Cyber Security: Blockchain Transformational Technology Towards Resilient Society Digital Infrastructures

Paul NICULESCU-MIZIL GHEORGHE
National Institute for Research and Development in Informatics - ICI Bucharest
paul.gheorghe@ici.ro

Abstract: In a world of constant change and the rise of the Internet light speed highways, the transaction of digital content has reached a new apogee, in all domains of the existing industries. In the Cybersecurity industry, which has been facing a true revolution through the Cloud Computing Infrastructures and Big Data processing power, now the world is facing a new paradigm shift with the introduction of Quantum Computers, Artificial Intelligence, Blockchain Technology and Decentralized Crypto Eco-systems.
The purpose of this paper is to reproduce the panorama of the modern decentralized technologies that is moving towards a peer-to-peer usability of the Internet and the aspect of the resilience of the digital infrastructures that manage, connect and help to operate the digital society. What simply begun as the technology behind Bitcoin, the Blockchain technology has seeped into every sphere of the modern society and there are constant efforts to research its potential capabilities, for it to deliver a next generation architecture of governance and a trust-based future of the Internet usability.
Keywords: Blockchain Technology, Artificial Intelligence, Resilient Society, Digital Infrastructures, Critical Infrastructure Protection

INTRODUCTION

Taking into consideration the development of Internet technology and the informational society across the planet, there is a confirmed trend to implement several new activities in cyberspace, common and accessible by anyone, anywhere, anytime, based on the moral vector of trust. From socialization and communication among people up to doing online business and everyday activities due to the easy access to information, the Internet has become a vital factor for personal and professional development.

This has resulted in a wide variety of applications and platforms, specifically designed according to each industry and activity. Cyberspace has managed to capture much of the public interest by providing everyone the opportunity to be able to promote and manage activities in the digital environment. Unlike classical usage, the Internet is still an experimental environment where there are no clear rules of operation, but faced strong developments trends of substitution and created new infrastructures to meet the nowadays challenges in terms of Cyber Security.

Where there are areas of activities, potential and money, there are also great interests to profit from them. But in reality, for all of these

society activities to properly function, they are to be regarded with increased wisdom, proper care in application and constantly developed towards a resilient digital infrastructure for the users of the Internet, from 2017 onwards (see Figure 1) [1].

