Impact of Blockchain Technology: Benefits and Security Risk and Threats

Vlad-Andrei ROTUNDU
Bucharest University of Economic Studies, Romania
vlad.rotundu@outlook.com

The accelerated dynamics of technological evolution has led to a reconfiguration of the security environment by addressing new vulnerabilities, risks and threats generated by the migration of risk-generating entities into cyberspace. These risks are also enhanced by the interest shown by criminal entities in technologies such as Blockchain, which are proving to be attractive in terms of existing functionalities. These changes in the security environment and, by extension, in the international economic environment, are challenges that require a proactive, sustainable and integrated approach. This article aims to analyze the impact of blockchain technology on society in terms of both the benefits and risks of exploiting this technology.

Keywords: *Blockchain, Cryptocurrency, Organized Crime, Terrorism, Artificial Intelligence, Security Threats, Malware, Botnet*
DOI: 10.24818/issn14531305/26.2.2022.04

1 Introduction

In order to achieve their illicit goals, threat actors have undertaken activities to increase their actionable capabilities in cyberspace including through emerging and disruptive technologies [1].

Blockchain technology, especially by its association with cryptocurrencies, has seen the most significant increase of the use among threat actors, with money laundering, distribution, management and monetization of malware, financing extremist-terrorist groups, cyber fraud or child pornography being among the purposes served. Such activities carried out using blockchain technology are a source of significant security risks, and the rate of evolution of this phenomenon indicates that the international economic environment may be affected by the paradigm shift caused by international recognition of cryptocurrencies as a means of payment for goods, services and other assets, without raising awareness about the technology.

The issue of security threats generated by the abuse of blockchain technology is of interest in terms of identifying preventive actions through the adoption of measures under the security-by-design concept, both from a technical and legislative perspective.

In the context of the increasing popularity of blockchain technology in society and its use by entities generating security threats to pursue their own agendas, strategic documents [26] [27] have been proposed/adopted at European and national level, in which emerging and disruptive technologies are presented as supporting sustainable economic and administrative development, but also as enabling elements for the vulnerability of key areas of the society. For example, the inclusion of blockchain technology in the text of the Strategy of the Ministry of Internal Affairs for Information Security in Electronic Format 2021-2026 reveals the interest of the local authorities in the sphere of national security and public order in preventing and counteracting the abuse of technology for illicit purposes and the establishment of a security-by-design perspective [28] in order to anticipate and provide early warning of new threats caused by the use of blockchain technology for malicious purposes.

Such approaches need to be supported in order to be translated into action in an integrated manner that consists of developing research on blockchain technology to meet societal needs [29] and to address security vulnerabilities that may impact the international economic environment.

In this sense, it is necessary to raise awareness among stakeholders about the benefits of blockchain technology and to eliminate its stigmatization as being a tool used by threat actors to carry out illicit actions.

The research aims to make a comparative analysis of the benefits and threats of blockchain technology. The first part of the research will analyze how threat actors such as organized crime groups or extremist terrorist organizations use blockchain technology.

The second part of the research will present the benefits of using this technology in areas such as preventing and combating disinformation or digital evidence management, and the conclusions of the research will present the impact of this technology on society.

2 Threat actors who use Blockchain Technology

As the popularity of blockchain technology rises among the population, even though most of its users do not have the technical knowledge to understand the process, a series of risk generator entities have reoriented their capabilities in order to use this technology, among which the following stand out: organized crime and cyber groups, terrorist/extremist groups.

2.1 Organized crime and cyber groups

Assessments presented in the Europol report on the use of cryptocurrencies by exponents of the criminal phenomenon reveal that although the amounts circulated via cryptocurrencies have remained constant in relation to the total value of the sums obtained from illegal activities, there has been a numerical increase in cryptocurrency transactions [2]. This indicates an increased focus in blockchain technology by these criminal groups and also supports the hypothesis that such entities will devote financial, logistical and human resources to the development of blockchain-based solutions to support the financing of organizations and the laundering of the proceeds of illegal activities, aspects which represent risks and threats to the international economic environment. A total of 14 billion USD was reported in 2021 as being obtained from illegal activities, most of the sums being obtained through fraud (Figure 1).

