International Journal of Applied Sciences: Current and Future Research Trends
(IJASCFRT)
ISSN: 2790-3990
https://ijascfrtjournal.isrra.org/index.php/Applied_Sciences_Journal

Innovative Approach for the Implementation of Blockchain in Command and Control Systems of Critical Infrastructure Networks

Topor Sorin*

National Institute for Research and Development in Informatics - ICI Bucharest, Romania
Email: sorin.topor@ici.ro

Abstract

Blockchain technology is becoming increasingly attractive for a series of decision-making processes based on the facilities of the digitized environment for any field of human society. The foundation of blockchain technology is data and information structured in a distributed and immutable ledger through cryptographic mechanisms and consensus protocols. In this paper, we present a critical analysis of the possibilities of implementing this technology at the level of critical infrastructure networks that are priority targets to hit in the event of a conflict situation. Using the SWOT method, we highlight the advantages of blockchain implementation and propose some directions for transforming vulnerabilities and weak points into opportunities for the development of decision support methods at the level of distributed critical infrastructures networks.

Keywords: Blockchain technology; Decision optimization; Critical infrastructures; Digitization; Cyber security.

1. Introduction

The rapid developments of communications and IT technologies have facilitated the emergence of conditions for the optimization of all decision-making processes, with a strong impact on the economic, socio-political and military fields. The advantage of the use of the Internet and the decision-making digitization has allowed the emergence of blockchain technology, which is becoming increasingly popular, being adopted in a variety of technical and social solutions. Its main strengths are decentralization [1], information exchange, the role of nodes and technical consents of data [2]. It is essentially a distributed ledger with lists of records called blocks. Inside a block, information is processed through algorithms in technical and/or human memories. The resulting product is information distributed to the other blocks characterized by a time and a hash value.

Received: 3/29/2023
Accepted: 4/22/2023
Published: 5/13/2023

---

* Corresponding author.

Any activity performed by a block changes the hash for the subsequent block. This technology is attractive for its implementation in a C2 (command and control) system by the method of information encryption, namely the allocation of hash to each resulting information and communicated to all blocks. Chowdhury sees blockchain as a very good secure distribution of digital assets for untrusted clients [3]. At the level of critical infrastructures, a blockchain-based SCADA (Supervisory Control and Data Acquisition) system would solve many problems arising during crisis situations (disasters or terrorism) and war. SCADA and blockchain are two different technologies. SCADA is used to monitor and control industrial processes and blockchain is a distributed ledger (DLT) for recording and managing data and information transactions. However, blockchain can be used in SCADA to ensure the security and integrity of data in the system being different depending on the type of blockchain used (public, private or hybrid) as well as according to its purpose (requirements and technical specifications), known being the fact that there are currently many blockchain platforms such as Ethereum, Hyperledger, Corda etc., each with their own programming software and consensus protocols. We believe that in an automated system the role of a blockchain is established from the design phase. Our research focuses on hybrid systems with human-machine interaction. Within such a system, information is destructured into data that can be processed through the algorithms of a distributed ledger. Thus, the basis of the SOWT method we want to highlight the advantages and disadvantages of using blockchain in hybrid C2 systems for critical infrastructures.

2. Critical Analysis of Concepts of Blockchain Versus Traditional Command and Control Chain

Currently, this topic is highly analysed through the number of scientific publications and indexed patents. A simple search with Google Scholar identifies 632,000 already published (figure 1). Even if many of these are limited to results obtained through laboratory research simulations, the obtained results anticipate premises for the evolution of cyber technology and trigger useful analyses on some research directions and correction of those that do not lead to a positive evolution.