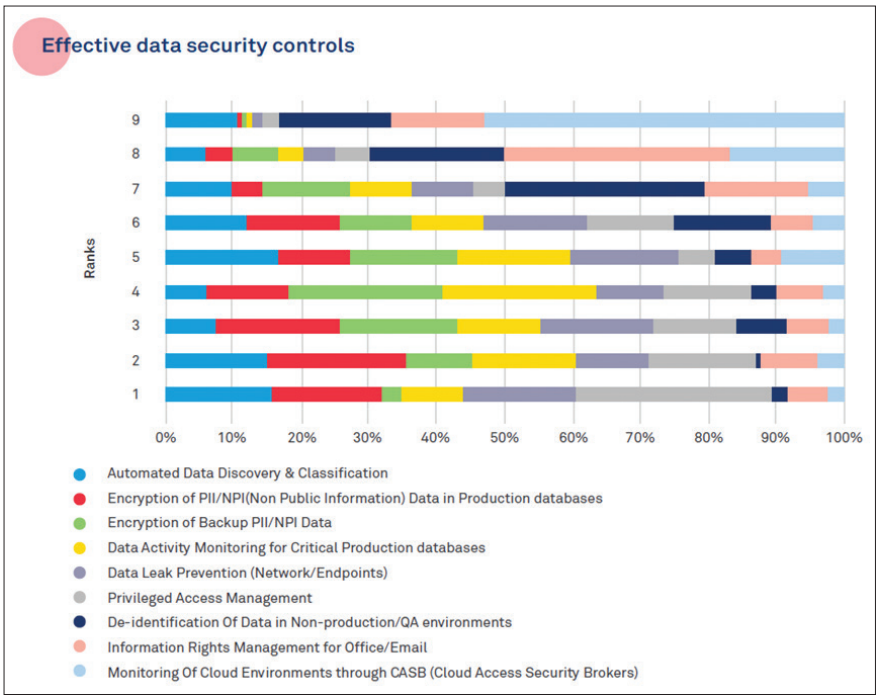

***Figure 1**: Data Security Controls ranked by effectiveness - 2017.*

Cybersecurity is an industry which has been expressively impacted by the transformational Blockchain technology with an opportunity for more in the future. The motive why this new technology has enlarged its popularity is that a user can put any digital asset or transaction into the blockchain and that it can prevent any types of data breaches, identity thefts, cyber-attacks or unfair play in transactions [2].

KEY CONCEPTS REGARDING BLOCKCHAIN TRANSFORMATIONAL TECHNOLOGY TRENDS WITHIN CYBERSECURITY

Foreshown as a disruptor for the countless industries, there is real evidence that blockchain deliveres substantial advantages for the world of business. The value of the global blockchain technology market is expected to be worth 20 billion USD by the end of the year 2024. There is need for a strong voice and solid reasons to adopt a strategy for implementing new technologies, not taken into consideration how much advertisement it is causing [3].

The Blockchain technology will have a positive impact on information security and here are the efficient ways of operation:

a) Blockchain technology is decentralized - this fact effectively passes by the intermediary - there is no more reason for a third-party institution to process the transactions. Instead of uploading data in a Cloud Computing server architecture or deposit it in single locations, blockchain is processing the data into many reduced parts and dispenses them crosswise the entire network on a digital ladder of transactions without any central point of control.

b) Blockchain technology offers encryption and validation - Every recording that occurs on blockchain is encrypted. The data will not be altered and it offers means to prove it. Due to the fact that it has a distributed and immutable nature, the digital signatures across all the ledgers on all the nodes are validated by the entire decentralized network.

c) Blockchain is impossible to hack - Blockchain makes the hacking of its network unfeasibly hard. Hackers can break into traditional networks and corrupt data found in a single location, but not on blockchain. The information

is decentralized, encrypted and cross-checked by the entire network. Each transaction is legitimately confirmed by multiple nodes of the decentralized networks. To efficaciously hack the blockchain, there is need to hack most of the nodes of the network at the same time. Technically it is possible but only with enough supercomputing power and enough processing time. These facts are fortunately beyond the technical abilities of nowadays cybercriminals.

d) Blockchains are private or public - public blockchain enabled anonymity, so there is the possibility to limit the access to specific users. While having the benefits of a full decentralized peer-to-peer network, the users who accesses a private blockchain are obliged to authenticate their identity to gain access privileges. Their specific transactions cand be restricted.

In order to repel cyber-attacks, blockchain architecture must be developed and configured with security in mind. While some organizations are in a hurry to realize a use case for blockchain technology, security cannot simply be added as an addendum [4].

In terms of actual predictions for blockchain technology, the following are some of the most remarkable:

a) There will be substantial investments in blockchain technology. It will continue to exercise heavy investment in financial applications of blockchain, but it should also begin to see financiers taking an interest in the technology's wider applications;

b) Security industry players will aim to develop a unified framework for integration in blockchain. Whether this will be completed in the near future is difficult to say, but ultimately there will be an agreed set of security protocols and best practices for blockchain technology;

c) There will be a rise in blockchain uptake for the identity management space. Nobody likes giving away their personal information, and passwords are inherently a bad security protocol. Blockchain technology can solve both of these complications, so presume to perceive plenty of activity in this space in the near future.

In the year 2018 the amount of the funding of Blockchain projects through ICOs and ITOs (Initial Coin Offering and Initial Token Offering), was considered for more than 6.6 billion USD. These numbers are indicies of an accelerated expanding market within the blockchain discipline (see Figure 2) [5].