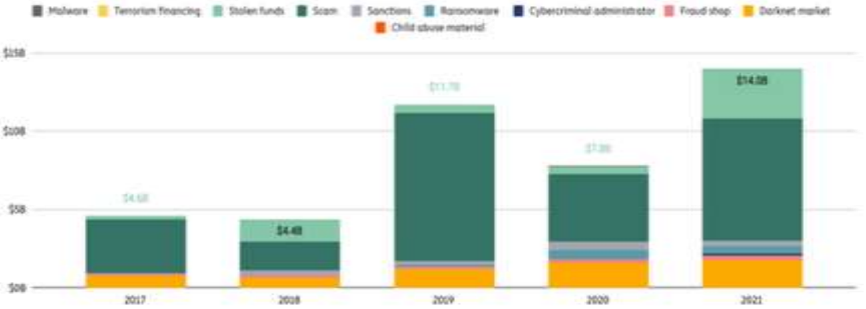

Fig. 1. Total cryptocurrency value received by illicit addresses, 2017-2021 [3]

The use of Blockchain technology by criminal groups or hacktivists is favored by its characteristics in terms of security and speed of transactions, but especially in terms of its decentralization concept which confers the perception of anonymity to certain activities, even if the blockchain is public [4]. Even if the direct attribution of a block is not technically possible, the possibility of monitoring the translatability in the blockchain and tagging known nodes or clusters (exchange, previous investigations, publicly assumed addresses, etc.) [5] facilitates the identification of users who are concerned about using the technology for illicit purposes [6].

The increasing number of people that handle cryptocurrencies, corroborated with their lack of expertise on how this technology works, has been exploited by organized crime groups and an increase in cryptocurrency fraud has been observed [7]. In this regard, in the United States, the number of crypto crimes reported in 2020 increased by 24,057% compared to 2016 [8] (table 1) this increase being directly proportional to increases in the value of Bitcoin (Figure 2).

Table 1. Increasing rates of crypto crimes in United States [9]

Year	Cryptocurrency	Bitcoin	Ethereum	Total reported crimes
2016	14	324	2	340
2017	311	1,574	188	2,073
2018	677	4,742	212	5,631
2019	1,757	18,937	117	20,811
2020	4,275	77,315	546	82,135
Total	7,034	102,891	1,065	110,990

