Viktor Huszár

APPLICATION POSSIBILITIES OF DECENTRALIZATION AND BLOCKCHAIN TECHNOLOGY USING COMPUTER VISION AND ARTIFICIAL INTELLIGENCE IN DEFENSE MANAGEMENT, MILITARY AND POLICE ORGANIZATIONS

DOI: 10.35926/HDR.2020.1.1

ABSTRACT: *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 in-terpretation with a new concept of cybersecurity, which led to an organic transforma-tion 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 revolutionize the multitude of industries. Such innovation is Distributed Ledger Technology (DLT) and Blockchain Technology supplemented with Artificial Intelligence and machine vision. The potential uses of the block chain represent a multitude of military technical scientific challenges. The technology makes it possible to co-operate freely with cryptographic pro-cedures on distributed networks without state control, but it can also serve military and defense management purposes.*

KEYWORDS: *decentralization, blockchain technology, machine learning, Artificial Intelligence*

INTRODUCTION

Information technology is constantly evolving and transforming. Early scientific pioneers, like Christensen highlighted the importance of "disruptive" innovations that can affect the overall operation of companies, governments.[1] The turbulent and dynamic computer science industry has witnessed the birth of the floppy disk, then the transition to CD, DVD and Blu-eray discs, but most remarkably, the evolution of the internet can be classified as a disruptive innovation. The most recent organic defragmentation of the ubiquitous information network is a revolutionary innovation based on the blockchain technology.[2] Most people identify this technology with bitcoin[3], but it is much more than the evolution of a new digital currency.

1 Bower, L. and Christensen, M. "Disruptive Technologies. Catching the Wave". *Harvard Business Review* 74/1. 1995. 43-53. https://hbr.org/1995/01/disruptive-technologies-catching-the-wave, Accessed on 20 April 2020.

2 Haber, S. and Stornetta, W. S. "How to time-stamp a digital document". *Journal of Cryptology* 3/2. 1991. 99–111. DOI:10.1007/bf00196791

3 Satoshi, N. "Bitcoin: A peer-to-peer electronic cash system". bitcoin.org. 2008. https://bitcoin.org/bitcoin.pdf

Blockchain is clearly a disruptive technology that changes the way the world works in economic, legal and information security terms.[4] It will have a significant impact on IT systems, but less attention has been paid to the opportunities and threats of the blockchain networks in military administration.

Defense areas for blockchain-based applications and solutions raise a wide range of scientific questions. In terms of military use, governmental development puts emphasis on hybrid warfare and globally substantially more funding is available for research and development of the field. Blockchain technology allows voluntary, distributed networks created for military purposes to co-operate through a cryptographic process without central and state control. Blockchain technology consequently results in a digital paradigm shift, characterized by decentralization, blockchain technology, machine learning, and Artificial Intelligence.

CHALLENGING MILITARY APPLICABILITY

The potential applications of the blockchain raise numerous military technical challenges. Blockchain is a computer-scientific term for a distributed data storage technology, a distributed ledger database that stores a list of entries in ever-increasing blocks. Each block also contains a link to the preceding block on each node that stores a structured chain.[5] An essential feature of systems using blockchain is the storage of blockchain nodes in all structured entries using a consensus algorithm. Despite the fact that bitcoin was an early adapter of the technology, today there are numerous systems under development that follow the same principle but differ fundamentally from bitcoin in their purposes and key technical elements. These systems together are often referred to as blockchain technology, not too precisely. The technology allows voluntary, distributed networks to be cryptographically deployed in a robust manner, without governmental and central state control. In addition to banking systems, virtual money and the development of Smart Contract,[6] real estate sales, exchange of assets and movable property are also emerging. However, military applications are even more interesting, as data security must be a priority in defense administration and in the daily communication of authorities.

