Wojciech MINCEWICZ
Uniwersytet Warszawski[1]
Wydział Nauk Politycznych i Studiów Międzynarodowych
Katedra Socjologii Polityki i Marketingu Politycznego
w.mincewicz@uw.edu.pl
ORCID 0000-0003-0460-9158
https://doi.org/10.34739/dsd.2020.02.08

BLOCKCHAIN TECHNOLOGY AND NATIONAL SECURITY. THE ABILITY TO IMPLEMENT A BLOCKCHAIN IN THE AREA OF NATIONAL SECURITY

ABSTRACT: The article undertakes an analysis of the potential of using blockchain technology to strengthen the security of the state, which is guaranteed by a strong and efficient army. As part of his own studies, the author first characterizes the solutions that were first implemented in 2008 with the creation of Bitcoin. Blockchain technology, described as the most important achievement of humanity since the creation of the internet. It is increasingly used in areas such as payment management, digitization, and contract storage, or in the private sector, where data security plays a key role. Available reports and studies indicate that the United States, the Russian Federation, and the People's Republic of China are intensively working on the implementation of technology in the functioning of their armies. In turn, countries such as South Korea or India began pilot programs in 2019, which will eventually lead to the implementation of blockchain technology in their armies. Hence, the question arises, what military application blockchain technology has or may have in the foreseeable future, and how its use by armies can contribute to improving the security of the state? In the study presented, the following three areas of potential application have been distinguished: security in cyberspace, supply chain management, and more effective and reliable communication.

KEYWORDS: Blockchain, Bitcoin, cryptocurrencies, security, cryptography, army

TECHNOLOGIA BLOCKCHAIN A BEZPIECZEŃSTWO NARODOWE. MOŻLIWOŚĆ WDROŻENIA ŁAŃCUCHA BLOKÓW W OBSZARZE BEZPIECZEŃSTWA PAŃSTWA

ABSTRAKT: W artykule podjęta została analiza potencjału wykorzystania technologii blockchain dla wzmocnienia bezpieczeństwa państwa, którego gwarantem jest silna i sprawnie funkcjonująca armia. Na początku autor dokonuje charakterystyki rozwiązań, które jako pierwsze zostały zaimplementowane w 2008 roku wraz z powstaniem Bitcoina. Technologia łańcucha bloków, określana jako najważniejsze osiągnięcie ludzkości od momentu powstania internetu. Coraz częściej znajduje zastosowanie w takich obszarach jak: zarządzanie płatnościami, digitalizacja

[1] The Warsaw University; Poland.

i przechowywanie umów, czy też w sektorze prywatnym, gdzie kluczową rolę odgrywa bezpieczeństwo danych. Dostępne raporty i opracowania wskazują, że intensywne prace nad wdrożeniem technologii w funkcjonowanie swoich armii prowadzą Stany Zjednoczone, Federacja Rosyjska oraz Chińska Republika Ludowa. Z kolei takie kraje jak Korea Południowa czy Indie w 2019 roku rozpoczęły programy pilotażowe, które finalnie mają także doprowadzić do implementacji technologii łańcucha bloków w ich armiach. Stąd też rodzi się pytanie, jakie militarne zastosowanie ma lub może mieć w dającej się przewidzieć przyszłości, technologia łańcucha bloków i jak jej wykorzystanie przez armie może przyczynić się do poprawy bezpieczeństwa państwa? W prezentowanym studium wyróżnione zostały trzy następujące obszary potencjalnego zastosowania: bezpieczeństwo w cyberprzestrzeni, zarządzanie łańcuchem dostaw oraz bardziej efektywna i niezawodna komunikacja.

SŁOWA KLUCZOWE: Blockchain, Bitcoin, kryptowaluty, bezpieczeństwo, kryptografia, wojsko

INTRODUCTION

Blockchain technology is historically inseparable from the creation of Bitcoin, the character of Satoshi Nakamoto and the Bitcoin article published on October 31, 2008: *A Peer-to-Peer Electronic Cash System*[2]. Increasingly, it is described as the most important invention since the creation of the Internet[3]. For several years, blockchain has been in the top ten list of the Council for New Technologies of the World Economic Forum in Davos, which is preparing a list of the most breakthrough technologies that have the greatest impact on improving the lives of societies, transformation of subsequent sectors of the economy and environmental protection[4]. Interest in its essence is also growing, as part of scientific and media discourse. Sometimes referred to as the next or trusted layer of the Internet[5]. Although cryptocurrencies are and will remain a natural, primary area of application of BCT, the possibility of using it is not limited to digital money. A decentralized network in various forms is implemented in the subsequent areas of functioning of institutions from the banking sector, private companies, and other organizations, where security plays a key role[6].