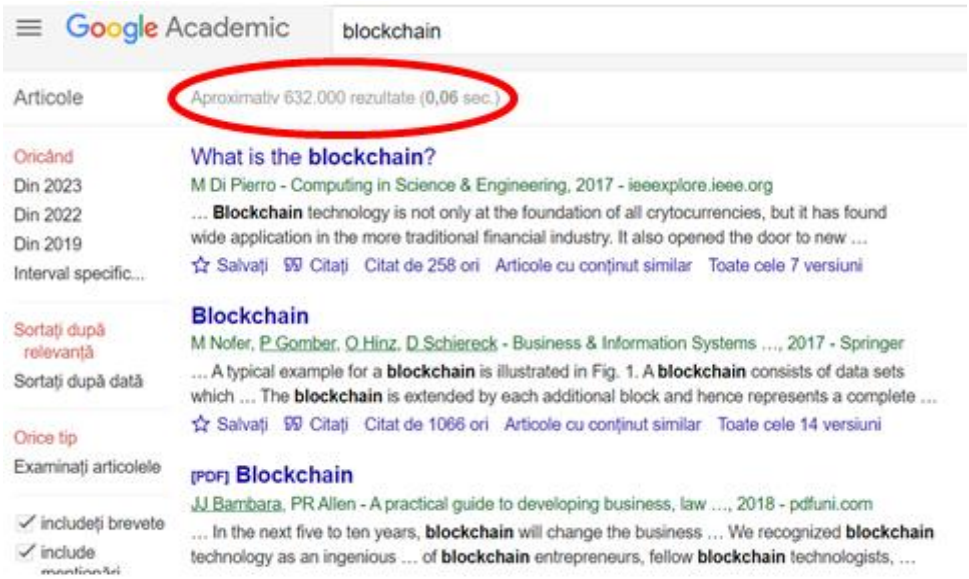

Figure 1: Works and patents with the topic of blockchain at March 15, 2023.

Overall, research findings indicate that blockchain is not just limited to digitization. This is a product that accumulates knowledge in all fields and provides safe and definite information. It is a kind of lt. commander Data, the famous android from the Star Trek series, who had the position of operational manager.

Currently, many blockchain-based structures are being experimented in various fields. It is observed that with small amounts of data they behave very well. But for full-scale applications big problems arise regarding very high processing times. Some of the technical solutions to reduce these times are parallel subchains, private blockchains, cloud codes in the form of "smart contracts", blockchain oracles for off-chain data interaction etc. The advantage of using the blockchain oracle is given by the fact that it also allows the import of data from anti-manipulation sensors, hardware devices that monitor a certain service such as scanning barcodes, heat alerts, importing data from logistics chains [4] etc. It is an artificial intelligence-based system that learns from its own representations.

Moreover, the products of a C2 system based on data and information use the historical mindset that leadership is achieved by rules. These are useful even if none of them are perfect. It is observed that artificial intelligence also preserves these customs but in digital ecosystems, the difference being that human intelligence is the perfect combination of explicit and tacit knowledge in order to achieve an objective. AI, still can't do that. Tacit knowledge is very difficult to explain even to humans. Likely to rely on emotion-based perceptions for one information set to the detriment of others. However, there are no scientific instruments to prove this hypothesis. But the advantage of using blockchain technology is determined by the transparent way of security of the data and information that is manipulate in the system. If an intruder connects to a network node (physical or virtual), by entering information with the same hash, he will be forced to leave the blockchain because all other nodes, except the attacked one, will have the unique version of that moment.

Thus, compliance with consensus protocols eliminates the possibility of executing any type of attack on information in a blockchain, excluding the possibility of data modification without the consent of all blocks. It is accepted that access to databases can be obtained relatively easily, with anyone being able to change the values of the stored data. However, blocks will not accept modified data without unanimous agreement. Information security is validated based on time and hash values. Encryption and hashing protect data change by being private, permanent and verifiable.

Thus, information transactions are transparent. But the technical platform that includes blockchain technology is big physical and logistical resources consuming, the operation is based on a distributed network.

We present a blockchain architecture model in figure 2.