For blockchain-based military use, there are several scientific challenges depending on the protocol in use. The need for a centralized data storage and uncontrolled security management system should be explored for the efficient use of resources. The problem extends to the artificial isolation of such a system and the military risks of "awaking" machine-learning or programmed Artificial Intelligence. Science should investigate how data security, data integration, isolation of the Artificial Intelligence decision-making environment, and the framework for authorization levels can be achieved in such an automated, distributed network-based military environment.

---

4 "Blockchains: The great chain of being sure about things". *The Economist,* 31 October 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, Accessed on 20 April 2020.

5 Huszár, V. "A decentralizáció és a blockchain-technológia felhasználási lehetőségei gépi látás és mesterséges intelligencia használatával a katonai szervezetekben". *Hadmérnök* 14/4. 2019. 179-189. DOI: 10.32567/hm.2019.4.11

6 Szabo, N. "Formalizing and securing, Relationships on public networks". *First Monday 2/9. 1997.* DOI:10.5210/fm.v2i9.548

Currently, due to centralized data storage and central control, fragile data communication between military and police departments is a major problem, especially in less developed countries. The most important aspect in terms of the degree of vulnerability is the activity of the user or the organization and – closely related to this – the value of their data. Particularly popular targets of attackers are financial institutions and organizations dealing with state or classified documents.[7]

Blockchain technology also raises the issue of user profiling. The problem is that the long-term use of the blockchain may allow monitoring of user behavior and the use of profiling. Government regulations require data protection measures based on the complete knowledge of a specific system, the personal data it processes, and the related data processing operations.[8]

Police forces aim at reducing illegal activities through appropriate regulations as there has been a transition from traditional means of payment to blockchain-operated cryptocurrencies. Central authorities, including the central bank of a country, may find it easier to filter the purpose of the cash flow, so money laundering, illegal substances or weapons will not be completed with cryptocurrency payments. The main argument supporting blockchain and cryptocurrencies, like bitcoin, are based on the transparency of the transactions which are all public. On the other hand, the analysis of public blocks lacks any KYC process (which is increasingly propagated by regulators to allow the identification and exclusion of prohibited operators.[9]

Hybrid Warfare

In Hungary, the Zrínyi 2026 Defense and Armed Forces Development Program has recognized that new types of challenges require special attention in order to build, maintain, and develop the Hungarian cyber defense capabilities[10]. In June 2019, the Cyber Training Center of the Hungarian Armed Forces was established, which serves as one of the most important pillars of our hybrid force development strategy. The cyber defense force's approach relies on the appropriate infrastructure and equipment but the establishment of a Hungarian cyber academy created the ability needed for hybrid warfare: digitally trained soldiers. The Cyber Training Center can serve a dual purpose, because in addition to supporting cyber defense capability development and harmonization, it can also directly become an institutionalized military technology research and development center which fundamentally determines the defense capability of a country[11]. Previous studies suggest that Hungary should specialize in IT areas such as electronics and software development. Given the fact, that blockchain-based military applications globally have not been explored, a key research target area should be

---

7 Folláth, J., Huszti A. and Pethő A. "Informatikai biztonság és kriptográfia". Debrecen: Kempelen Farkas Digitális Tankönyvtár, 2011. https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch03s04.html

8 Péterfalvi, A. "A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc ("blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban". NAIH. 18 July 2017. https://www.naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf

9 Cuen, L. "Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report". coindesk.com. 27 May 2019. https://www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report

10 "Zrínyi 2026 Programme to begin". Ministry of Defence, Hungary. 22 Dec 2016. 14. https://www.kormany.hu/en/ministry-of-defence/news/zrinyi-2026-programme-to-begin

11 Kovács, L. *A kibertér védelme*. Budapest: Dialóg Campus, 2018.

the distributed ledger systems. Countries like Hungary can gain global competitive military advantage with superior IT knowledge, which results in government-civil-military interoperability, educational, economic, and social added value. The development of hybrid warfare is therefore beneficial for key national objectives.