Daniel Drescher points out that the blockchain does not evaluate processed data, hence their scope as well as the number of areas of potential application is as wide and varied as the scope of human activity. As examples, he mentions: payment management, use in creating digital resources or digital identity. The blockchain can also be used, for example, in the digitization, storage and verification of documents and contracts, proofs of ownership, in the

[2] *Vide* S. Nakamoto, *Bitcoin: A peer-to-peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (02.01 2020).
[3] J. De Silva, K. Parker, P. Broun, *Blockchains – „The most importation since the internet it* self", Murfett Legal Professionalism. Understanding. Results, https://www.murfett.com.au/MurfettLegal/media/Documents/Article/35-Blockchains-The-Most-Important-Invention-Since-the-Internet-Itself.pdf, (02.01.2020).
[4] In 2019, Blockchain technology came in fifth on the list. *Vide* A. De Nisco Rayome, Innovation, *TOP 10 emerging technologies od* 2019, https://www.techrepublic.com/article/top-10-emerging-technologies-of-2019/, (03.01.2020).
[5] W. Mougayar, *The Business Blockchain: Promise, Practice and Application of the Nest Internet Technology*, Hoboken 2016, pp. 30-36.
[6] *Vide* e.g. M. Swam, *Blockchain: Blueprint for a new economy*, Sebastopol 2015; D. Tapscott, A. Tapscot, *Blockchain Revolution: How the Technology Behind Bitcoin is CHanging Monety, Business and the World*, Penguin, London 2016.

provision of notary services, conducting audits of audit services, or in voting during elections[7]. However, this set is not closed, because discussing all applications of the blockchain is practically impossible. However, it should be expected that new areas of implementation will constantly appear. This is because the decentralized network, distributed across hundreds of computers around the world, based on encryption using the public and private key is a secure structure for storing and transferring information and data. The blockchain can therefore potentially be used to streamline any processes and activities that require secure information or data transfer. Blockchain, as the name suggests, literally resembles a chain of subsequent blocks containing fragments of data previously entered into the system. Each transaction is saved in the list as a block containing specific data, which is attached to the previous one and together they form an inseparable chain. Hence, the name of this solution – a chain of blocks, although S. Nakamoto originally used the term chain of blocks in his article[8]. However, within a few years, the term blockchain was widely adopted. In practice, Blockchain is an electronic list in which individual operations are recorded chronologically. It is a distributed data register. Thanks to the technology used, the entered data is stored in many locations, because the database operates in a peer-to-peer[9] (P2P) network without a central unit. Blockchain functioning is based on known cryptographic solutions, such as hash function or asymmetrical cryptography. The decentralized database designed in this way, consisting of tens of thousands of users, based on proof of work and a trusted mechanism of distributed data transfer confirmation, is a secure structure for storing and using information and data. Importantly, the blockchain protocol ensures the integrity of data exchanged between system participants, without having to pass them through a third party. The elimination of the broker makes the exchange of information through it safe and fast.

The aim of the article is to analyze the potential of using blockchain technology to strengthen state security. There is a *consensus* among representatives of the social sciences that security, in the most general sense, includes satisfying human needs such as existence, survival, wholeness, identity, independence, peace, possession, and certainty. Security is subjective and can be defined as the certainty of existence and survival, ownership, and functioning, as well as the development of the entity. This certainty is the result of not only the lack of threats, but it is created primarily as a result of the creative activity of a given entity, it is changeable in time. As the basic typologizing criterion for security in science, it is considered subjective and based on it national security. Understood as state security, which is an individual category and refers to individual states, their societies, and nations. International security, which is the term

[7] D. Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, CA: Berkley 2017, pp. 226-227.
[8] S. Nakamoto, *op. cit.*, p. 7.
[9] In a peer-to-peer network, each node is equivalent, the network is distributed. This means that any user connected to the network can send and receive data. Each of the network elements can simultaneously act as a server and client (the opposite of a classic client-server network), which makes it possible to simultaneously download files and make them available to all network participants. *Vide* R. Schollmeier, *A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications*. In: *Proceedings First International Conference on Peer-to-Peer Computing* 2001, pp. 101-102.

usually used to characterize the security of a given population of states, including the international system. The second, often used criterion in the auxiliary security typology is the subject approach, on the basis of which the following types of security are distinguished: political, military, economic, social, cultural, ideological, and ecological[10]. In the presented study, the author refers to the subjective criterion as the leading criterion, in the center of which is the institution of the state.

The basic problem considered in the article is the question of the possibility of implementing blockchain technology in the area of defense. The study is divided into two parts. In the first one, the author presents a historical outline of technology development while indicating the most important elements of the blockchain structure from the development perspective. In the second – analytical, trying to answer the key research question – what military application is or may have in the foreseeable future blockchain technology, and how its use by armies can contribute to improving state security? Therefore, the areas of implementation of blockchain technology in national defense will be will be analyzed, and the aim is to identify and describe them. The starting point will be a report prepared by Neil B. Barns, United States Air Force major. In his study, he pointed out that blockchain technology can contribute to: (1) maintaining security in cyberspace, mainly in the area of data transmission and integrity, (2) supply chain management of products and services for the army, especially in emergency situations, (3) and for effective and reliable communication[11]. Secondary research on which the following study is based is an analytical technique used in classified research. As part of non-reactive research, secondary data analysis and comparative research are used. In the presented article, the source material includes data found in the form of: scientific studies, official reports as well as clippings and media reports.

THE ESSENCE OF BLOCKCHAIN TECHNOLOGY. HOW BLOCKCHAINS WORK?