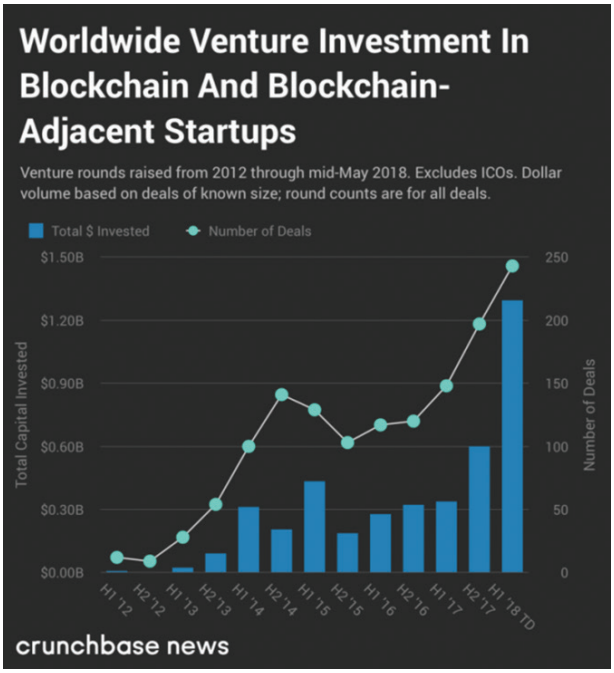

***Figure 2**: Worldwide Venture Investment in Blockchain and Blockchain - Adjacent Startups.*

INTELLIGENT SECURITY SYSTEMS (ISS)

Much like the blockchain movement, demand and momentum for Artificial Intelligence technology have only amplified in demand. In the year 2018, online threats continue to be a major distress for most of the businesses. Many people think that AI - Artificial Intelligence will play an essential role in the future of Cybersecurity.

In order to achieve innovative platforms, AI security companies continued to receive substantial funding. Cylance, an AI-powered endpoint protection vendor, had already received $177 million in funding before 2018. An investment over 40 million USD was granted for the Agari company, for its outstanding AI-powered e-mail security platform.

There a re no signs that these investments will slow down in the near future. AI impact on online threats is influencing virtually all the aspects of the cybersecurity market.

By the year 2025, the industry is expected to grow from 2.99 billion USD in 2016, to more than $34 billion USD, conferring to a 2018 report from marketsandmarkets.com online portal [6].

CYBERSECURITY EMBRACES ARTIFICIAL INTELLIGENCE

Cybersecurity is an important industry where Artificial Intelligence is motivating significant investment into startups. For the protection of computers, cybersecurity companies use different machine-learning techniques, nodes and other IT assets. These assets are treated well beyond the newest software update or virus scan capability.

The company Darktrace, takes its research methods from the human immune system. Its algorithms can literally surveil the unique patterns of every device and user activity on a network. It perceives the evolving problems before dangerous situations get out of control [7].

NEW THREATS AND CONSIDERATIONS FOR BLOCKCHAIN IN CYBERSECRITY

For the managing of cybersecurity risks, the permissioned blockchains present some unique opportunities. In order to enhance operations and services quality to the customers, the financial insdutry researches the use of permissioned blockchains. New commers industrial participants must distinguish the cybersecurity competences and risks linking to this technology [8].

The annual Internet Security Threat Report from Symantec, draws important trends in terms of malware variants, endpoint security and mobile protection. Researchers found an increase of 80% in new malware designed to target Apple computers, and a 54% increase in mobile variants. 5.4 billion instances of thwarted Wanacry attacks were as well reported in this document [9].

Symantec indicates a noteworthy spike in coin mining attacks, as the result of cypto currency boom in 2018, but as coin values have leveled out, mining attacks amplified. Crypto mining attacks were nearly nonexistent a few years ago, but rose from roughly 7% of the malware versions from 2017 to more than 30% through the first half of the year 2018, according to Skybox “Security’s Vulnerability and Threat Trends 2018” [10].