Distributed General Ledger (DLT) technology is able to make optimal use of new innovations such as Artificial Intelligence and machine vision.[12] A distributed general ledger is a database of digital data distributed (decentralized), shared, and synchronized across multiple geographic locations, countries or institutions.

The potential use of deep neural network learning capabilities that can be run on such a general ledger poses a number of military scientific challenges, and consequently creates new platforms for cyber operations.

The everyday work of military and police forces has been supported by security camera feeds. Computer vision and automated image analysis could save military resource. An image analyzed means the actual image data structure changes: images become image descriptions, which can be classified into image groups. The purpose of computer vision is to create three-dimensional models based on images or videos.[13] This requires data processing, analysis, and image recognition, all of which require high computing power, so current image analysis methodologies are often slow and do not operate in real time. Blockchain based networks achieved outstanding computing power capabilities. Shockingly, in 2013 all mining computers had a combined computing capacity of 250 times the capacity of the 500 largest supercomputers,[14] and the mining community's aggregate consumption in 2017 was higher than the average annual electricity demand of 159 countries.[15] It is legitimate to use blockchain-based technologies to help machine vision, thus reducing expensive hardware and resource requirements. Without resource efficient IT backend, computer vision research expenses can get out of control. The price of the first Hungarian 5G automotive test track proves the massive cost related to the implementation of innovative machine vision based R&D results.[16]

Blockchain technology might be a revolutionary research field for military engineering but there is still space for better understanding the advantages and disadvantages of decentralization, by studying the international military applications that have already been implemented or are under current development.

---

12 "Distributed Ledger Technology: Beyond block chain". London: UK Government Office for Science, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

13 Csetverikov, D. "Digitális képelemzés alapvető algoritmusai". Budapest: ELTE, 2015. https://www.inf.elte.hu/dstore/document/297/Csetverikovjegyzet.pdf

14 Cohen, R. "Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!". *Forbes,* 28 November 2013. https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#381f46086e5e

15 Williams-Grut, O. "The electricity used to mine bitcoin this year is bigger than the annual usage of 159 countries". Markets Insider. 27 November 2017. https://markets.businessinsider.com/currencies/news/bitcoin-mining-electricity-usage-2017-11-1009558934

16 "Mintegy 40 milliárd forintból épül járműipari tesztpálya Zalaegerszegen". autoszektor.hu. 19 May 2016. http://www.autoszektor.hu/hu/content/mintegy-40-milliard-forintbol-epul-jarmuipari-tesztpalya-zalaegerszegen, Accessed on 15 January 2019.

BLOCKCHAIN TECHNOLOGY

More and more frequently scientific authors publish that blockchain technology will be the next technological revolution[17] that will impact our lives similarly as it happened with Internet. It will affect, for example, the more conservative financial sector but also recent popular research areas, such as Artificial Intelligence. The importance of blockchain – distributed fault tolerance, seamless transaction – has already been recognized by the industry, and research is under way on how to possibly migrate various existing systems to blockchain basis, in whole or in part.

It is worth considering blockchain-based technologies as implementing a distributed ledger.[18] In the context of blockchain technologies, the ledger is an entry repository where entries can be stored and cannot be modified once they are in the repository (this ledger may also have a narrow "ledger" semantics depending on the blockchain technologies and their application, but this is not nearly a regularity). Blockchain technologies implement distributed ledger by keeping it in sync with nodes in the distributed network, which can be geographically distant or owned by different companies, so each node has its own equivalent copy of the ledger. Any changes to the ledger – and the rest of the nodes in the network agree – will appear within minutes on other nodes, even seconds on some solutions, and will allow any trusted central monitoring body to access the information stored in the entries, without involving its internal processes and rules.[19]

The ledger is maintained by distributed network nodes – based on some sort of consensus algorithm – that heavily use cryptography to store and verify transactions. This allows the network to remain functional even with a large number of defective nodes, provided that the number of defective nodes is below the maximum number of defective nodes. IT knows and applies a great deal from the distributed consensus algorithm or, more generally, from the distributed consensus protocol. In a given application context, the selection of the consensus protocol is influenced by factors such as hypothesized failure modes, maximum system size, consensus response time, and synchronization requirements. Accordingly, it is not surprising that different blockchain technologies also use a number of different consensus protocols. However, what is common in blockchain technologies is that the problem of distributed consensus is addressed by some protocol.