In 2009, the first practical implementation of solutions appeared, on which cryptography specialists had been working for several decades. The idea of a cryptographically secured blockchain was presented as early as the early 1990s by Stuart Haber and William Scott Stornett[12]. However, it was only with the creation of Bitcon that the first practical implementation of specific technological solutions was made. At that time, for the first time in history, the problem of reaching consensus in a distributed environment with an untrusted network of participants was solved. Public key cryptography and Proof of Work (PoW)[13] were

[10] *Vide* R. Zięba, *Instytucjonalizacja Bezpieczeństwa Europejskiego – koncepcje – struktury – funkcjonowanie*, Warszawa 1999, pp. 27-36.
[11] N.B. Barnas, *Blockchains in national defense: Trustworthy systems in a trustless world*, Alabama 2016, pp. 28-31.
[12] *Vide* S. Haber, W.S. Stornetta, *How to Time-Stamp a Digital Document*, In *Conference on the Theory and Application of Cryptography*, Heidelberg, pp. 437-455.
[13] In addition to PoW, there are other ways to get consensus. One of the more popular is the so-called Proof of Stake. It has been implemented in a blockchain version called Serenity. This algorithm is based on the assumption that each user is properly involved in the system. It is based on the amount of currency held - the greater the number of units of a given cryptocurrency is in the system participant's possession, the greater the chance that he will create

used to provide a secure, controlled, and decentralized method of generating digital currency and to ensure that consensus could be reached. The most important innovation was organizing the list of blocks that make up the transaction and are cryptographically secured using a proof of work mechanism. The simplified definition indicates that the blockchain is an ever-growing, secure, common record keeping system in which each user stores a copy of the data. The chain can only be updated if all parties involved in the transaction agree. The technical definition, in turn, suggests that blockchain is a distributed register operating in a peer-to-peer network, which is cryptographically secure, allows only the addition of data, is non-modifiable and updated only on the basis of consensus between its users[14].

Based on the evolution and development directions of blockchains in recent years, they can be divided into several categories that have different attributes. Due to the possibility of access to the register, a public and private blockchain can be distinguished. The public chain is available to anyone who can participate in block decision-making. All system participants store a copy of the registry at the local node and use the mechanism of achieving consensus in a distributed environment to decide on the final state of the registry. Bitcoin, Ethereum are examples of a public chain. A private chain, in turn, is defined only for a specific consortium, organization, or group of people who share the register with each other. Examples of private blockchains are HydraChain and Quorum. Although both optionally can become public, they are intended to operate in private mode. Others, apart from the two most popular solutions, include the situation when the chain is partially private (sometimes called federal[15]), i.e., a fragment of the chain is private and the rest is public; side chain (pinned), allowing you to transfer funds from one blockchain to another and back, used to create altcoins[16].

Another division that Krzysztof Piech draws attention to indicates that the blockchain can be shared with network participants with prior permission (permissioned) or shared with anyone (permissionless). In this case, the bitcoin chain is included in the second category and is undeniable. This means that you can only add information to it and not correct the existing ones. A few years ago, the concept of corrected blockchains appeared, allowing interference with

a new block. The most popular example of PoS implementation is Ethereum. An innovative solution has been used for another consensus mechanism, i.e. Delegated Proof-of-Stake. In this case, the node that checks the correctness of the new block is selected by voting. Only delegates are allowed to add new blocks to the blockchain, for which they receive rewards. Consensus based on dPoS was used, e.g. in BitShares. W. Li et al.., *Securing Proof-of-Stake Blockchain Protocols*, (ed.) J. Garcia-Alfaro et al, *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, ESORICS International Workshops DPM, Oslo 2017, p. 297-315. In the literature, in addition to the consensus algorithms described above, the most popular are: Proof of Elapsed Time, Proof of Deposit, Proof of Importance, Proof of Activity, Proof of Capacity, Proof of Storage. However, this list is not complete, but contains the most important algorithms. *Vide* I. Bashir, *Mastering blockchain*, Birmingham 2017, pp. 28-30.

[14] I. Bashir, *op. cit.*, pp. 16-17.

[15] Biance Academy, *Private, Public and Consortium Blockchains - whats-the Difference?*, https://www.binance.vision/pl/blockchain/private-public-and-consortium-blockchains-whats-the-difference, (06.01.2029).

[16] I. Bashir, *op. cit.*, pp. 24-27. *Vide* D.L.K. Chuen, R. Deng, *Handbook of blockchain, digital finance, and inclusion: cryptocurrency, fintech, insurtech, regulation, Chinatech, mobile security, and distributed ledger*. Volumen 2, Academic Press 2017, pp. 145-177.

historical data contained therein. This solution is most often used in private chains used by commercial entities[17]. Despite the differences, each blockchain is:

- electronic combined list;
- some blockchain data is included in each node;
- each node contains a cryptographic abbreviation of the preceding node and a time stamp
- several network participants enter information into the system independently at one time[18].

On the basis of constitutive features, a definition has been built defining blockchain as a type of database that contains a number of records collected in the block. Each block is connected to the next using a cryptographic signature. The chain of blocks in which the chronological continuity of transactions is recorded is a distributed registry that can be shared and confirmed by anyone with the appropriate permissions[19].

The individual elements that make up the distributed registry technology are primarily cryptographic solutions, such as: hash function, hash trees, and public key infrastructure. The first on which blockchain technology is based, and thus Bitcoin, is the hash function, i.e., the result of the hash function. Hash function is one of the most important elements of modern cryptography. This is a function that assigns to any large string any string having a nonspecific value of a fixed size. It always contains a fixed number of bits. The cryptographic hash function should additionally fulfill such properties as: unidirectionality, resistance to a second counter picture, and the so-called "collision"[20]. The calculation of the hash is an easy task, and the opposite is practically impossible. The Bitcoin system uses the RIPEMD 160 and SHA-256 algorithms. RIPEMD in the blockchain is used to create Bitcoin addresses, and the SHA-256 algorithm is used to verify the computational effort generated by miners. The hash function based on the 256-bit SHA algorithm is a precompiled access contract at address 0x2 and generates the SHA256 hash input. The amount of fuel required for the algorithm depends on the size of input data. In the case of the SHA-256 algorithm, the input data can be up to 32-bit. The hash function based on the 160-byte RIPEMD algorithm is used to create the 160-bit RIPEMD hash and is available at address 0x3. The output from this function is a 20-byte value. The amount of fuel required to generate it, similar to SHA, depends on the amount of input data[21].

The hash function for Bitcoin is used to implement a second cryptographic tool, which is a digital signature. In order to eliminate the intermediary, the system developers used public key cryptography and an open transaction register, which is stored in the so-called blockchain.

---

[17] K. Piech, *Leksykon pojęć na temat technologii blockchain i kryptowalut*, Warszawa 2016, p. 6

[18] *Vide* P. Włodarek, *Enterprise blockchains are a HUGE overpromise*, 2.11.2016, https://medium.com/the-blockchain-times/enterprise-blockchains-are-a-huge-overpromise-7ca2d19324b3 (08.01.2020).

[19] Distributed Ledger Technology: beyond blockchain. A raport by the UK Government Chief Scientific Adviser, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, (10.01.2020), pp. 17-21.

[20] P. Rodwald, *Kryptograficzna funkcja skrótu*, „Zeszyt Naukowy Akademii Marynarki Wojennej" 2013 nr 2 (193), pp. 91-92.

[21] *Vide* I. Bashir, *op.cit.*, p. 222-227 or L. Wang, X. shen, J. Li, et al., *Cryptographic primitives in blockchains*, „Journal of Network and Computer Applications" 127, pp. 43-58.

The digital signature is the second of the cryptographic mechanisms that is used to provide users with authentication of transactions between network nodes. The operation of the digital signature is based on the use of the Rivest Shamir Adleman (RSA) algorithm[22]. The algorithm for creating a digital signature using RSA is a two-step process. The data package abbreviation is calculated first. At this stage, data integrity is ensured because the hash can be recalculated on the recipient side and matched to the original hash to check that the data has not been modified during the transfer. The shortcut is signed using the sender's private key because only the signing entity has the private key specified. In this second step, units receive a guarantee of signature authenticity and data signature. Digital signatures therefore have several important features. First, they are authentic, which means that the recipient can check the correctness of digital signatures. They are also unaffected, which means that you cannot generate a signed message other than that created by the legitimate sender. They are also disposable, which means that the key can be used only once. This signature is unique for each data set and contains information about the sender, content, and time of the event[23].

To eliminate the intermediary, the system developers used public key cryptography and an open transaction register, which is stored in the so-called blockchain. Encryption and data transfer is possible thanks to the use of cryptography. Bitcoin uses asymmetric cryptography. Asymmetric key cryptography uses a pair of keys: a public key and private key, which are mathematically related to each other, using usually the Euler function. Private keys are used to digitally sign transactions. Public keys are used to output addresses, enabling a one-to-many pseudonymous approach. Public keys are used to verify signatures generated using private keys. Asym Asymmetric key cryptography allows you to check if a user passing a value to another user has a private key that is able to sign the received messages. The private key should be stored in a safe place, because its loss will result in the inability to use the cryptocurrency. Private keys are used to digitally sign transactions. The private key is 256-bit randomly selected numbers from the range specified in the Elliptic Curve Algorithm (ECDSA) recommendations. The private key is usually encoded in the Wallet Import Format (WIF), which makes it easy to copy and use. WIF allows you to save the complete private key in a different format. Data in WIF format can be converted into a private key and vice versa[24].

The public key is in blockchains and all network users have access to them, so it is widely available and published by the owner of the private key. Public keys are generated based on private keys due to the mathematical relationship between key types. When a transaction signed with a private key is distributed in the Bitcoin network, public keys are used by the nodes to check that the transaction has actually been signed with the appropriate private key. The basic feature of blockchain technology is the ability to build connections in a peer-to-peer network

[22] Digital Signature Algorithm (DSA) is another popular algorithm used for digital signatures.
[23] *Vide* I. Bashir, *op.cit.*, pp. 95-98 or L. Wang, X. Shen, J. Li, *op. cit.*
[24] *Vide* E. Vaskovskyi, *Technologia blockchain – możliwości zastosowania,* Ośrodek Badań i Analiz Systemów Finansowych ALTERUM, http://alterum.pl/uploaded/EVblockchain.pdf, (12.01.2020), p. 13.

between system participants, which eliminates the need for a parent unit that controls the transaction. Blockchain is the technology behind digital currencies that ensures that every transaction is carried out and saved correctly.

In the case of Bitcoin, blockchain is a distributed, fully decentralized database that maintains a constantly growing list of records that are checked, verified, and then grouped into blocks. Each of these blocks contains: a time stamp, a cryptographically calculated checksum, and the checksum of the previous block. This means that in such a chain the history of a given coin's flow is stored - whether it is the state of the currency account or, for example, the location of the product in the world warehouse. Thanks to this construction, the blockchain bitcoin is perfectly transparent, which further increases the credibility of its records. You can trace the complete history of each bitcoin from the moment the system was created to the current day, quite differently than in the case of traditional cash[25].

In his article, S. Nakamoto lists the following phases of the registry:

1. sending new transactions to all nodes in the system;
2. collecting transactions in the block by each of the nodes;
3. searching for each block's processing certificate for its block;
4. after finding the solution, send the block to all other nodes;
5. block acceptance only when all transactions contained in it are correct;
6. proof of block acceptance is starting processing of the next block, which adopts the hash of the block that has just been accepted[26].