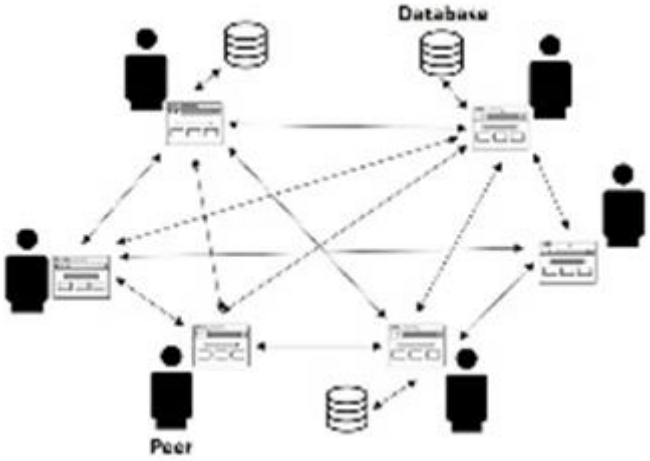

Figure 2: Structure of a blockchain-based decentralized network model [5].

The traditional decision-making way involves a series of operational optimization methods that are based on reducing the time values required for information processing sequences. In essence, they accumulate the effort to identify an operative solution of a group of specialists in various fields and the communication of the result for validation by the superior leader.

A blockchain-based decision algorithm is in Figure 3.

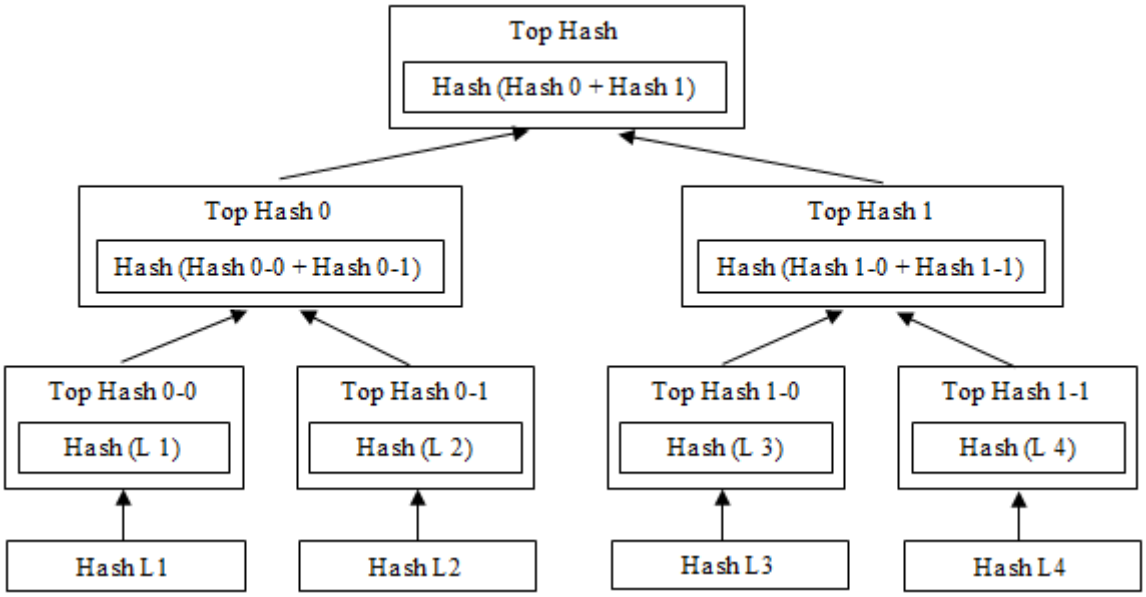

Figure 3: The structure of blocks in the blockchain [6].

The decision-making process is triggered by an input (the task information that also contains the presentation of the situation at that moment) to a senior leader who organizes, transmits, lead and establishes the objectives following which all staff members analyse the information, propose alternatives courses of actions, to identify

the vulnerabilities, strong and weak points of the proposed solutions, to create a matrix of synchronization of actions, finally, by consensus, to establish a concept to be validated [7] by the senior leader. Following its validation or modification, an optimal course of action is obtained that will provide the basis for planning future actions.

Apart from the fact that this method fundamentally depends on the perception, level of training and leadership style of the leaders, it can be modified periodically according to the evolution of the action.

A correct and timely decision requires a good knowledge of the real situation achieved through on-time and historical data and information, provided by a lot of sensors. The decision is communicated through established hierarchical network. Considering the need for quick triggering of the action, even during the decision-making process fragmentary commands can be issued to the execution elements, mainly for the purpose of preparing the action. Timing is of the essence to gain an advantage over a competitor or to surprise an adversary. The control of the fulfilment of the proposed objectives implies verification points of the fulfilment of partial objectives and the correction of the action in order to achieve the final objective.