Almost independently of blockchain technology, the blockchain has a common structure. In a sense, blockchain is a transaction log (journal) whose entries are stored in blocks in a strictly chronological order. As shown in Figure 1, these blocks are time-stamped and identified by some suitably selected cryptographic hash. Each block contains a reference to the block preceding it. In this way, the blocks are organized into a backward-chained list, which, at worst, can be processed from the first block to clearly determine the current state of the distributed database (of course, when there is consensus between nodes on the block-

---

17 Tapscott, D. and Tapscott, A. Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World. London: Penguin. 2016.

18 Kakavand, H., Kost de Sévres, N. and Chilton, B. "The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies". *Social Science Research Network* 2017. DOI:10.2139/ssrn.2849251 ; https://www.semanticscholar.org/paper/The-Blockchain-Revolution%3A-An-Analysis-of-and-to-Kakavand-S%C3%A8vres/df2e88f4ce56c0456e0472d29b8f660fdd865e78

19 Pinna, A. and Ruttenberg, W. *Distributed ledger technologies in securities post-trading revolution or evolution?*. Frankfurt am Main: European Central Bank, 2016. DOI:10.2866/270533

chain). If the consensus protocol is "strong", then it is not possible to change or delete an earlier operation without the client that is aware of enough nodes in the system to notice it.

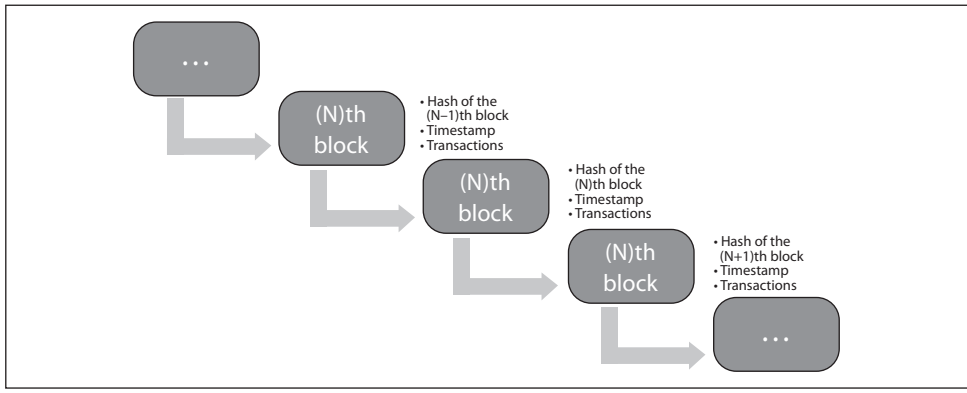

Figure 1 *Structure of blockchain*[20]

The decentralized nature of blockchain technology (Figure 2) means that it does not rely on a central entity, a checkpoint. The lack of authority makes the system fairer and more secure. The way in which data is recorded on the blockchain reflects the value of decentralization.[21] Instead of relying on a central authority to secure transactions with other users, blockchain uses innovative consensus protocols on the node network to authenticate transactions and record data in an unbiased manner. Thus, the blockchain is not stored by a central data controller, but practically all users store it on their own computers.

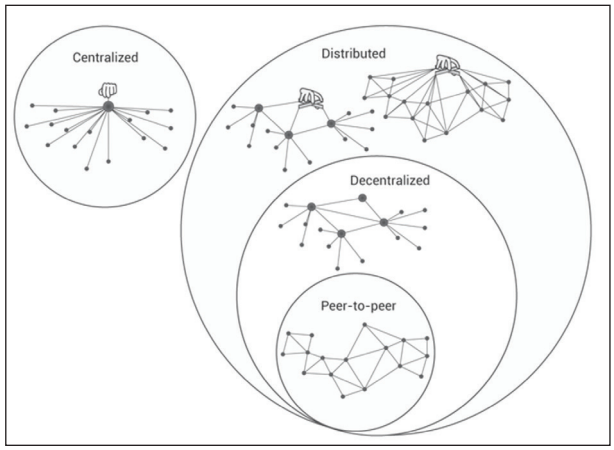

Figure 2 *Representation of different (centralized, distributed, decentralized) systems*[22]

[20] Huszár. "A decentralizáció és a blockchain-technológia felhasználási lehetőségei…"

[21] Buterin, V. "Ethereum White Paper: A next-generation smart contract and decentralized application platform". blockchainlab.com. April 2014. 6. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[22] Dwyer, G. P. "The Economics of Bitcoin and Other Private Digital Currencies". MPRA Paper 57360. 8 May 2014. 2. https://mpra.ub.uni-muenchen.de/57360/3/MPRA_paper_57360.pdf

Blockchain technology is also extremely useful in national defense applications. Several applications are being investigated by the governments, which use blockchain and has an operational and support role.

COMPUTER PROTECTION: DATA INTEGRITY

Cybersecurity is the closest low-cost but high-paying application of blockchain technology. Blockchain technology is independent of secrets and trusts, just like the previous systems based on it. Blockchain retains its credibility in two ways. First, it ensures that digital events are widespread and transmitted to other nodes in the network. Then, by consensus, these events are entered into databases that can never be modified by a third party.

In addition, blockchain enhances the perimeter security strategy of computer security, not by keeping walls, but by constantly monitoring walls and all information inside. The increasing complexity of modern systems, including weapon systems, makes vulnerability more likely and less perceptible.

A typical American warship, like an Arleigh Burke-class destroyer, combines more than ninety missile launchers with its radar systems, two independent Phalanx defense systems and six torpedo launchers, not to mention many other weapon systems.[23] The challenge is for all these combat systems to work together. The secret to the success of the US Navy is system integration, which is currently being implemented by the Aegis Combat System. This is a centralized command-and-control (CCS) system that establishes a proper connection between sensors and weapons, just as a boxing brain connects eyes and fists. But centralization is the weak point, when the brain shuts down, the whole system fails. That is why the blockchain can be used.

The Navy can use a blockchain database architecture to structure its next-generation combat systems around decentralized decision nodes. This speeds up fire control, thereby (greatly) improving survival. Artificial-intelligence processors loaded into different weapon systems can coordinate their activities and verify that they are working from the same data. In the 20th century, processing power was expensive, but data was cheap. That is why, in 1969, it made sense to centralize on-board decision-making in a single Aegis brain. Today, processing power is cheap and data is more expensive. Therefore, twenty-first century naval combat systems are likely to use blockchain technology.[24]

SUPPLY CHAIN MANAGEMENT

Many industry organizations are working to use blockchain technologies in supply chain logistics and management. There is a growing concern about security systems supply chain management, which is increasingly using commercial off-the-shelf (COTS) components for embedded software systems. And these components may contain intentional vulnerabilities that the opponent can exploit at the time of his choice. This threat has been

[23] MaidSafe. "Evolving Terminology with Evolved Technology: Decentralized versus Distributed". Medium. 4 December 2015. https://medium.com/safenetwork/evolving-terminology-with-evolved-technology-decentralized-versus-distributed-7f8b4c9eacb

[24] "Arleigh Burke-Class (Aegis) Destroyer". Naval Technology. https://www.naval-technology.com/projects/burke/

made sensational by the novel Ghost Fleet, in which China has downed the entire fleet of F-35 aircraft by a deliberately embedded commodity circuit board error.[25]

Blockchain offers a solution that tracks the life of every circuit board, processor, and software component from production to user. The card design company can use blockchains to log the design iteration of each circuit. Manufacturers may report all models and serial numbers of each card manufactured. Finally, distributors can report the sale of circuits to system integrators, who can log the distribution of circuits to a particular aircraft assembly, etc. In this context, blockchains maintain a permanent record of transfers of assets between owners, thereby creating a derivative.