The S. Nakamoto project was presented to the public in 2008, and the first online transaction was carried out in January 2009. A year later, the concept of creating a decentralized name system for Internet domains - BitDNS appeared - and in 2011 Namecoin was launched. This was the first example of using a blockchain for purposes other than cryptocurrencies. Namecoin forms the basis of a decentralized domain name system, i.e., URLs that can put an end to online censorship. The existence of a decentralized domain name system means that there may be Top Level Domain domains that are not owned by anyone[27].

An important element in the development of blockchain technology was 2013. At that time, Vitalik Buterin stated that Bitcoin needs a scripting language to build decentralized applications[28]. Due to the lack of agreement with the community, Bitcoin began work on a new, distributed and decentralized platform for processing computer data based on blockchain technology. He announced his concept on January 23, 2014. At that time, the software development of a new blockchain-based network began. The first version of Ethereum,

[25] M. Grzybowski, S. Bentyn, *Kryptowaluty: dlaczego jeden bitcoin wart będzie milion dolarów?,* Poznań 2018, p. 27.
[26] S. Nakamoto, *op. cit.*, p. 3.
[27] D. Gilson, *What are Namecoins and .bit domains?*, https://www.coindesk.com/what-are-namecoins-and-bit-domains, (12.01.2020).
[28] V. Buterin, *Ethereum White Paper: A next generation smart contract & decentralized application platform*, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, (14.01.2020), pp. 11-13.

Olympic, was released in May 2015. Two months later, in July 2015, the Frontier version was introduced. Around 2016, the Homestead version appeared with various improvements, and the final version is Serenity. In the authors' intention, the Ethereum chain is to offer new functional possibilities not available in Bitcoin.

The creators of the system sought to develop a complete language in the Turing sense[29], which would give the possibility to write any programs for the blockchain and create decentralized applications. This approach differs from the model used in Bitcoin, where the scripting language is inherently limited and allows only the necessary operations to be performed. The authors therefore designed a solution in which it would be possible to use applications / scripts that perform practically any calculations or store data. The most important achievement of Ethereum is the design of Smart Contracts, which, after joining the blockchain, remain unchanged and operate as originally programmed. Thanks to the existence of smart contracts, it is possible to add further automation functions to the blockchain based on a set of rules specified in the contract. In the author's intention, the Ethereum network was to become not only a registry recording cryptocurrency transactions, but also a "global computer" – a platform that allows creating distributed applications using the benefits of blockchain technology on which they would be embedded. Ethereum is an open source platform that allows you to develop your own decentralized applications within Blockchain[30]. Finally, Ethereum was launched on July 30, 2015, and since then it has been constantly developing as a kind of alternative to the world's first cryptocurrency.

Final, as Vikram Dhillon and other co-authors point out in their work *Blockchain Enabled Applications*, it can be stated that two schools formed representing different views on the script language, which in functional terms, from the point of view of the construction and use of the blockchain, is the most important difference. S. Nakamoto's proposal is an example of a classic approach and a scripting language with very limited functionality was proposed there. This avoids problems with the security of the entire system. This functionality is sufficient to create registers, which is the basic task of Bitcoin. V. Butarin perceived the blockchain as more than just a register. He proposed a blockchain that will be a calculation platform. In his design, the Ethereum Virtual Machine (EVM) chain could perform well-defined functions using contracts and arguments. The design of the machine will allow complete isolation of executable code and safe operation of applications based on it[31].

[29] The creator is Alan Mathison Turing, a British mathematician cryptologist, creator of the Turing machine and one of the creators of computer science. Turing's language is a general-purpose language, meaning it is potentially the language of choice for a wide range of applications. The assumption is to improve the operational reliability of the application, increase performance and increase the level of security of the devices working on it. *Vide* R.C. Holt, J.R. Cordy, *The Turing language report*. University of Toronto. Computer Systems Research Group, Toronto 1983.

[30] B. Klinger, J. Szczepański, *Blockchain-historia, cechy i główne obszary zastosowań*, „Człowiek w cyberprzestrzeni" (1) 2017, p. 13-14.

[31] V. Dhillon, D. Metcalf, M. Hopper, *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You*. Apress, Orlando 2017, p. 26.

MILITARY USE OF THE BLOCKCHAIN

The properties of blockchain technology indicated and characterized above indicate high potential, which is increasingly often noticed in various areas of society life. New opportunities are constantly noticed by specialists in other areas of social life. After a visible lack of trust and caution, observed especially in the first period of blockchain operation, work on the implementation of new concepts accelerated in 2013. After more than four years of operation, it was noticed that blockchain is a stable technology, the application of which brings the expected results and gives a chance to make a technological leap.

It was therefore natural that the idea of using blockchain technology in the area of national defense, in which gaining technological advantage is a source of success, and sometimes determines the final result of actions. There are more and more voices that blockchain will revolutionize the traditional war paradigm, and that the armed forces must use the potential of blockchain technology to be effective[32]. Available data shows that work on the use of blockchain technology in the military field is carried out by the three largest powers: the United States of America, the Russian Federation, and the People's Republic of China. In turn, countries such as South Korea and India announced pilot test programs in 2019. Potential that can be used to strengthen security also seems to be noticed by the North Atlantic Alliance (NATO). Anders Fogh Rasmussen, the former Secretary General of the Alliance, has repeatedly pointed out in press interviews that securing data transfers using blockchains in the future will be commonplace[33].

