com/safenetwork/evolving-terminology-with-evolved-technology-decentralized-versus-distributed-7f8b4c9eacb

Minnick, Wendel: *Computer Attacks Form China Leave Many Questions.* Defense News, 13. 08. 2017. http://minnickarticles.blogspot.com/2009/09/computer-attacks-from-china-leave-many.html

Mintegy 40 milliárd forintból épül járműipari tesztpálya Zalaegerszegen. Autószektor, 2016. 05. 12. www.autoszektor.hu/hu/content/mintegy-40-milliard-forintbol-epul-jarmuipari-tesztpalya-zalaegerszegen

Munk Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*. Hadtudomány, 2018/1., 113–131. http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf DOI: 10.17047/HADTUD.2018.28.1.113

Nakamoto, Satoshi: *Bitcoin: A peer-to-peer electronic cash system*. 2008. https://bitcoin.org/bitcoin.pdf

Négyesi Imre: *Changing Role of the Internet in the Light of an International Conference.* Hadmérnök, 2008/3., 147–153. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2106/2008_3_negyesi.pdf?sequence=1&isAllowed=y

Négyesi Imre: *Die Vision der tragbaren Informationstechnologiegerate.* Hadmérnök, 2008/4., 173–179. http://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2107/2008_4_negyesi.pdf?sequence=1&isAllowed=y

Pálinkás József: *Nemzeti érdek a globális kihívások korában*. Nemzeti Érdek, Új folyam, 2015/11–12.

Peplow, Mark (ed.): *Distributed Ledger Technology: Beyond block chain.* UK Government, Office for Science, 01. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Perkins, David: *Blockchains – The great chain of being sure about things.* The Economist, 31. 10. 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

Péterfalvi Attila: *A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban.* 2017. 07. 18. https://

docplayer.hu/68689343-A-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-allasfoglalasa-a-blokklanc-blockchain-technologia-adatvedelmi-osszefuggeseivel-kapcsolatban.html

Pinna, Andrea – Ruttenberg, Wiebe: *Distributed ledger technologies in securities post-trading revolution or evolution?* ECB Occasional Paper, no. 172, 28. 04. 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770340

Porkoláb Imre – Négyesi Imre: *A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben.* Honvédségi Szemle, 2019/5. https://honvedelem.hu/wp-content/uploads/2019/09/HSz-2019-5_03-20_Porkol%C3%A1b-Imre_A-mesters%C3%A9ges-intelligencia.pdf

Scharre, Paul: *Killer Robots and Autonomous Weapons With Paul Scharre*. Council on Foreign Relations, 01. 06. 2018. www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre

Sticz László: *A védelmi ipar helye szerepe a katonai képességfejlesztés folyamatában a HM Rt-k és azok privatizációja bemutatása tükrében*. Hadmérnök, 2009/3., 375–388. http://hadmernok.hu/2009_3_sticz.pdf

Szabo, Nick: *Formalizing and Securing Relationships on public networks*. First Monday, vol. 2, no. 9, 01. 09. 1997. https://firstmonday.org/ojs/index.php/fm/article/view/548/469 DOI: 10.5210/fm.v2i9.548

Tapscott, Don – Tapscott, Alex: *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin Random House, New York, 2016.

Thatcher, Chris: *Technology's dilemmas: Are we wired to respond?* Vanguard, 11. 05. 2015. https://vanguardcanada.com/2015/05/11/technologys-dilemmas-are-we-wired-to-respond/

Williams-Grut, Oscar: *The electricity used to mine bitcoin this year is bigger than the annual usage of 159 countries.* Business Insider, 26. 11. 2017. https://uk.news.yahoo.com/electricity-used-mine-bitcoin-bigger-080700148.html

Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program. https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf