HADMÉRNÖK
VÉDELMI INFORMATIKA

14. évfolyam (2019) 4. szám 179–189.
DOI: 10.32567/hm.2019.4.11

Huszár Viktor[1]

A decentralizáció és a blockchain-technológia felhasználási lehetőségei gépi látás és mesterséges intelligencia használatával a katonai szervezetekben

Application Possibilities of Decentralisation and Blockchain Technology Using Computer Vision and Artificial Intelligence in Military Organisations

A hadtudomány újfajta kihívások elé nézett a 20. század végén az internet megjelenésével. A hagyományos biztonságot veszélyeztető kihívások és fenyegetések olyan új értelmezést kaptak a kiberbiztonság mint új fogalom létrejöttével, ami a katonai műszaki tudományok és az informatikai tudományok szerves átalakulásához vezet. Ahogy az internet alapjaiban megváltoztatta a világ működését, úgy olyan új technológiák keletkeztek a hálózaton, amelyek ismét forradalmasíthatják iparágak sokaságát. Ilyen innováció az elosztott főkönyv (DLT) és a blokklánc-technológia és az ezekre építhető gépi látásra alapuló mesterséges intelligencia. A blokklánc lehetséges felhasználási területei katonai műszaki tudományos kihívások sokaságát veti fel. A technológia ugyanis lehetővé teszi önkéntes, elosztott hálózatok kriptográfiai eljárással történő együttes, robosztus fellépését, állami ellenőrzés nélkül, így akár katonai célokat is szolgálhat.

Kulcsszavak: **decentralizáció, blokklánc-technológia, gépi tanulás, mesterséges intelligencia**

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola, doktorandusz, Teqball Kft. ügyvezető igazgató, e-mail: viktor@teqball.com, ORCID: https://orcid.org/0000-0001-5402-0208

Military science has faced new challenges at the end of the 20th century with the emergence of the Internet. Challenges and threats to traditional security got a new interpretation with a new concept as cybersecurity, which leads to an organic transformation of military engineering and IT. As the Internet has fundamentally changed the way the world works, new technologies have emerged on the network that can revolutionise the multitude of industries. Such innovation is Distributed Ledger Technology (DLT) and Blockchain Technology supplemented with Artificial Intelligence and computer vision. The potential uses of the blockchain represent a multitude of military technical scientific challenges. The technology makes it possible to co-operate freely with cryptographic procedures on distributed networks without state control, but can also serve military and defence management purposes.

Keywords: **decentralisation, blockchain technology, machine learning, artificial intelligence**

Bevezetés

Az informatika folyamatosan fejlődik, átalakul. Már Christensen 1995-ben is rávilágított, a „bomlasztó" innovációk jelentőségére, amelyek cégek, kormányok teljes működését befolyásolhatják [1]. A floppylemez, a CD, az internet mind ilyen újítások voltak. A mindent átszövő információs hálózaton azonban megjelent egy forradalmi innováció, ami a blokklánc- (blockchain-) technológiára alapul [2]. A legtöbben a bitcoin kriptovalutával azonosítják a technológiát, de sokkal többről van szó, mint egy új fizetőeszközről. A blokklánc egyértelműen olyan diszruptív technológia, ami gazdasági, jogi és legfőképpen informatikai értelemben változásokat hoz a világ működésében [3]. A technológia komoly hatással lesz az informatikai rendszerekre, a védelmi igazgatásban viszont kevésbé foglalkoztak még a blokkláncban rejlő lehetőségekkel és veszélyekkel.

A blokklánc lehetséges felhasználási területei katonai műszaki tudományos problémák sokaságát vetik fel. A technológia ugyanis lehetővé teszi önkéntes, elosztott hálózatok kriptográfiai eljárással történő együttes, robosztus fellépését, állami ellenőrzés nélkül. A banki rendszerek, a virtuális pénzek mellett a Smart Contract – okos szerződés – kifejlődésével [4] az ingatlan adásvétel, vagyontárgyak, ingóságok cseréje is új lehetőségek elé néz. Azonban a katonai felhasználási területek még ennél is érdekesebbek, hiszen az adatbiztonság kiemelten kezelendő a védelmi igazgatásban, a hatóságok mindennapi kommunikációjában.

A blokkláncalapú katonai felhasználás esetén protokollfüggően több tudományos probléma is felmerül. Az erőforrás-hatékony felhasználás esetén a központi adattárolás és kontroll nélküli védelmi igazgatási rendszer létjogosultsága kutatandó. A probléma kérdésköre kiterjed egy ilyen esetleges rendszer mesterséges izolációjára, a katonai kockázatokra egy esetleges gépi tanulás és programozott mesterséges intelligencia „öntudatra" ébredése esetén. A tudománynak vizsgálnia kell, hogy miként lehetséges az ilyen automatizált, elosztott hálózatra alapuló katonai felhasználási környezet adatbiztonsága, adatintegrációja, és a mesterséges intelligenciával kapcsolatos

döntéshozatali környezet elszigetelése, a jogosultsági szintek keretrendszerének meghatározása.

Jelenleg a központi adattárolás, és központi kontroll miatt komoly problémát jelent a feltörhető adatkommunikáció a szervezeti egységek között. A veszélyeztetettség mértéke szempontjából a legfontosabb szempont a felhasználó vagy a szervezet tevékenysége és – ami ezzel szorosan összefügg – az adataik értéke. A támadók különösen kedvelt célpontjai a pénzintézetek és az állam- vagy szolgálati titkokat kezelő szervezetek [5].

A blokklánc-technológiához kapcsolódóan felmerül a felhasználói profilozás kérdése is. A probléma az, hogy a blokklánc hosszú távú használata lehetővé teheti a felhasználó magatartásának megfigyelését és az úgynevezett profilalkotást. A jogalkotó véleménye az, hogy ezt a kérdést csak egy konkrét rendszer, az abban kezelt személyes adatok és ahhoz kapcsolódó adatkezelési műveletek teljes körű ismerete kapcsán lehet megítélni [6].

Érdekes kérdés lehet a nemzetvédelem szempontjából a szokásos fizetőeszközökről kriptovalutára való áttérés esetén megfelelő szabályozással az illegális tevékenységek csökkentése. Könnyebben szűrni lehet a pénzforgás célját, így nem lehetne illegális drogokhoz vagy fegyverekhez jutni kriptovalutás fizetéssel. Az egyik oldal azt mondja, hogy a blockchain és a kriptovaluták, mint a bitcoin, természetesen teljesen nyilvánosak, de anonimak kell legyenek. A másik oldalon az érv az, hogy a nyilvános blokkolás elemzését párosítani kell a bankokkal és a KYC-folyamatokkal (know your customer – „ismerd meg az ügyfeled" ügyfélazonosítási elterjedt elv, amelyeket a szabályozók egyre gyakrabban elvárnak), hogy lehetővé tegyék a tiltott szereplők megjelölését és kizárását a piacról [7].

Képelemzés esetén az adatstruktúra változik: képekből képleírások lesznek. Az alakfelismerés képleírásokkal operál és objektumosztályokat hoz létre. Végül, a számítógépes látás célja pedig háromdimenziós modellek megalkotása képek vagy videók alapján [8]. Ehhez szükség van feldolgozásra, elemzésre és felismerésre egyaránt, amelyek nagy számítógépes kapacitást is igényelnek, így a jelenlegi képelemzési módszertanok sokszor lassúak és nem valós időben operálnak. Az összes bányász számítógép együttes számítási kapacitása már 2013-ban meghaladta az 500 legnagyobb szuperszámítógép kapacitásának 250-szeresét [9], a bányászközösség összesített fogyasztása pedig nagyobb volt 2017-ben, mint 159 ország átlagos éves villamosenergia-szükséglete [10]. Jogosan merül fel a blokkláncalapú technológiák használata a gépi látás segítésére, így a drága hardver- és erőforrásigények csökkennének. A zalaegerszegi járműipari tesztpálya ára is mutatja, hogy milyen drága az innovatív gépi látás alapú K + F eredmények implementációi [11].

Mindezek miatt cikkemben a blockchain-technológia hátterét, a decentralizáció előnyeit és hátrányait, valamint a már megvalósult vagy fejlesztés alatt álló felhasználási lehetőségeket mutatom be.

Blockchain-technológia

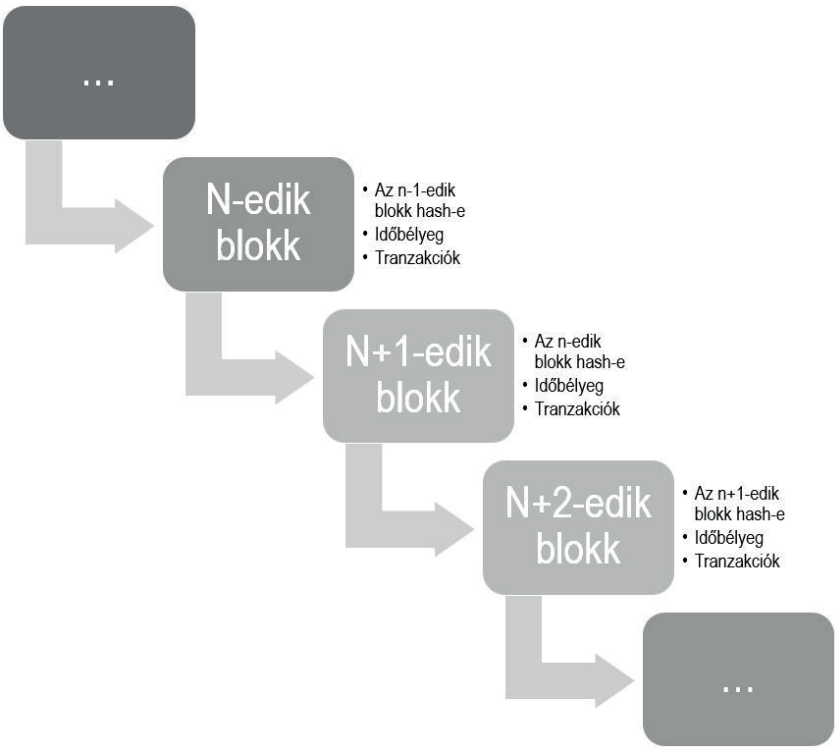
A blockchain („blokkok lánca") az informatikában egy elosztott adattárolási megközelítés, egyfajta elosztott adatbázis, amely sorrendezett bejegyzések egy folyamatosan növekvő blokkokba szervezett listáját tárolja. Az egyes blokkok minden, a blokkláncot tároló csomóponton tartalmaznak egy linket a megelőző blokkra is. A blokkchaint alkalmazó rendszerek alapvető jellemzője az összes rendezett bejegyzések blokklánc-csomópontjainak tárolása és az aktuális állapotról valamilyen konszenzus segítségével állapodnak meg. Az elosztott adattárolás ezen megközelítését a bitcoin elosztott „kriptopénz"-rendszere tette közismertté és népszerűvé, ma már azonban számtalan olyan rendszer létezik, és áll fejlesztés alatt, amelyek ugyanezt az alapelvet követik, de céljukban és kulcsfontosságú műszaki elemeikben a bitcointól alapvetően különböznek. Mindazonáltal e rendszerekre együtt – nem túl precíz módon – blockchain-technológiaként szoktunk hivatkozni.

Sokan hisznek abban, hogy a blockchain-technológia lesz a következő technológiai forradalom [12], amely legalább olyan hatással lesz az életünkre, mint annak idején az internet volt [13]. Hatással lesz például a pénzügyi szektorra, de akár a mesterséges intelligenciára is. A blockchain jelentőségét – elosztott hibatűrő működés, meghamisíthatatlan tranzakció – már az ipar is felismerte, és folyamatban vannak azok a kutatások, hogy esetlegesen hogyan lehet különböző létező rendszereket részben vagy egészben átültetni blockhain alapra.

Érdemes a blockchainalapú technológiákra úgy tekintenünk, mint amelyek egy elosztott „ledger"-t, magyarul főkönyvet valósítanak meg [14]. A blockchain-technológiák kontextusában a ledger egy bejegyzéstároló, ahol a bejegyzések bármit tárolhatnak, és nem lehet őket módosítani miután a tárolóba kerültek (ennek a ledgernek egyébként lehet szűken vett „főkönyv" szemantikája is a blockchain-technológiáktól, és annak alkalmazásától függően, de ez közel sem törvényszerű). A blockchain-technológiák oly módon valósítanak meg elosztott ledgert, hogy azt szinkronban tartják az elosztott hálózat csomópontjai között – amelyek között akár jelentős geográfiai távolság is lehet, illetve különböző vállalatok birtokában is lehetnek, ezáltal mindegyik csomópontnak megvan a saját egyenértékű másolata a ledgerről. Bármilyen változtatás, ami a ledgeren történik, és amibe a hálózat fennmaradó csomópontjai is megegyeznek, a többi csomópont ledgerjében 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 és szabályai bevonása nélkül [15].

A ledger karbantartását az elosztott hálózat csomópontjai végzik, valamilyen megegyezési algoritmus (konszenzus) alapján, amelyek a tároláshoz és a tranzakciók ellenőrzéséhez erősen használják a kriptográfiát. Így a hálózat még nagy számú hibás csomópont esetén is működőképes maradhat, feltéve, ha a hibás csomópontok száma nem éri el a maximálisan megengedett hibás csomópontok számát. Elosztott konszenzusalgoritmusból, illetve 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 szinkronitáskövetelmények. Ennek megfelelően nem meglepő, hogy a különböző blockchain-technológiák is számos különböző konszenzusprotokollt alkalmaznak. Közös azonban a blockchain-technológiákban, hogy az elosztott konszenzus problémáját valamilyen protokoll segítségével kezelik.

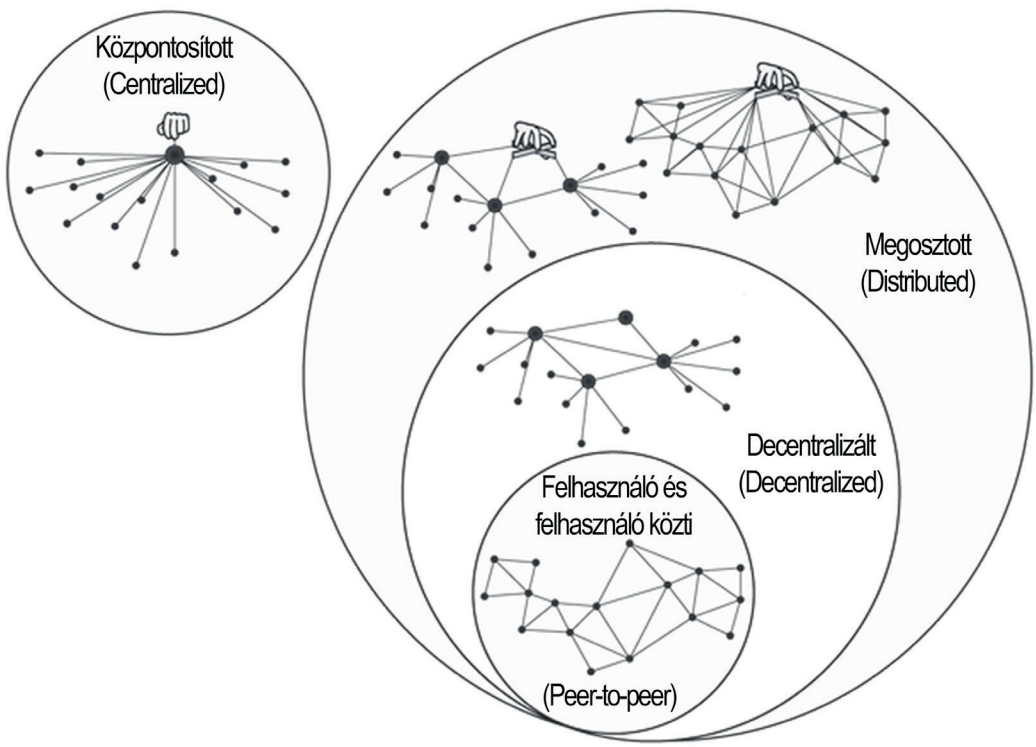


1. ábra

Blockchain-struktúra felépítése (a szerző szerkesztése [15] alapján)

Blockchain-technológiától szinte függetlenül a „blokkláncnak" van egy közös struktúrája (1. ábra). Bizonyos értelemben a blockchain egy tranzakciónapló (journal), aminek bejegyzéseit szigorúan időrendi sorrendben, tömbösítve tároljuk a blokkokban. Ahogy az 1. ábra is mutatja, ezeket a blokkokat időbélyeggel ellátjuk, és valamilyen megfelelően megválasztott kriptografikus hashükkel azonosítjuk. Minden blokk tartalmaz egy referenciát, amely az őt megelőző blokkra mutat. Így a blokkok egy visszafelé láncolt 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). Amennyiben 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 blockchain-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 való rögzítésének módja tükrözi a decentralizáció értékét [16]. Ahelyett, hogy egy központi hatóságra támaszkodnánk, hogy biztonságosan tranzakcióba lépjen a többi felhasználóval, a blockchain 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 számítógépein.



2. ábra

Különböző (központosított, megosztott, decentralizált) rendszerek ábrázolása
(a szerző szerkesztése [17] alapján)

A blockchain technológia kiemelten hasznos a nemzetvédelmi alkalmazásokban is. A következő fejezetben ilyen jellegű alkalmazásokat gyűjtöttem össze, amelyekben a blockchain operatív és támogató szerepet tölt be.

Számítógépes védelem: adatintegritás

A kibervédelem a blockchain-technológia legközelebbi, alacsony költségű, de magas kifizetődésű alkalmazása. A blockchain-technológia független a secretektől és trustoktól, nem úgy, mint az eddigi rendszerek, amik ezen alapultak. A blokkchain két módon őrzi meg a hitelességét. Először biztosítja, hogy a digitális események széles körben elterjedjenek, továbbítva ezeket a hálózat más csomópontjaiba. Ezután konszenzus alkalmazásával ezek az események olyan adatbázisokba kerülnek, amelyet külső fél soha nem változtathat meg.

Ezen túl a blockchain fokozza a számítógépes védelem perimetrikus biztonsági stratégiáját, nem falak megtartásával, hanem a falak és minden bennük levő információ folyamatos megfigyelésével. A modern rendszerek, köztük a fegyverrendszerek egyre növekvő összetettsége a sebezhetőséget valószínűbbé és kevésbé érzékelhetővé teszi.

Egy tipikus amerikai hadihajó, mint egy Arleigh Burke osztályú romboló egyesít több mint kilencven rakétakilövő cellát a radarrendszereivel, két független Phalanx védelmi rendszerrel és hat torpedóindítóval, nem beszélve számos más fegyverrendszerről [18]. A kihívás az, hogy mindezek a harci rendszerek együttműködjenek. Az amerikai haditengerészet sikerének titka a rendszerintegráció, amelyet jelenleg az Aegis Combat System teljesít. Ez egy központosított irányítórendszer (command and control system, CCS), megfelelő kapcsolatot létesít az érzékelők és a fegyverek között, mint ahogy egy ökölvívó agya összeköti a szemeket és az öklöket. De éppen a központosítás a gyenge pont, ha kikapcsol az agy, bukik az egész rendszer. Ezért merül fel a blokklánc használatának lehetősége.

A haditengerészet egy blockchainadatbázis-architektúrát használva strukturálhatja a következő generációs harci rendszereit a decentralizált döntési csomópontok körül. Ez felgyorsítja a tűzszabályozást, ezzel (nagyban) javítva a túlélést. A különféle fegyverrendszerekbe betöltött mesterséges intelligenciával dolgozó processzorok összehangolhatják tevékenységüket és ellenőrizhetik, hogy ugyanazon adatokból dolgoznak-e. A 20. században a feldolgozási teljesítmény drága volt, de az adatok olcsók voltak. Ezért volt 1969-ben értelme központosítani a fedélzeti döntéshozatalt egyetlen Aegis-agyban. Ma a feldolgozási teljesítmény olcsó és az adatok drágábbak. Ezért valószínű, hogy a haditengerészet 21. századi harci rendszerei blokklánc-technológiát fognak használni [19].

Ellátási lánc (supply chain) menedzsment

Számos iparági szervezet dolgozik azon, hogy az ellátási lánc logisztikájában és menedzsmentjében blokklánc-technológiákat használjon. Egyre nagyobb aggodalomra ad okot a védelmi rendszerek ellátásilánc-menedzsmentje amely egyre inkább a kereskedelmi off-the-shelf (COTS)[2] [20] komponenseket használja a beágyazott szoftverrendszerekhez. A probléma az, hogy ezek az összetevők olyan szándékos sebezhetőségeket tartalmazhatnak, amelyeket az ellenfél az általa választott időpontban kihasználhat.

[2] Commercial Off-The-Shelf.

Ezt a fenyegetést a Ghost Fleet újdonsága szenzációs hatásúvá tette, amelyben Kína az F–35-ös repülőgépek teljes flottáját letiltotta egy árucikk-áramkör kártya szándékosan beágyazott hibájával [21].

A blockchainek olyan megoldást kínálnak, amely minden áramköri lap, processzor és szoftverkomponens életét leköveti a gyártástól a felhasználóig. A kártyatervező cég használhatja a blockchaineket, hogy minden áramkör tervezési iterációját naplózza. A gyártók minden gyártott kártya minden modelljét és sorozatszámát bejelenthetik. Végül a forgalmazók bejelenthetik az áramkörök értékesítését a rendszerintegrátorok számára, akik naplózhatják az áramkörök elosztását egy adott repülőgép-szerelvényhez stb. Ebben az összefüggésben a blockchainek állandó nyilvántartást készítenek a tulajdonosok közötti eszközök átruházásáról, ezáltal létrehozva a származtatást.

Sok fegyverrendszert terveztek 30 éves vagy annál hosszabb élettartammal. Azonban a számítástechnikai technológiák, amelyeket ezek a rendszerek használnak, ritkán készülnek több mint egy évtizede. Ennek következtében az elavult alkatrészek cseréje idővel nehezebbé válik. Továbbá több országban a törvények tiltják, hogy olyan alkotóelemet használjon a hatóság, amelynek eredete nem állapítható meg. A tulajdonviszonyok megszakadása egyes részeket használhatatlanná tesz, még akkor is, ha funkcionálisak és nagy kereslet van rájuk. Így a viszonteladók is gazdasági ösztönzést kapnának arra, hogy nyomon kövessék az azonosított kereskedelmi off-the-shelf-komponenseiket egy blokkban, hogy megőrizzék származásukat, ami viszont növeli értéküket.

A Magyar Honvédségben a decentralizált technológiákkal még külön nem foglalkoznak, de nemzetközi kitekintésben már elindult a kutatás és fejlesztés a témában. A NATO C4ISR[3] és az Amerikai Védelmi Minisztérium (DoD) viszont már saját blokkláncprogramokat indított [22], SBIR 2016.2 néven már biztonságos, decentralizált üzenetküldési applikációt fejlesztenek a hadsereg számára.

Rugalmas kommunikáció

A bitcoin egy peer-to-peer üzenetküldő modellt használ, amely minden üzenetet másodperceken belül a világ minden aktív csomópontjához továbbít. A bitcoinhálózat minden csomópontja hozzájárul ehhez a szolgáltatáshoz, beleértve az okostelefonokat is. Ha egy csomópont földi, vezeték nélküli vagy műholdas internetszolgáltatása megszakad, egy bitcoinüzenet küldhető alternatív csatornákon keresztül, mint például nagyfrekvenciás rádió, fax, vagy akár vonalkódba írva és kézzel is. Beérkezés után a szervízcsomópont ellenőrzi az üzenetet, majd továbbítja azt minden egyes kapcsolt résztvevőnek. A csomópontok egymástól függetlenül aggregálhatják az üzeneteket az új blokkokba [23]. Végül, a konszenzusmechanizmus biztosítja, hogy a tisztességtelen szereplők által generált érvénytelen üzeneteket és blokkokat figyelmen kívül hagyják. Ezek a protokollok együttesen biztosítják, hogy a hitelesített üzenetek forgalma megbízhatóan továbbítható legyen a világ minden táján, annak ellenére, hogy

[3] C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance.

a kommunikációs útvonalak, az egyes csomópontok vagy maga a blokklánc ellen támadás történik.

Gépi tanulás és mesterséges intelligencia

A Maven-projekt [24] már tavaly április óta fut. Az Algorithmic Warfare Cross-Functional Teamnek (AWCFT) nevezett program célja az, hogy a gépi tanulás segítségével kutassa át a drónok által készített digitális fotókat és videókat, ugyanúgy, ahogy a röntgenképeken vagy a bőrelváltozásokon a rákra utaló homályos foltokat. Jelen esetben az álló- és a mozgóképeken szereplő objektumok – például az autók – azonosítása a feladat. A drónok által szállított felvételmennyiség olyan nagy, hogy azzal a humán elemzők már nem tudnak megbirkózni. Ezért alkalmazzák erre a célra a mesterséges intelligenciát, amely a gépi tanulásnak köszönhetően egyre jobb lesz a tárgyak felismerésében és osztályozásában. A mesterséges intelligencia ebben már évek óta hatékonyabb az embereknél.