As can be seen, the collection and transfer of information is a priority function of the decision-making system, which aims to anticipate events and adapt action to real time circumstances. In the event of an informational attack, based on the identification by the adversary of some vulnerabilities of the information and communications system, the specialists of the operations planning group can introduce into the analysis process information truncated or controlled by the adversary, distorting the evolution of the execution. Incidentally, this is the information warfare purpose.

Establishing the credibility of information involves a number of control components to compare it with other current and historical information, which assumes additional time. They are never considered when estimating the time to develop the decision. This sequence can be waived and all information entered in the processing process will be considered correct and accepted. But who bears such liability in case of failure? Conversely, other leaders may be overly suspicious and run additional checks, their overzealousness causing serious delays.

An optimal technical solution is to apply to management decentralization techniques, in order to transmit command authority to subordinate components to ensure freedom of action. It can be seen from afar that traditional management methods require competence, correct perception and common understanding of information, mutual trust, knowledge of action orders (total and partial), understanding of the senior leader's intention, disciplined initiative and risk acceptance [8].

In his study, Kambhampati notes that AI can be a useful tool or technology for many applications in the following three key areas [9]:

- Game theoretic models (eg to understand dynamic security paradigms for defending a moving target);
- Planning and reasoning methods (for example, to optimize logistics routes, to help discover previously unidentified attack paths etc.);

• Machine learning (eg to identify malware, intrusion detection etc.).

Kambhampati suggested that while there is an attraction to the advantages of ML for various security problems, AI is broader than ML and can be much more useful in terms of combining multiple approaches.

We present in figure 4 a model of the decision-making process for the fulfilment of a mission.

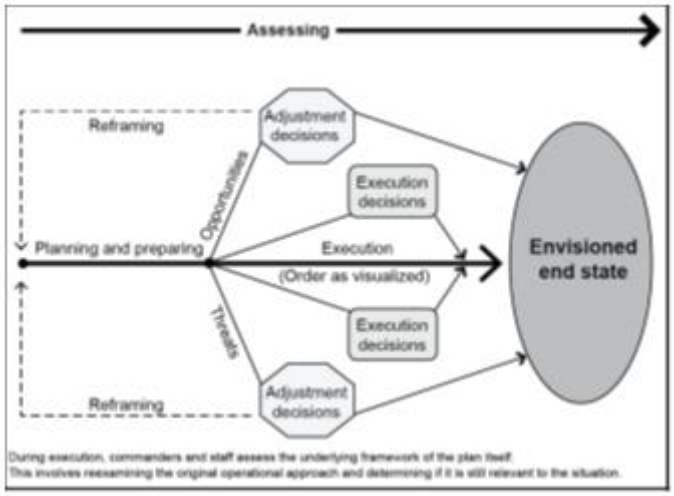

Figure 4: The decision-making process for accomplishing the mission [10].

3. Blockchain Method in Decision Assistance

Blockchain technology is extremely useful in uncertain information environments. A decentralized decision-making authority can avoid the discomfort created by the lack of confidence in the information provided and achieve maximum time values. This technology is already implemented in some logistics and financial activities. The most publicized examples are related to virtual currency trading, the delivery of goods in logistics flows, decision optimization in government projects etc.

We start from the premise that the optimization of the decision-making process within a critical infrastructure based on the principles of decentralized management can be achieved through blockchain technology. We propose the following blockchain model for decision support, which includes all hierarchical, strategic, operational, tactical levels and can ensure the management of the activities of tactical components (figure 5).

As can be seen the blockchain is a smart development framework based on a distributed network with a hierarchical structure. The network also contains functional but non-operative blocks, which ensure the reserve of the hierarchical echelon. They can also provide the role of decentralized storage environments. The advantage of such a solution is that in the event of a conflict characterized by material and human losses (specialists, experienced personnel etc.), damaged or destroyed blocks can be quickly replaced with already trained and functional ones.