The first area where blockchain technology can be implemented is to ensure security in cyberspace. Already in 2008, after the largest cyberattack on Estonia[34], a report was created that pointed to the value of nonmilitary aspects of warfare[35]. According to contemporary forecasts, the war of the future will be waged in cyberspace and armies should make efforts to be ready for such threats. In practice, this means, as the *DoD Digital Modernization Strategy* report, developed by the US Department of Defense, indicates that blockchain is an information technology that potentially reverses the cyber security paradigm[36]. Decentralization of the blockchain makes it an ideal technology to be used to ensure security in cyberspace. With it, you can securely send sensitive medical or financial data. Blockchain is virtually indestructible because each participant stores the transmitted data. Any attempt to destroy or otherwise

[32] *Vide* IANS, *Armed forces must be equipped to meet challenges of moder warfare: Rajnath Singh*, https://timesofindia.indiatimes.com/india/armed-forces-must-be-equipped-to-meet-challenges-of-modern-warfare-rajnath-singh/articleshow/71889592.cms, (16.01.2020).

[33] A. Singer, *weaponizing Blockchain – Vest Potential, but Projects Are Kept Secret*, https://cointelegraph.com/news/weaponizing-blockchain-vast-potential-but-projects-are-kept-secret, (16.01.2020).

[34] *Vide* e.g. W.C. Ashmore, *Impact of alleged Russian cyber attacks*, "Baltic Security & Defence Review" 11(1), 2009, p. 4-40.

[35] National Intelligence Council (US), *Global trends 2025: A transformed world*. National Intelligence Council 2008, https://www.files.ethz.ch/isn/94769/2008_11_Global_Trends_2025.pdf, (20.01.2020), p. 71 and all.

[36] D. L. Norquist, *DoD Digital Modernization Strategy: DoD Information Resources Management Strategic Plan FY19-23*. OSD Washington United States 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF, (22.01.2020), p. 48.

interfere with the book would require interference among all network nodes at the same time. The computing power that would potentially have to be used for such an attack would exceed the power that all countries in the world could potentially generate. Hacking the chain is therefore impossible.

Blockchain technology can potentially be used, for example, to ensure security in an atomic weapons system. In 2010, the Armed Forces of the United States of America lost their ability to communicate with 50 ICBM Minuteman III ballistic missiles for forty-five minutes. Then there was a suspicion that there might have been unauthorized access[37]. As indicated by the Royal Institute of International Affairs, one of the most important think tanks researching international relations, in its 2018 report - the likelihood of cyberattacks on the nuclear weapons service system is relatively high. The threat in this case comes from both hostile countries and other non-state actors, such as terrorist organizations[38]. The implementation of blockchain technology seems to be the ideal answer to this defined threat, because in this case it is not possible to lose control. The potential of blockchain technology and its use to increase security in cyberspace is also recognized by representatives of the Russian Federation. On June 25, 2018, under the decree of President Vladimir Putin No. 364, the *Era Military Innovation Technopolis Research Center* was established[39]. The task of ERA, in cooperation with the Eighth General Staff of the Armed Forces of the Russian Federation, will be to develop blockchain technologies seeking to implement. According to the assumptions, blockchain technology can be used in the Russian army to protect data in cyberspace and detect and neutralize hacker attacks. The development of an intelligent system for detecting and preventing attacks in cyberspace on facilities with critical information infrastructure of the Armed Forces of the Russian Federation is one of the ERA's priorities[40].

The second potential area where blockchain technology can be used in the military field is to increase the efficiency of military supplies. Supply chain management of products and services for the military, especially in emergency situations in difficult regions of the world, is crucial to the final settlement. The proper implementation of the tasks set for the army requires the provision of a wide spectrum of material resources, ranging from the simplest, such as supplies for consumption or medical products to materials used on the battlefield. The supply chain is created by people and companies involved in the creation and distribution of a specific product or service - from initial suppliers to end users and customers. Today, almost every supply chain management system, regardless of whether civil or military, strives to achieve

[37] N. Shachtman, *Comm*unication With 50 Nuke Missiles Dropped in ICBM Snafu, https://www.wired.com/2010/10/communications-dropped-to-50-nuke-missiles-in-icbm-snafu/, (23.01.2020).
[38] T. Adams, *Why Military blockchains is Critical in the Age of Cyber Warfare,* https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619, (23.01.2020).
[39] Министерство обороны Российской Федерации (Минобороны России), *Военный инновационный технополис «ЭРА»*, http://mil.ru/era.htm,
[40] Н. Сурков, А. Рамм, *Блокчейн оденут в камуфляж - В военном технополисе разрабатываются уникальные средства выявления хакерских атак*, https://iz.ru/758288/nikolai-surkov-aleksei-ramm/blokchein-odenut-v-kamufliazh, (24.01.2020).

adequate efficiency and transparency. The vast majority of supply networks encounter difficulties when trying to integrate all parties involved in the process.

For a supply chain system to be defined as an efficient data flow, it must be smooth. Blockchain technology provides new ways to record, transfer, and share data. In addition, the network is designed as a distributed system, so by definition it is highly resistant to any modifications. To make modifications, the entire network must agree to this. It is therefore, as already indicated, an ideal space for providing information, and those in the supply chain are, for example, information about the location of products, or current information about the owner of the product. Each participant can therefore check what is happening with a particular product and when it reaches its destination[41].