Ma már legalább 90 ország rendelkezik drónokkal, ebből 16 ország fegyveres drónokkal, köztük számos nem állami csoport. Ezek közül sok a robotika szempontjából nem túl kifinomult, de a legtöbb távolról vezérelt vagy távvezérelt. Az autonómia egyre inkább megjelenik a különböző járművek kezelésében. Ilyen például a G-NIUS által kifejlesztett Guardium egy izraeli pilóta nélküli földi jármű (unmanned ground vehicle, UGV), amelyet a gázai határ mentén fellépő küzdelemre és védelemre használnak. A jármű önvezető, de a rajta található fegyverekért emberek felelősek.

Paul Scharre (amerikai biztonsági szakértő), is úgy gondolja, hogy a mesterségesintelligencia-alkalmazásokat a katonai feladatok esetén nem is kell nagymértékben módosítani, és ugyanolyan egyszerűen beépíthetők a fegyverrendszerekbe, mint a civil megoldásokba [25], [26].

A tervezett kamerarendszer egyesítése is blokklánc és mesterséges intelligencia bevonásával lenne igazán hatékony. Ehhez a gépi látás fejlesztéseit is ki kéne aknázni a képfelismerés és képelemzés alkalmazásával. Így még könnyebb lenne a terrorcselekmények vagy más bűncselekmények megelőzése és egyéb nemzetbiztonsági feladatok ellátása. A bűncselekmények és körözött személyek azonosítása pedig nem igényelne annyi időt és erőforrást.

Következtetések

A blockchain-technológia megfordítja a számítógépes biztonsági paradigmát. Először is megbízható, mivel mind a belső mind a külső felhasználók kompromisszumot kell vállaljanak a hálózaton. Másodszor átláthatóan biztonságos, nem támaszkodik meghibásodást okozó csomópontokra, hanem inkább egy olyan kriptográfiai adatszerkezetre, amely rendkívül bonyolult és azonnal nyilvánvalóvá teszi a manipulációt. Végül a blokchain-hálózatok hibatűrők, a megbízható csomópontokat összehangolják, míg a megbízhatatlanokat elutasítják. Ennek eredményeképpen a blockchainhálózatok

nemcsak csökkentik a meghiúsulás valószínűségét, hanem jelentősen nagyobb költségeket is okoznak az ellenség számára az eléréshez.

A decentralizált blockchain-technológia csak egy évtizedes. Ez azt jelenti, hogy teljes potenciálja jelenleg még nem ismert. Ennek megfelelően javasolt a szerves szakértelem fejlesztése blockchain-technológiák témakörében a központi védelmi igazgatási szerveken belül. Érdemes partnerkapcsolati lehetőségeket keresni az iparággal, hogy együttműködések alakuljanak ki a blockchainalapú technológiák fejlesztése és a velük járó kölcsönös előnyök érdekében.

Hivatkozások

[1] J. L. Bower and C. M. Christensen, "Disruptive Technologies: Catching the Wave," *Harward Business Review,* January-February 1995, pp. 43–53.

[2] S. Haber and W. S. Stornetta, "How to time-stamp a digital document?" *Journal of Cryptology,* vol. 3, no. 2, pp. 99–111, Jan. 1991. DOI: https://doi.org/10.1007/BF00196791

[3] Blockchains, "The great chain of being sure about things," *The Economist,* 31 Oct. 2015.

[4] N. Szabo, "Formalizing and Securing Relationships on public networks," *First Monday,* vol. 2, no. 9, 1 Sep. 1997. DOI: https://doi.org/10.5210/fm.v2i9.548

[5] J. Folláth, A. Huszti és A. Pethő, *Informatikai biztonság és kriptográfia*, *A veszélyeztetettséget befolyásoló tényezők.* Budapest: Kempelen Farkas Hallgatói Információs Központ, 2011.

[6] A. Péterfalvi, *A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban.* 2017. július 18.

[7] L. Cuen, "Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report." *CoinDesk,* 27 May 2019. [Online]. Elérhető: www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report (Letöltve: 2019. 05. 15.)