While blockchain could possibly change how we operate, the technology is accessible to both consumers and malicious attackers. It is important to feature in the need to do real-time blockchain network analytics and implement built-in validation checks to defend the blockchain networks [11].

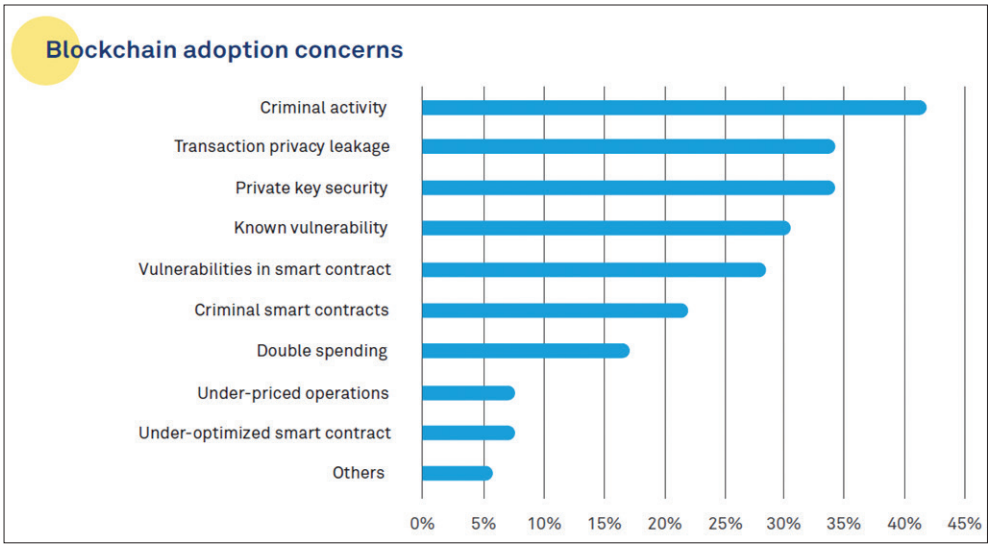

***Figure 3**: Blockchain technology adoption in Cybersecurity activities*

Studies like State of Cyber Security Report 2018 show the risks that concern organizations the most regarding blockchain technology, 42% of the respondents chose criminal activity to be the risk they were most concerned about. Transaction privacy leakage and private key security were the next two causes for concern with 34% share each of the total responses (see Figure 3).

The architecture, deployment and procedures of a permissioned blockchain affects the cybersecurity risks of the network. Vital reflections of this technology include the number and kinds of users in the network; the sensitivity of the records or transactions recorded in the electronic ledger; the facility of untrusted or unauthorized persons to participate in the network; the design and robustness of the initiation; the strength of the cryptographic hash algorithms; the extent of reliance on externally-sourced data; consensus validation rules and processes; and the ability to correct deceitful, malicious, or erroneous records. Due to the fact that permissioned blockchains are in constant development, the cybersecurity controls that best mitigate risk also continue to evolve.

CYBERSECURITY TOWARDS A RESILIENT SOCIETY - A DIGITAL CRITICAL INFRASTRUCTURE

For a permissioned blockchain, cybersecurity values from current legal frameworks, regulations, and industry leadership are critical components to an operative cybersecurity program. Economic regulators have issued detailed supervision for financial institutions cybersecurity programs, and equally must inform the management for the permissioned blockchains used.