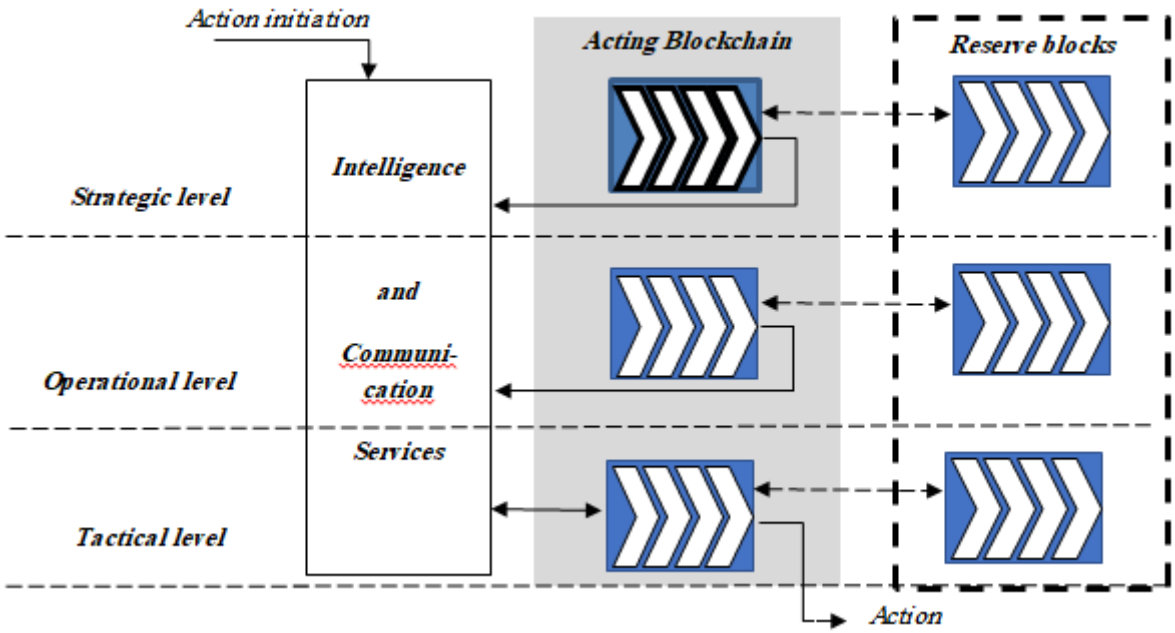

Figure 5: Multilevel blockchain model for decision optimization.

The focus is on those working on the block (creators, developers, miners, service etc.) and not just on the technical side of the network. For example: the informational ecosystem of critical infrastructures assigned to be hit, based on the combat action synchronization matrix, in the case of a military operation. We bear in mind the lessons learned from the war in Ukraine started by Russia in February 2022, in which, even if nuclear power plant sites were avoided, in addition to combatant units, energy facilities, communications, other industrial targets, which represented critical infrastructures, were hit in the war economy.

In the traditional system, for the validation of a decision in conditions of uncertainty, a third party accepted by all the actors is used to manage the risks and ensure the management of vulnerabilities. That is not blockchain no matter how digitized the decision-making processes and communication network. In the version proposed by the blockchain for decision support, the upgrade can be carried out up to the replacement of an entire hierarchical blockchain module, given that, at the tactical level, the physical erosion and destruction of the structures engaged in an action (crisis, conflict, normal activity in conditions of uncertainty etc.) is much more pronounced.

In our analysis we will use the SWOT method. The blocks of a blockchain-based critical infrastructure have the following aspects:

Inside the system:

A. Strengths:

- It has a single distributed network system for the transfer of information in order to fulfill the respective task/mission;

- It has only one point of information entry into the blockchain. Based on compliance protocols sensors are verified and accepted. Blockchain technology ensures the security of information blocks having the hash value;

- Blocks that do not perform, are damaged or are destroyed are quickly replaced. Damaged ones can be revitalized or abandoned;

- Sensor blocks can implement AI, VR and AR technologies for automatic assistance of information processing and decision sequences.