[8] Cs. Dmitrij: *Digitális képelemzés alapvető algoritmusai*. Budapest: ELTE, 2015.

[9] R. Cohen, "Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!" *Forbes,* 28 Nov. 2013.

[10] O. Williams-Grut, "The electricity used to mine bitcoin this year is bigger than the annual usage of 159 countries," *Business Insider,* 27 Nov. 2017. [Online]. Elérhető: https://uk.news.yahoo.com/electricity-used-mine-bitcoin-bigger-080700148.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAC9XfuVYanxvzhEKLoKZKp5VbZJkTKGOPy2_OYcZZSgjfboUVJltlG7nApcfby4bMKFIeTDi99xme3txS1GHVaJBpInb_scMX3MFUy4NyXXG8osyq0ODf168lF8CfALQpoSmSy2AZt3klmwGgY_q90SUXxBdk9xImdxr5foiJAay&guccounter=1 (Letöltve: 2019. 01. 15.)

[11] „Mintegy 40 milliárd forintból épül járműipari tesztpálya Zalaegerszegen," *Autószektor,* 2016. május 19. [Online]. Elérhető: www.autoszektor.hu/hu/content/mintegy-40-milliard-forintbol-epul-jarmuipari-tesztpalya-zalaegerszegen (Letöltve: 2019. 01. 15.)

[12] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* New York: Penguin Random House, 2016.
[13] I. Négyesi, "Changing Role of the Internet in the Light of an International Conference," *Hadmérnök,* 3. évf. 3. sz., pp. 147–153, 2008.
[14] H. Kakavand, N. K. De Sevres and B. Chilton, *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.* 2017. DOI: https://doi.org/10.2139/ssrn.2849251
[15] A. Pinna and W. Ruttenberg, "Distributed ledger technologies in securities posttrading revolution or evolution?" *ECB Occasional Paper,* no.172, 2016.
[16] V. Buterin, *A next-generation smart contract and decentralized application platform.* Ethereum White Paper, 2014, p. 6.
[17] G. P. Dwyer, *The Economics of Bitcoin and Similar Private Digital Currencies*. Madrid: University of Carlos III, ECO 2010-17158 Project, 2014, p. 2.
[18] MaidSafe, "Evolving Terminology with Evolved Technology: Decentralized versus Distributed," *Medium,* 4 Dec. 2015.
[19] Naval Technology, "Arleigh Burke-Class (Aegis) Destroyer," *Naval Technology,* [Online]. Elérhető: www.naval-technology.com/projects/burke/ (Letöltve: 2019. 01. 15.)
[20] I. Négyesi, „Die Überprüfung der Voraussetzungen von COTS Systemen," *Hadmérnök,* 7. évf., 2. sz., pp. 371–376, 2012.
[21] S. Babones, "Smart 'Blockchain Battleships' Are Right Around the Corner," *The National Interest,* 17 May, 2018. [Online]. Elérhető: https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872 (Letöltve: 2019. 01. 15.)
[22] C. Thatcher, "Technology's dilemmas: Are we wired to respond?" *Vanguard,* 11 May 2015. [Online]. Elérhető: https://vanguardcanada.com/2015/05/11/technologys-dilemmas-are-we-wired-to-respond/ (Letöltve: 2019. 01. 15.)
[23] A. A. Malik, A. Mahlboob, A. Khan and J. Zibairi, "Application of Cyber Security in Emerging C4ISR Systems," in *Crisis Management: Concepts, Methodologies, Tools, and Applications,* Hershey: IGI Global, 2014, pp. 1705–1738. DOI: https://doi.org/10.4018/978-1-4666-4707-7.ch086
[24] S. Berta, *Maven projekt – a Google könnyen pótolható*, Sg.hu, 2018. június 6. [Online]. Elérhető: https://sg.hu/cikkek/it-tech/131574/maven-projekt-a-google-konnyen-potolhato (Letöltve: 2019. 01. 15.)
[25] P. Scharre, "Killer Robots and Autonomous Weapons With Paul Scharre," *Podcast,* 1 June 2018. [Online]. Elérhető: www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre (Letöltve: 2019. 01. 15.)
[26] I. Négyesi, „Die Vision der tragbaren Informationstechnologiegerate," *Hadmérnök,* 3. évf. 4. sz., pp. 173–179, 2008.