In the case of using blockchain in the supply chain for the army, one should also pay attention to the potential economic benefits of implementing the above solution. The experience of other industries[42] indicates that technology, e.g., makes it easier to track products along with data transparency, which helps to identify areas where resources are wasted. Supply chain management in the defense industry is a cumbersome procedure and has many strategic difficulties. Blockchain in the defense industry guarantees that the information will remain unchanged, as all parties involved in the exchange would agree to. Blockchain defense technology can potentially help remove and reduce the number of counterfeits and errors in defense contracts.

The fact that blockchain is based on a distributed registry makes it seem to be an ideal solution for providing a secure and stable link. Therefore, blockchains can be used by the military in the area of communication. One of the first potential attack vectors are traditional communication methods, and the first target will be, e.g., satellites or base transceiver station. Signal disturbance, interference with the message content, or suppression may potentially lead to communication paralysis. The ideal answer to these threats is blockchain. The mesh topology used is a decentralized communication alternative that allows nodes to communicate directly without a central unit. In addition, protection against unauthorized access by unauthorized persons is a component closely related to security in cyberspace. Here, the role of public and private key cryptography, which underpin the blockchain system and ensure security, should be emphasized.

The three areas characterized above seem to be the first and most natural at the moment in which blockchain technology can be used in the field of defense. However, these are not the only variants, because you can also indicate other, where such may be used. Regarding the original use of blockchain – cryptocurrencies, in the media we find information that Chinese

[41] *Vide* Blockchain Expert, *Blockchain in Defence and Security*, 24 april 2019, https://www.blockchainexpert.uk/blog/blockchain-in-defence, (24.01.2020).
[42] *Vide* K. Kosior, *Potencjał technologii Blockchain w zapewnianiu bezpieczeństwa i jakości żywności*, „Żywność: nauka-technologia-jakość" 2018 4 (117), pp. 18-32.

soldiers can receive part of their salary in digital currency[43]. The Middle Kingdom is increasingly entering the cryptocurrency market, which is why the potential remuneration received in this form may become increasingly popular over time, especially in view of the relative stabilization of cryptocurrency markets.

CONCLUSIONS

The properties of blockchain technology mean that it can potentially be the answer to many civilization challenges that we face every day. Its dissemination will most likely contribute to the improvement of the quality of all people living on earth. The fact that blockchain technology is increasingly used in the banking sector or in the process of digitizing the lives of societies indicates its substantial potential. It is worth pointing out that blockchain is a relatively new technology, created and presented on the occasion of the first of cryptocurrencies - Bitcoin. In the following years, new ideas began to appear, which are based on the solutions proposed by S. Nakamoto. The dynamics of development indicates that it should be expected that its development will continue to progress and will only become fully functional in a few years, because the blockchain is not a static structure. Analysis of existing solutions indicates that so far it has been successfully implemented in the functioning of the so-called Internet of Things, in government institutions, healthcare, finance, and multimedia. However, this catalogue is not closed.

Blockchain technology can also help improve security. In the presented study, the author presented the potential possibilities of implementing blockchain technology in the military area. Due to their nature, these areas refer only to cyberspace, which, according to experts, will constitute the area of a new war waged in the 21st century. Therefore, increasing the level of security related to hacking resistance, protection against unauthorized access, or ensuring the security of communication and weapon management devices is potentially an area of technology implementation in the army's operations. Therefore, referring to the aim of the article, it should be indicated that the existing reports and studies indicate the possibility of implementing the technology in several key areas from the security perspective. Its further use may lead to a revolution in the field of defense and, in the longer term, to a change in the war paradigm.

Potential further directions in the development of the blockchain will primarily aim at improving the technology used. Hash functions, database structure, cryptography, and network architecture are the areas of intensive research, hence it should be expected that there will be intensive changes in this area. Another area that research and attempts to improve blockchain should focus on is improving the level of scalability. In this area, work will be carried out, for example, on: improving network performance or consensus algorithm. It is also worth emphasizing that concepts related to the functioning of the chain are constantly evolving.

[43] M. Huillet, *China's Army Considering a Blockchan Rewards System, Raport*, https://cointelegraph.com/news/chinas-army-considering-a-blockchain-rewards-system-report, (25.01.2020).

Therefore, it should be expected that their evolution in the near future will allow isolating further areas of potential implementation of blockchain also in the area of defense. Hence, the growing interest in technology signaled at the beginning of the article as part of media and scientific discourse. Technology is an interesting object not only for the representatives of technical sciences, but also, for example, for economists, lawyers, or representatives of other social sciences. The dynamics of its development indicate that it will both gradually penetrate into subsequent areas of the individual's functioning that are of interest to these areas of life.

BIBLIOGRAPHY

Ashmore William Carlos. 2009. "Impact of alleged Russian cyber attacks". Baltic Security & Defence Review, 11(1): 4-40.

Barnas Neil.B. 2016. Blockchains in national defense: Trustworthy systems in a trustless world. Blue Horizons Fellowship, Alabama: Air University, Maxwell Air Force Base.

Bashir Imran. 2017. Mastering blockchain. Birmingham: Packt Publishing Ltd.

Biance Academy. 2020. Private, Public and Consortium Blockchains - whats-the Difference?, https://www.binance.vision/pl/blockchain/private-public-and-consortium-blockchains-whats-the-difference.

Buterin Vitalik. 2014. A next-generation smart contract and decentralized application platform. white paper, http://blockchainlab.com/pdf/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Chuen Dave Lee Koa, Deng Robert. 2017. Handbook of blockchain, digital finance, and inclusion: cryptocurrency, fintech, insurtech, regulation, Chinatech, mobile security, and distributed ledger. Volumen 2, p. 145-177. Academic Press.