These principles and controls should include:

• Information security programs with consistent procedures, designed to ensure that the customer information system is accurate;

• Evaluation of the practices of the cybersecurity risk management systems and of the internal control systems, must be verified with a feasible structured audit program, in compliance with regulations, legal frameworks and corporate IT risk policies;

• Encryption of user information must be granted at all times, including management systems that protect the data in-transit or *in-saving* mode from unauthorized individuals;

• Backgroud chek of the employees through dual-control proceedings and segregation of tasks for hired personnel with granted acces to customer sensitive records;

• Response programs for unauthorized individuals' intrusion and action taking solutions against sensitive financial customer data damaging, including extensive reports to law enforcement authorities;

• Risk and threats modelling software must be elaborated by highly skilled expert teams for best understanding of this technology and for delivering an adequate mitigation in a detailed manner;

• Detection and surveillance systems for attempted attacks or intrusions into sensitive custormer data systems.

Existing cybersecurity standards are highly appropriate for guaranteeing the security of permissioned blockchains. Existing standards and guidance provide a strong foundation for guarding permissioned blockchains from cyber-attacks.

BLOCKCHAIN AND CYBERSECURITY: A NEXT GENERATION TECHNOLOGY AS A PROTECTION OF THE INTERDEPENDENCIES OF CRITICAL INFRASTRUCTURES

According to World Economic Forum's transformational maps online interface, international teams of experts studied the interdependencies of the Cybersecurity topic on a global scale, and represented it in a graphical interactive version for the public (see Figure 4).

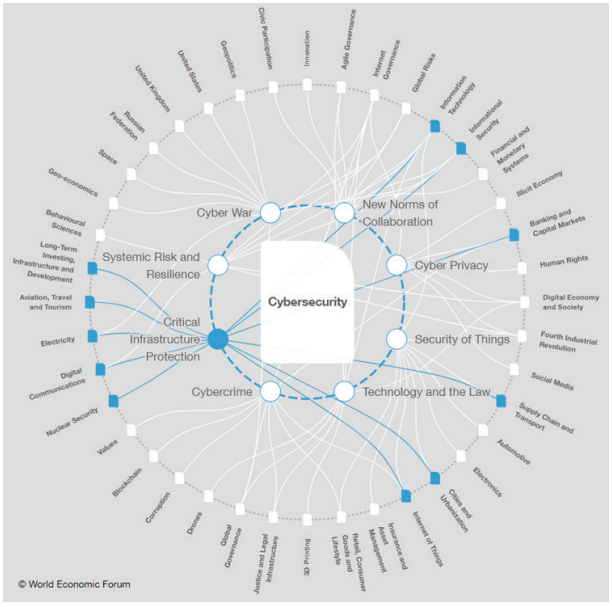

***Figure 4**: World Economic Forum - Cybersecurity transformational map.*

CRITICAL INFRASTRUCTURE PROTECTION

The todays society faces sophisticated challenges for its necessity to defend the cyber integrity, its fabric of digital self, like the energy grids, sanitation complex systems and many others, being part of the critical infrastructures architecture. The spread of systems that unite the cyber and physical worlds by combining physical infrastructures with IT power, will increase its functionality, but as well it will generate more goals for cyber attackers. A single attack on only one critical infrastructure sector, e.g. energy-related systems, financial systems, communications networks, or water services, will have as concequencies the crippeling of communities or entire nations [12].

The implementation of the Blockchain technology may serve as a cross cutting technology for keeping track of all transactions that the parts of the industry are generating along their time-based interactions. Some of the potential implementation of decentralized networks and Artificial Intelligence appliance are most suited in following sectors:

• ***Supply chain and Transport***

While the economic performance of supply chains has improved, their environmental impact and vulnerability have become major sources of concern. The responsibility for much of the physical movement, handling and storage of products has been subcontracted to dedicated logistics service providers, and their task grows more complex as global economic activity expands.

• ***Nuclear Security***

In a period of increased geopolitical stiffness, an international focus on nuclear non-proliferation and disarmament is as important as ever; the possibility of a new arms race cannot be ruled out. Meanwhile the advent of nuclear energy programs in a number of countries around the world deserves close attention.

• ***Digital Communications***

The digital communications industry is enabling exceptional levels of global internet use, online social interaction, and financial enclosure. As the industry is transmuted, effective policy and regulation that support businesses could increase productivity. At the same time, the industry must be open to new models of cooperation and governance, in order to better address challenges like data privacy and growing demands on infrastructure.

• ***Information technology***

Information technology is at the center of a pervasive democratization of innovation, and advances in the industry are having an impact on all continents and in every business. A number of related aspects deserve close study: the social aspects of impending and fundamental changes in employment; trust and privacy; “cyber-resilience”; and moves in digital policy and governance.

• ***Electricity***

In industrialized economies, distributed energy resources and digital technologies are changing system planning and operations. These technologies are also creating occasions to bring electricity to more than 1.1 billion people with absence to access to this essential commodity. Efforts are ongoing to expand regional markets and create greater geographical interconnections, and to certify the security of supply in the danger of cyber threats and natural disasters.

• ***Aviation, Travel and Tourism***

The evolution of the industry has been resilient in the face of geopolitical insecurity and economic instability; by 2030, it is expected to provide to 1.8 billion international tourists, compared with 25 million in 1950. Its ability will continue to generate growth, create jobs and enable regional and national development, will be affected by security risks, travesl and trade barriers, necessary infrastructure investments, digitalization of assets, demographic shifts, and global regulatory frameworks.

• ***International Security***

States, international organizations and trans-national performers all seek to ensure their vital interests and survival. Some of the most relevant present trends in international security contain the return of great power competition, the encouraging of a new arms race as a consequence of the military application of

cutting-edge technology, the rising influence of non-state actors, and the expansion of domains of conflict at an unprecedented rate into space, cyberspace, the oceans and the Arctic region.

• ***Cities and Urbanization***

While urbanization generates many challenges that intimidate the quality of life, that's because the density of cities enables innovation, by readily providing testbeds to measure the effectiveness of related solutions. Through the collective efforts of governments, the private sector, non-governmental organizations, and the public, and through the harnessing of transformative technologies and wise urban policies, it is possible to realize the true potential of the cities of the future.

DIGITAL CRITICAL INFRASTRUCTURES FOR A RESILIENT DIGITAL SOCIETY - NEW WAYS FOR MORE PARTICIPATION, TRANSPARENCY AND INNOVATION.

Digital structural change - the growing use of modern networking technology is omnipresent in the daily social and economic lives of the people. Nowadays, anyone can participate interactively in digital architectures. These facts are giving the opportunity to new forms of participation and new patterns of value creation to emerge, towards a shifting power to the citizen and prosumer sovereignty.

Open Innovation - with many external ideas that have been implemented, the greater combinations are at hand to create new sollutins. Open innovation as well involves risks, due to the fact that classic value creation patterns have to be modernized and broken up with modern strategies and new interaction aptitudes.

Open Government - more and more political institutions and government agencies are constantly opening up to increase the interaction with the public. The public data availabilitye can lead to new applications and business models. Interactions help the government to receive external feedback through participatory models that can be developed between government agencies and its citizens. As a collateral result, democracy turn out to be transparent and more interactive.

Open Access - The dissemination of scientific information, has been fundamentaly improved through the user friendly acces to the Internet technologies. The knowledge that has been efficiently and ergonomically spread through a proactive policy of open access of the users, has enhanced the potential of the innovation of the global economy.

Open and free culture - People are ripping the rewards of the digital age in the creative sphere. More knowhow is being offered in virtual forums. The users are being stimulated to contribute and interact with peers. By making various projects, compositions, construction plans or blueprints accessible and/or adaptable, through these facts positive effects will come together into the innovation process. All these open and innovative participation will cultivate a joint digital society in which users will join constantly.

THE WAY FORWARD? SECURE. VIGILANT. RESILIENT.

There are no cyber defense or information systems can be measured as 100% secure. What the users consider safe today, it won't be safe tomorrow. That fact is given by the profitable nature of cybercrime and the criminal's ingenuity to always look for new weaknesses and methods of attack. In order to defend the technical infrastructure of an organization from external attacks, cybersecurity standards must be preferably adopted using blockchains as well as the confidentiality and integrity of the IT architecture [13].

While cybersecurity is essential to the large adoption of the blockchain technology, key components like operations, technology architecture, consortium building, talent and global regulations are to be considered in a serious manner.

***Figure 5**: Strategy and Governance within Blockchain technology development.*

The present state of blockchain, needs to build new improved techniques and processes that will secure the governance of the network from hacking, manipulation and vulnerability breaches (see Figure 5).

To avoid such fissures, the following statements should be able to shape blockchain eco-systems in a secure manner:

- Most blockchain frameworks will slender towards incorporating the principle of privacy by design into their architecture;
- Better, faster and efficient consensus methods, using plug-and-play components and IoT around consensus and membership services will be applied;
- Information security standards will advance to certify data confidentiality;
- Interoperability between different distributed ledger protocols will become a necessity and a requirement to permit globally verifiable identity and authentication;
- Crypto Wallet Management will change. Wallet application will have to become more secure;
- Privacy-preserving smart contracts will become the order of the day without giving any private information to the wallet providing services;
- As a diverse perspective of technologies like quantum computing, advanced components like Quantum Resilient Ledgers with methodologies to do real-time migration of data between ledgers will start making their presence felt;
- Governance controls to ensure that there are no run-away contracts or Artificial Intelligence bot wars that use the blockchain networks.

The above-presented points, when correctly implemented and mainstreamed, will resolve many of the existing concerns of organizations interested in implementing decentralized technologies and Blockchain solutions.

Meanwhile, looking from a global security landscape, the blockchain technology will help in intensifying the resilience of existing threat response mechanisms which is needed for the ever-expanding threat landscape. In conclusion, cybersecurity and blockchain are so closely connected that it is easy to foresee their partnership in their technology evolution journey in the near future [14].

CONCLUSIONS

Given the possibility for developing various applications, like securing transactions and storing data in a secure manner, the industry will profit from the growth of blockchain advent. The cyber threats to the industry continue to evolve in complexity and intensity, some upcoming technologies likes permissioned blockchains will contribute to the vital targets of combatting cybersecurity risk. It will adequately protect consumers' private information and the integrity of the global blockchain networks.

Significant cybersecurity capabilities are offered by permissioned blockchains, they share similar cyber risks that distress other IT systems. They also have exclusive characteristics, all of which deserve further evaluations by regulators and industry stakeholders. It is necessary to reassure extra conversations about the cyber security benefits of blockchain technology systems for appropriate government policies.

ROMANIA - CYBERSECURITY AND BLOCKCHAIN TECHNOLOGY AS A SERVICE SOLUTION?

Romania needs an up-to-date and efficient cybersecurity legal framework, serving the national strategic interests, synchronized with the joint

European, NATO and International cooperation agenda. There are well known international companies who released private Blockchain service technologies (e.g. Microsoft Azure and IBM Hyperledger) and that will make the process of accessing Blockchain more simplified and will be no longer limited to specific parts of the world.

It is the Government's task to settle the draft law and certify its implementation, making the dedicated institutional structures fully operational and advancing measures to enable awareness raising and implementation of practical solutions applicable to the public and private sectors for a reliable cybersecurity governance system.

As an upcoming advent, Blockchain technology requires new and refined algorithms to be more efficient in energy use and time of processing of large amounts of data and must contribute to the establishment of trust among its users and expanding towards Artificial Intelligence, Big Data Processing and Cloud Computing Infrastructures.

Can the transformational and cross cutting Blockchain technology reveal the benefits within the protection of the interdependencies of critical infrastructures for an answer to a more resilient cyber security?

References

[1] Wipro. (2018) *State of Cybersecurity Report 2018. Foresight for the global cybersecurity community*. Wipro - consulting and business process services company. Online available at: https://www.wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of-cybersecurity-report-2018.pdf [Accessed: March 6th, 2019].

[2] Toshendra, K., S. (2018) *The future of Cybersecurity: Blockchain Technology*. Blockchain Council online portal. Online available at: https://www.blockchain-council.org/blockchain/the-future-of-cyber-security-blockchain-technology/ [Accessed: March 1st, 2019]

[3] Drolet, M. (2018) *4 reasons blockchain could improve data security*. CSO – Infosec at your service. Online available at: https://www.csoonline.com/article/3279006/4-reasons-blockchain-could-improve-data-security.html [Accessed: March 3rd, 2019]

[4] Cylance Protect. (2019) What is Cylance Protect? Official web portal. Online available at: https://www.g2crowd.com/products/cylanceprotect/details [Accessed: March 10th, 2019]

[5] Kudelski Security Team. (2019) 2019 *Cybersecurity Trends to Watch: Blockchain and Cloud Security*. Modern Ciso official portal. Online available at: https://modernciso.com/2019/02/05/2019-cybersecurity-trends-to-watch-blockchain-and-cloud-security/ [Accessed: March 12th, 2019]

[6] Walker, A. (2018) *Cybersecurity Trends 2019 Update: Blockchain and AI*. G2 Learning Hub official platform. Online available at: https://learn.g2crowd.com/cybersecurity-trends-2019 [Accessed: February 25th, 2019]

[7] Rejcek, P. (2019) *The world's most valuable AI companies, and what they're working on*. Singularity Hub official platform. Available online at: https://singularityhub.com/2019/02/27/the-worlds-most-valuable-ai-companies-and-what-theyre-working-on/#sm.001jdkqac12j7ddsrwo2b9dd93crj [Accessed: February 22nd, 2019]

[8] Microsoft Cybersecurity content hub. (2019) *Advancing blockchain cybersecurity*. White paper. Available online at: https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity [Accessed: February 26th, 2019]

[9] Symantec official report. (2018) *Executive summary: 2018 Internet Security Threat Report*. Symantec Corporation official platform. Volume 23. Available online at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf [Accessed: March 7th, 2019]

[10] Skybox security official report. (2018) *Vulnerability and threat trends report. 2018 Mid-year Update*. Skybox Security web portal. Available online at: https://lp.skyboxsecurity.com/WICD-2018-07-Report-VT-Trends-MY_03Asset.html [Accessed: February 2nd, 2019]

[11] Deloitte official report. (2018) *Blockchain & Cyber Security. Let's discuss*. Deloitte technology portal. Available online at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf [Accessed: February 17th, 2019]

[12] World Economic Forum. (2019) *Cybersecurity and Critical Infrastructure Protection*. World Economic Forum – Transformation Maps. Available online at: https://toplink.weforum.org/knowledge/insight/a1Gb00000015LbsEAE/explore/summary [Accessed: February 15th, 2019]

[13] Deloitte. (2018) Blockchain and Cybersecurity: An assessment of the security of blockchain technology. Deloitte – Technology, Media and Telecomnications portal. Available online at: https://www2.deloitte.com/tr/en/pages/

technology-media-and-telecommunications/articles/blockchain-and-cyber.html [Accessed: March 10th, 2019]
[14] Wipro report. (2018) *State of Cybersecurity Report 2018. Foresight for the global cybersecurity community*. Wipro - consulting and business process services company. Online available at: https://www.wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of-cybersecurity-report-2018.pdf [Accessed: February 19th, 2019].

Figures

[Figure 1] https://www.wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of cybersecurity-report-2018.pdf
[Figure 2] https://techcrunch.com/wp-content/uploads/2018/05/jason-one2.png?w=642
[Figure 3] https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyber POV_0417.pdf
[Figure 4] https://toplink.weforum.org/knowledge/insight/a1Gb00000038qmPEAQ/explore/summary
[Figure5]https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications /Blockchain-and-Cyber.pdf