B. Weaknesses:

- The communication and information network must provide a mobile architecture with a high transfer rate and speed (probably 4G/5G). There are currently studies showing a multitude of vulnerabilities and risks for 5G network operators. We are not limited to current functional vulnerabilities. We believe that infrastructure poses great problems for optimal operation;

- The communication and IT system architecture is extremely large and complex. This implies very high costs for acquisition, update, upgrade and maintenance;

- The personnel providing technical and logistical support must be numerous and well trained in multidisciplinary fields, not only in communications and IT;

- The migration of specialists from a block must be drastically reduced, considering the preparation time for the specifics of the block's activity. For this, personnel policies are needed that keep human operators loyal to their position and do not routinize them. At the same time, reconversion programs are necessary in the event of a decrease in performance or its aging;

- The outsourcing of some services, such as those intended for gathering information or in the area of audit services to replace miners, must be carefully analysed based on the efficiency-cost ratio. Such services can produce additional costs compared to supporting own components even if they are exploited occasionally, as needed.

Outside the system:

C. Opportunities:

- Cyberspace is approached as the operational environment in which conflicting activities between similar technologies are carried out. Their development is one of the prerequisites for the good functioning of any modern society. Ensuring the security of cyberspace is a concern of all actors involved. Blockchain represents a solution;

- AI, VR and AR technologies and components are already implemented in some applications. Currently,

more and more actors are showing interest in their development. Blockchain and metaverse, even if they are solutions in early stages, are being developed to optimize decision-making comfort;

- The blockchain technology to assist the decision could develop new directions of professional reconversion especially in the field of information gathering, it being known that it is much easier and useful is the processing by a human of some data and information. For example: in the case of image processing, emotions cannot be reproduced by cybernetic algorithms. Such a solution can determine real information that does not obey any technical algorithm and that no sensor can establish based on physico-chemical principles;

- New parameters of adversary behaviour can be identified and stimulated. Knowing the interest in cyberspace, new behavioural benchmarks of tactical systems that use blockchain can be identified. It is obvious that many actors, especially in the first phases of the action, will focus exclusively on information from cyberspace, but the problem arises when the respective critical infrastructure is in a long-drawn crisis;

- New directions for the development of the economy of a conflict can be developed by diversifying the fields of action that lead to the strengthening of staff confidence in blockchain technology and to the stimulation of new environments and techniques of human interaction under conditions of physical security and protection of personal data.

D. Threats:

- Even if the blockchain technology is safe from direct attacks, it is vulnerable to "phishing" attacks executed on the human component. Thus, hackers can act with scams through DeFi (decentralized finance) programs, applications and forums in which we also include DYOR (Do Your Own Research) and Sybil attacks (disinformation through fake accounts on Facebook, Twitter, WhatsApp, Reddit etc.), placing malicious codes in open-source applications or in unaudited applications, facilitating access to applications of programs run by anonymous teams etc. Unable to keep isolated for a long time, the human staff serving an infrastructure must be kept under observation. Auditing blocks and informing staff about new types of attacks is a priority requirement;

- The governors' reserve for legislative change and the delay in the adoption of some political decisions can lead to ensuring a competitive advantage for potential opponents on the goods and services markets. For blockchain, cyber security services with all the implications they entail are extremely important;

- Current technological changes in terms of pace and technical performance can generate serious gaps between competitors/combatants. Failure to adapt technologies at extreme performance values can lead to erroneous perceptions, a decrease in ambitions and the lack of identification and elimination of vulnerabilities whose exploitation by an adversary can produce catastrophic effects at the level of a critical infrastructure;

- The replacement of specialized and experienced personnel will be increasingly difficult to achieve in the absence of an operational reserve even if most of the new technologies are still at the project stage. We draw particular attention to those with an audit function that fulfil the role of functional miners of blockchain technology.

4. Research Results

In the perspective of the digitization of many sociological and technical fields, the study on the implementation of blockchain technology to assist the critical infrastructure decision leads us to the following results:

1. In order to transform the opportunities (C) into strengths (A), funds must be allocated for staff training investing and for the acquisition of technology adapted to the current parameters of the digitized environment. Staff training must include two directions, namely: specialized training in accordance with the role and function held in institution and a general training to perceive digital technologies as a progress factor and not as a future threat to one's own societal comfort. The digital technology to be purchased must be carefully selected according to the requirements of the activity carried out. Regardless of the performance of VR, AR and even AI equipment, for critical infrastructures the priority is the purchase of cyber security technologies.

2. Cyber security remains a major issue through the highly diversified approaches. Even if it is unanimously accepted that digitization influences all social fields, it is still attributed to communications and IT. This contemporary reality deepens the fracture between perceptions that the social, humanities and political sciences have no role in the development of digitalization-based technologies. Any individual, through the activity they carry out in society, can be the victim of a cyber-attack that steals their digitized identity even for short moments and affects their societal comfort. We appreciate that through a modernized legislative system, adapted to the conditions of a cyber conflict, combined with continuous training in an educational system adapted to these conditions, a multitude of threats (D) can be transformed into opportunities (C).

3. To transform weak points (B) into strong points (A), each decision-maker, depending on the hierarchical level it occupies in blockchain, must create programs to attract human capital and provide stimulant benefits to employed personnel. We appreciate that the pool of specialists making, organized in various types of professional associations whose main activity is to provide specialized consultancy or to transmit knowledge through practical-applicative courses, can represent a strategy that ensures a good institutional evolution. At the same time, these organizations could provide audit services or, sometimes, replace miners in the decision-making blockchain.

Also, the network architectures reorganization produces changes in the level of security of the entire infrastructure. These are both physical and cyber changes. From this point of view, we consider that scientific research with proprietary results and products represents a much more reliable solution compared to the purchase of technical components. We observe that the profoundly positive effects on the infrastructure security

will also open up new directions of its attacks. Excessive use of AI, for example, can facilitate the introduction and analysis of disruptive data and information produced by electronic warfare systems. Thus, a jamming emission accepted as a useful from a sensor can produce catastrophic effects once it has been accepted into the blockchain. Falsification of reality, especially for a strike vector can turn it from a defense tool to an attacker or vice versa. The examples are multiple and that is why we recommend that blockchain implementation be done with great discernment and with careful preparation of operators and decision-makers.

5. Conclusions

The main statement and observations that lead us to consider that blockchain technology will not be implemented soon at the level of human society, but which do not exclude the development of some research directions, relate to knowledge and the way of perceiving the advantages of its use are the following:

- At the institutional level, the content of the blockchain concept is not known. The security and governance mechanisms of public authorities are centralized by their nature however the topics of decentralization and networking are addressed. No matter how many information security applications and procedures are adopted, it does not even rise to the level of a pseudo-blockchain.

- The centralized transfer of information and the preservation of the supreme authority veto are approaches that undermine blockchain technology. In this situation, the solution is adopted right from the discovery of the problem by the supreme authority, following which the decision support elements validate it or, in some situations, highlight its major vulnerabilities, depending on the real parameters of the security environment.

- The management procedures of a management situation do not ensure the personnel safety for those involved in. For this situation there are other procedures aimed only at the personnel security regardless of the function and role held within the system. The lack of a procedure's harmonization, against the background of their centralization under a higher authority, often causes an excessive exposure of the executors to insecure conditions or to the appearance of interference with third parties that can quickly turn into internal threats. These vulnerabilities are at odds with the security principles of blockchain technology.

- Related to cyber security, resistance to censorship based on the defense of human rights principles and the protection of individuals regarding the processing of personal data is another contemporary issue. Ignorance of blockchain supports this baseless resistance even if the technology would eliminate it immediately.

Digital infrastructures with public and private keys, with digital signatures, with temporary markers and replicated databases specific to distributed ledgers, with increasingly complex cyber security systems etc., have been around for a long time and are used in various software and digital platforms, autonomous or on the Internet. Blockchain should not be confused with the digital society. The introduction of digital signatures, time values and hash, digital decision support methods, blocks organized by modules etc., even if it is a small part of

the solution is not blockchain.