Many weapon systems are designed with a lifespan of 30 years or more. However, the computing technologies used by these systems have rarely been made for more than a decade. As a result, replacing obsolete parts becomes more difficult over time. Furthermore, in several countries it is prohibited by law to use a component whose origin cannot be ascertained. Loss of ownership makes some parts unusable, even if they are functional and in high demand. This would give the resellers an economic incentive to track their identified off-the-shelf commercial components in a block to retain their origin, which in turn adds value.

Decentralized technologies are not dealt with separately in the Hungarian Defense Forces, but international research and development is already under way. However, NATO's C4ISR and the US Department of Defense (DARPA – DoD) have already launched their own blockchain programs,[26] developing a secure, decentralized messaging application for the military under the name SBIR 2016.2.

FLEXIBLE COMMUNICATION

Bitcoin uses a peer-to-peer messaging model that delivers every message to every active node in the world in seconds. All nodes in the Bitcoin network contribute to this service, including smartphones. If a node's terrestrial, wireless, or satellite Internet service is interrupted, a bitcoin message can be sent through alternative channels such as high-frequency radio, fax, or even barcode-based and manually. Upon receipt, the service node checks the message and forwards it to each associated participant. Nodes can independently aggregate messages into new blocks.[27] Finally, the consensus mechanism ensures that invalid messages and blocks generated by rogue operators are ignored. Together, these protocols ensure that the traffic of authenticated messages can be reliably relayed anywhere in the world, even though communication paths, individual nodes, or the blockchain itself are attacked. Cyber superiority is not individually maintained by the nodes, but the network system can be kept controlled with current and expected data.[28]

---

[25] Babones, S. "Smart 'Blockchain Battleships' Are Right Around the Corner". *The National Interest,* 17 May 2018. https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872

[26] Singer, P. W. and Thatcher, C. "Technology's dilemmas: Are we wired to respond? an interview with P. W. Singer". *Vanguard,* 11 May 2015. 32-34. https://vanguardcanada.com/2015/05/11/technologys-dilemmas-are-we-wired-to-respond/

[27] Malik, A. et al. "Application of Cyber Security in Emerging C4ISR Systems". In *Crisis Management: Concepts, Methodologies, Tools, and Applications.* Hershey: Information Science Reference, 2014. DOI:10.4018/978-1-4666-4707-7.ch086

[28] Swan, M. Blockchain - Blueprint for a new economy. Gravenstein: O'Reilly Media. 2015.

MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

The Maven project[29] has been running since April last year. The program, called the Algorithmic Warfare Cross-Functional Team (AWCFT), is designed to scan machine-generated digital photos and videos of drones with machine learning, as well as blurred patches of cancer on x-rays or skin lesions.[30] In this case, the task is to identify objects, such as cars, in the still and motion pictures. The amount of footage that drones carry is so large that human analysts can no longer cope. That is why Artificial Intelligence is used for this purpose, which, thanks to machine learning, will be better at recognizing and classifying objects. For many years, Artificial Intelligence has been more effective than humans.

Today, at least 90 countries have drones, 16 of them even armed drones, including many non-state groups. Many of these vehicles are not very sophisticated in robotics, but most are remotely controlled. Autonomy is becoming increasingly apparent in the management of different vehicles. For example, the Guardium, developed by G-NIUS, is an Israeli unmanned ground vehicle (UGV) used for combat and defense along the Gaza border. The vehicle is self-propelled, but people are responsible for the weapons on it.