De Nisco Rayoma Alison, TOP 10 emerging technologies, https://www.techrepublic.com/article/top-10-emerging-technologies-of-2019.

De Silva Janson, Parker Kelly, Broun Peter, Blockchains – „The most importation since theinternet it self", Murfett Legal Professionalism. Understanding. Results, https://www.murfett.com.au/MurfettLegal/media/Documents/Article/35-Blockchains-The-Most-Important-Invention-Since-the-Internet-Itself.pdf.

Dhillon Vikram, Metcalf David, Hooper Max. 2017. Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Orlando: Apress.

Drescher Daniel. 2017. Blockchain Basics: A Non-Technical Introduction in 25 Steps. Berkley: CA: Apress, Berkley. p. 223-233.

Gilson David. 2013. What are Namecoins and .bit domains?, https://www.coindesk.com/what-are-namecoins-and-bit-domains.

Grzybkowski Michał, Bentyn Szczepan. 2018. Kryptowaluty: dlaczego jeden bitcoin wart będzie milion dolarów?. Poznań: Wydawnictwo Crypto-logic Sp. z o. o.

Haber Stuart, Stornetta Wiliam Scott. 1990. How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography. Berlin-Heidelberg: Springer, p. 437-455.

Holt Ric, Cordy James Reginald. 1983. The Turing language report. University of Toronto. Computer Systems Research Group.

IANS. 2019. Armed forces must be equipped to meet challenges of moder warfare: Rajnath Singh, https://timesofindia.indiatimes.com/india/armed-forces-must-be-equipped-to-meet-challenges-of-modern-warfare-rajnath-singh/articleshow/71889592.cms.

Klinger Bartłomiej, Szczepański Jacek, 2017. „Blockchain-historia, cechy i główne obszary zastosowań". Człowiek w cyberprzestrzeni (1): 11-27.

Kosior Katarzyna. 2018. „Potencjał technologii Blockchain w zapewnianiu bezpieczeństwa i jakości żywności". Żywność: nauka-technologia-jakość 4 (117), p. 18-32.

Li Wanting, Andreina Sebastien, Bohli Jens-Matthias. Karame Ghassan. 2017. Securing proof-of-stake blockchain protocols. In Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham: Springer, p. 297-315.

Mougayar William. 2016. The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons. p. 30-36.

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

National Intelligence Council (US). 2008. Global trends 2025: A transformed world. National Intelligence Council.

Norquist David L. 2019. DoD Digital Modernization Strategy: DoD Information Resources Management Strategic Plan FY19-23. OSD Washington United States.

Piech Krzysztof. 2016. Leksykon pojęć na temat technologii blockchain i kryptowalut. Warszawa: Ministerstwo Cyfryzacji.

Rodwald Przemysław. 2013. „Kryptograficzne funkcje skrótu". Zeszyty Naukowe Akademii Marynarki Wojennej 54(2) (193):. 91-102.

Shachtman Ndah. 2010. Communication With 50 Nuke Missiles Dropped in ICBM Snafu, https://www.wired.com/2010/10/communications-dropped-to-50-nuke-missiles-in-icbm-snafu.

Schollmeier Robert. 2001. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In Proceedings First International Conference on Peer-to-Peer Computing, 101-102. IEEE.

Singer Andrew. 2019. Weaponizing Blockchain – Vast Potential, but Projects Are Kept Secret, https://cointelegraph.com/news/weaponizing-blockchain-vast-potential-but-projects-are-kept-secret.

Swan Melanie. 2015. Blockchain: Blueprint for a new economy. "O'Reilly Media, Inc."

Tapscott Don, Tapscott Alex. 2016. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

Walport Mark. 2016. Distributed ledger technology: Beyond blockchain. UK Government Office for Science 1.

Włodarek Piotr. 2016. Enterprise blockchains are a HUGE overpromise, https://medium.com/the-blockchain-times/enterprise-blockchains-are-a-huge-overpromise-7ca2d19324b3.

Wang Licheng, Shen Xiaoying, Li Jing., Shao Jun, Yang Yixian. 2019. "Cryptographic primitives in blockchains". Journal of Network and Computer Applications 127: 43-58.

Vaskovskyi Eduaord. 2018. Technologia blockchain–możliwości zastosowania. Warszawa: Ośrodek Badań i Analiz Systemu Finansowego.

Zięba Ryszard. 2004. Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje-struktury -funkcjonowanie. Warszawa: Scientific Publisher „SCHOLAR".

Сурков Николай, Рамм Алексей. 2018. Блокчейн оденут в камуфляж. В военном технополисе разрабатываются уникальные средства выявления хакерских атак, https://iz.ru/758288/nikolai-surkov-aleksei-ramm/blokchein-odenut-v-kamufliazh [Surkov Nikolaj, Ramm Alieksiej. 2018. Blokchejn odenut v kamuflazh. V voennom

tekhnopolisie razrabatyvajutsja unikal'nyje sredstva vyjavlenija khakerskihk atak, https://iz.ru/758288/nikolai-surkov-aleksei-ramm/blokchein-odenut-v-kamufliazh].

Министерство обороны Российской Федерации (Минобороны России). 2018. Военный инновационный технополис «ЭРА» http://mil.ru/era.htm [Ministerstvo oborony Rossijskoj Federatsii (Minoborony Rossii). 2018. Voennyj innovatsijonnyj tekhnopolis "ERA" W http://mil.ru/era.htm].