But the creation of pseudo-blockchain technologies should not cause researchers to give up their work, currently quite large budgets are allocated to the transformation of governance, procedures, documentation and standard technologies into systems that provide superior services. The introduction of various pseudo-blockchain applications into everyday life can be considered beneficial in stimulating psycho-social perception and preparing institutions for a future implementation of this technology at the critical infrastructures level. In addition, the organization of courses, conferences, hackathons and other serious-gaming zones will form a solid basis for its development in which information security will hold the leading role in a digitized world.

In conclusion, even if blockchain still involves very high costs, we are convinced that future scientific research will make it extremely attractive to implement the technology at the level of critical infrastructures to serve a sustainable society based on digital technologies. From a military point of view, because war is part of the human society ecosystem, it itself will be assimilated to a blockchain platform with all its rules, the stake being governance for the economic development of that society. Furthermore, innovation must be harnessed at all levels, both within a digitized society and globally. This can be done through university-affiliated research centres, public and private research institutes, as well as other research and development structures of the defense industry and commercial sectors, in domestic programs and with foreign partners. Only in this way can an asymmetric advantage be obtained for solving the problems determined by the new challenges in the field of national security and defense.

References

[1]. Sabz A. P. F., Niculescu-Mizil Gheorghe P., "A Blockchain-Enabled Model to Enhance Disaster Aids Network Resilience", No.2 Vol.3/*Romanian Cyber Security Journal*, 2021 [on-line]. Available at: https://rocys.ici.ro/fall-2021-no2-vol-3/a-blockchain-enabled-model-to-enhance-disaster-aids-network-resilience/ [March 14, 2023]

[2]. Powell Warwick et al., "From premise to practice of social consensus: How to agree on common knowledge in blockchain-enabled supply chain", *Computer Networks*, Volume 200, 108536, 2021 [on-line]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1389128621004606 [April 03, 2023]

[3]. Chowdhury, M. J. M. et al., "Blockchain versus Datababe: A Critical Analysis", Conference Paper: August 2018 [on-line]. Available at: https://www.researchgate.net/publication/327483781 [March 27, 2023]

[4]. Kriptomat, "Blockchain, Real World Blockchains, What is blockchain oracle?" ["Blockchain, Blockhain-uri din lumea reală, Ce este oracolul blockchain?"], Internet: https://kriptomat.io/ro/blockchain/ce-este-oracolul-blockchain/ [March 15, 2023]

[5]. Park J. S., Youn T.Y. & Kim H.B., "Smart Contract-Based Review System for an IoT Data

Marketplace", ReasearchGate, 2018, [on-line]. Available at: https://www.researchgate.net/publication/328468453_ Smart_Contract-Based_Review_System_for_an_IoT_Data_Marketplace [March 15, 2023]

[6]. Grosu, G. M. et al., "A Note on Blockchain Authentication Methods for Mobile Devices in Healthcare", Spring 2022, No. 1 Vol.4/*Romanian Cyber Security Journal* [on-line]. Available at: https://rocys.ici.ro/spring-2022-no-1-vol-4/a-note-on-blockchain-authentication-methods-for-mobile-devices-in-healthcare [March 12, 2023]

[7]. Burkepile, K., "Campaign Planning Handbook", Academic Year 2023, US Army War College, Dep. Military Strategy, Planning, and Operations, Carlisle Barracks, Pennsylvania 17013-5242, pp.153-155 [on-line]. Available at: https://warroom.armywarcollege.edu/wp-content/uploads/AY23_Campaign_Planning_Handbook.pdf [March 15, 2023]

[8]. ADP 5-0 , "The Operations Process", Headquarters, Department of the Army, Washington, D.C., 2019, pp.1-10 [on-line]. Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18126-ADP_5-0-000-WEB-3.pdf [April 05, 2023]

[9]. Kambhampati S., Knoblock C.A. & Yang O., "Planning as refinement search: a unified framework for evaluating design tradeoffs in partial-order planning", *Artificial Intelligence Volume* 76, 167-238, 1995 [on-line]. Available at: https://www.sciencedirect.com/science/article/pii/000437029400076D [April 04, 2023]

[10]. ADP 5-0, "The Operations Process", Headquarters, Department of the Army, Washington, D.C., 2019, pp.4-6 [on-line]. Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18126-ADP_5-0-000-WEB-3.pdf [April 05, 2023]