Paul Scharre (US Security Expert) also believes that Artificial Intelligence applications do not require major modifications to military tasks and can be integrated into weapon systems just as easily as civilian solutions.[31]

Combining the planted camera systems[32] with blockchain and Artificial Intelligence would be really effective. To do this, we should also take advantage of machine vision enhancements using image recognition and image analysis. This would make it easier to prevent terrorist acts or other crimes or to perform other national security tasks. Identifying crimes and persons wanted would not require so much time and resources. Countries with limited financial and infrastructural resources realized the need to enhance information operation developments.[33] Such a system could be a cost efficient implementation to increase crime prevention results.

CONCLUSIONS

Blockchain technology reverses the computer security paradigm. First of all, it is reliable because both internal and external users have to compromise on the network. Second, it is transparently secure and does not rely on malfunctioning nodes, but rather on a cryptographic data structure that makes manipulation extremely complex and immediately apparent. Finally, blockchain networks are fault tolerant, coordinate trusted nodes, and reject untrusted

---

[29] Berta, S. "Maven projekt - a Google könnyen pótolható". Sg.hu. 6 June 2018. https://sg.hu/cikkek/it-tech/131574/maven-projekt-a-google-konnyen-potolhato

[30] Haig Zs. "Connections between cyber warfare and information operations". *AARMS* 8/2. 2009. 329-337. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1900/13haig.pdf?sequence=1&isAllowed=y

[31] Scharre, P. "Killer Robots and Autonomous Weapons With Paul Scharre". Podcast. Council on Foreign Relations. 1 June 2018. https://www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre

[32] "Hamarosan itthon is beindulhat a mindent látó Nagy Testvér". *Népszava,* 22 October 2018. https://nepszava.hu/3012846_hamarosan-itthon-is-beindulhat-a-mindent-lato-nagy-testver, Accessed on 20 April 2020.

[33] Haig, Zs. "Az információs hadviselés kialakulása, katonai értelmezése". *Hadtudomány* 21/1-2. 2011. 12-28. http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf

ones. As a result, blockchain networks not only reduce the likelihood of failure, but also significantly increase the cost to the enemy to reach. Decentralized blockchain technology is only a decade old. This means that its full potential is currently unknown.

Accordingly, it is recommended to develop organic expertise in blockchain technologies within the Central Defense Management Authorities. It is worth looking for partnerships with the industry to develop synergies for the development of blockchain-based technologies and the mutual benefits they bring.

BIBLIOGRAPHY

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

Babones, S. "Smart 'Blockchain Battleships' Are Right Around the Corner". *The National Interest*, 17 May 2018. https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872

Berta, S. "Maven projekt – a Google könnyen pótolható". Sg.hu. 6 June 2018. https://sg.hu/cikkek/it-tech/131574/maven-projekt-a-google-konnyen-potolhato

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

Bower, L. and Christensen, M. "Disruptive Technologies. Catching the Wave". *Harvard Business Review* 74/1. 1995. 43-53. https://hbr.org/1995/01/disruptive-technologies-catching-the-wave

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

Cohen, R. "Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!". *Forbes,* 28 November 2013. https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#381f46086e5e

Csetverikov, D. "Digitális képelemzés alapvető algoritmusai". Budapest: ELTE, 2015. https://www.inf.elte.hu/dstore/document/297/Csetverikovjegyzet.pdf

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

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

Dwyer, G. P. "The Economics of Bitcoin and Other Private Digital Currencies". MPRA Paper 57360. 8 May 2014. https://mpra.ub.uni-muenchen.de/57360/3/MPRA_paper_57360.pdf

Folláth, J., Huszti A. and Pethő A. "Informatikai biztonság és kriptográfia". Debrecen: Kempelen Farkas Digitális Tankönyvtár, 2011. https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch03s04.html

Haber, S. and Stornetta, W. S. "How to time-stamp a digital document". *Journal of Cryptology* 3/2. 1991. 99–111. DOI:10.1007/bf00196791

Haig, Zs. "Az információs hadviselés kialakulása, katonai értelmezése". *Hadtudomány* 21/1-2. 2011. 12-28. http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf

Haig Zs. “Connections between cyber warfare and information operations”. AARMS 8/2. 2009. 329-337. http://m.ludita.uninke.hu/repozitorium/bitstream/handle/11410/1900/13haig.pdf?sequence=1&isAllowed=y

“Hamarosan itthon is beindulhat a mindent látó Nagy Testvér” *Népszava,* 22 October 2018. https://nepszava.hu/3012846_hamarosan-itthon-is-beindulhat-a-mindent-lato-nagy-testver, Accessed on 20 April 2020.

Huszár, V. “A decentralizáció és a blockchain-technológia felhasználási lehetőségei gépi látás és mesterséges intelligencia használatával a katonai szervezetekben”. *Hadmérnök* 14/4. 2019. 179-189. DOI:10.32567/hm.2019.4.11

Kakavand, H., Kost de Sévres, N. and Chilton, B. “The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies”. *Social Science Research Network* 2017. DOI:10.2139/ssrn.2849251. https://www.semanticscholar.org/paper/The-Blockchain-Revolution%3A-An-Analysis-of-and-to-Kakavand-S%C3%A8vres/df2e88f4ce56c0456e0472d29b8f660fdd865e78

Kovács, L. *A kibertér védelme*. Budapest: Dialóg Campus, 2018.

MaidSafe. “Evolving Terminology with Evolved Technology: Decentralized versus Distributed”. Medium. 4 December 2015. https://medium.com/safenetwork/evolving-terminology-with-evolved-technology-decentralized-versus-distributed-7f8b4c9eacb

Malik, A., Mahboob, A., Khan, A. and Zubairi, J. “Application of Cyber Security in Emerging C4ISR Systems”. In *Crisis Management: Concepts, Methodologies, Tools, and Applications.* Hershey: Information Science Reference, 2014. 1705-1738. DOI:10.4018/978-1-4666-4707-7.ch086

“Mintegy 40 milliárd forintból épül járműipari tesztpálya Zalaegerszegen”. autoszektor.hu. 19 May 2016. http://www.autoszektor.hu/hu/content/mintegy-40-milliard-forintbol-epul-jarmuipari-tesztpalya-zalaegerszegen, Accessed on 15 January 2019.

Pinna, A. and Ruttenberg, W. *Distributed ledger technologies in securities posttrading revolution or evolution?.* Frankfurt am Main: European Central Bank, 2016. DOI:10.2866/270533

Péterfalvi, A. “A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc (»blockchain«) technológia adatvédelmi összefüggéseivel kapcsolatban”. NAIH. 18 July 2017. https://www.naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf

Satoshi, N. “Bitcoin: A peer-to-peer electronic cash system”. bitcoin.org. 2008. https://bitcoin.org/bitcoin.pdf

Scharre, P. “Killer Robots and Autonomous Weapons With Paul Scharre”. Podcast. Council on Foreign Relations. 1 June 2018. https://www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre

Singer, P. W. and Thatcher, C. “Technology’s dilemmas: Are we wired to respond? an interview with P. W. Singer”. *Vanguard,* 11 May 2015. 32-34. https://vanguardcanada.com/2015/05/11/technologys-dilemmas-are-we-wired-to-respond/

Swan, M. *Blockchain – Blueprint for a new economy.* Gravenstein: O’Reilly Media. 2015.

Szabo, N. “Formalizing and securing, Relationships on public networks”. *First Monday* 2/9. 1997. DOI:10.5210/fm.v2i9.548

Tapscott, D. and Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. London: Penguin. 2016.

Williams-Grut, O. “The electricity used to mine bitcoin this year is bigger than the annual usage of 159 countries”. Markets Insider. 27 November 2017. https://markets.businessinsider.com/currencies/news/bitcoin-mining-electricity-usage-2017-11-1009558934

“Zrínyi 2026 Programme to begin”. Ministry of Defence, Hungary. 22 Dec 2016. https://www.kormany.hu/en/ministry-of-defence/news/zrinyi-2026-programme-to-begin