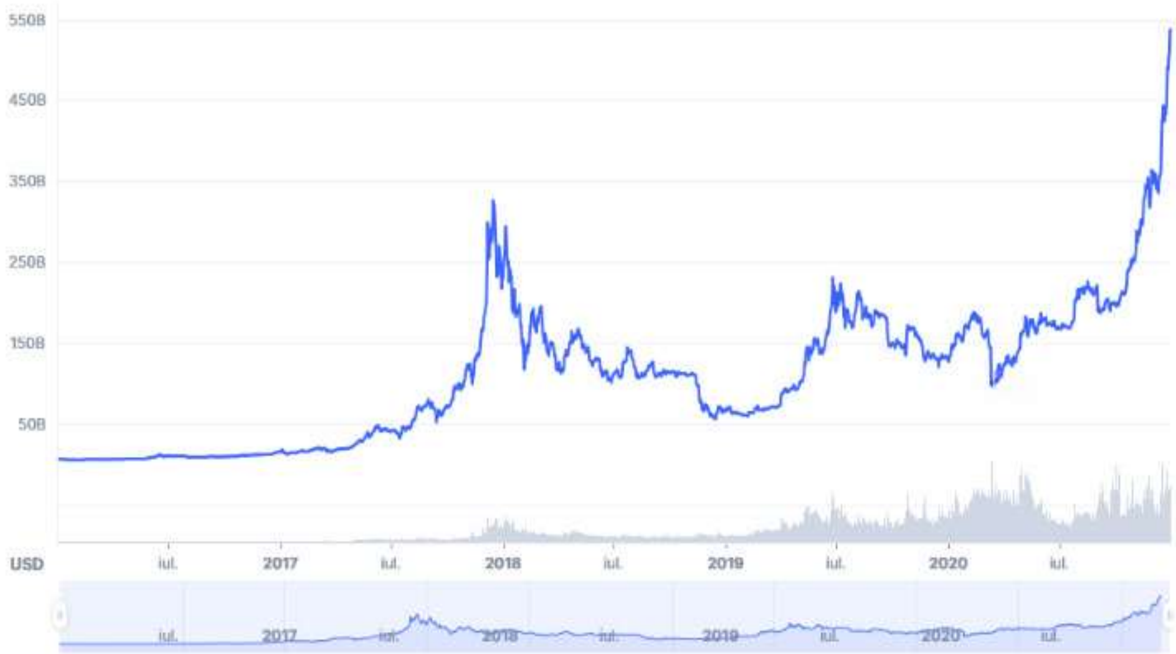

Fig. 2: Bitcoin Marker Cap evolution (USD), 2016-2020 according to www.coinmarketcap.com

At the same time, the lack of user expertise as well as the increase in the value of cryptocurrencies has led to a 500% increase in illicit activities involving the stealing of funds (Figure 3).

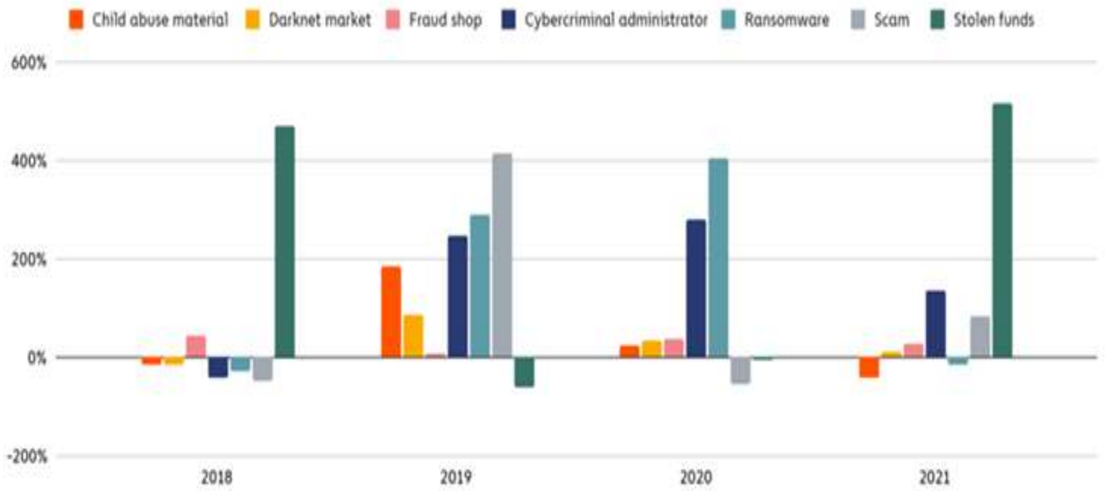

Fig. 3: Percent change in value received by crime type [10]

2.2 Terrorist/extremist groups

In the context of the measures adopted by the international community in order to prevent and combat terrorism, the possibilities of financing these groups have been considerably limited, particularly in terms of the use of conventional transfer services and conventional financial system [11], [12]. The concept of decentralization, as well as the perception of anonymity of transfers of blockchain-based currency, has led to increased use of this technology by extremist-terrorist, especially regarding the use of cryptocurrencies [13], [14], [15]. This statement is also supported by the quantitative increase in transactions in blockchain carried out through addresses tagged as being used by terrorist entities or that have been included in their related clusters.

Expert assessments have revealed that the main use of blockchain technology is for fundraising to finance terrorist activities. Unlike cybercrime groups that have the necessary expertise and the capabilities to engage in research to identify opportunities to facilitate illicit activities through blockchain technology, terrorist groups use this technology without the necessary expertise, strictly to satisfy their pecuniary interests [16]. This is also reinforced by the increasing interest of terrorist organizations to use cryptocurrency exchanges (figure 4). In this sense, blockchain technology represents an alternative for these organizations to previously used illicit parallel financial systems, such as Hawala system, which denotes their intention to adapt their operating modes to the current reality characterized by the intensive use of technology to perform conventional tasks.

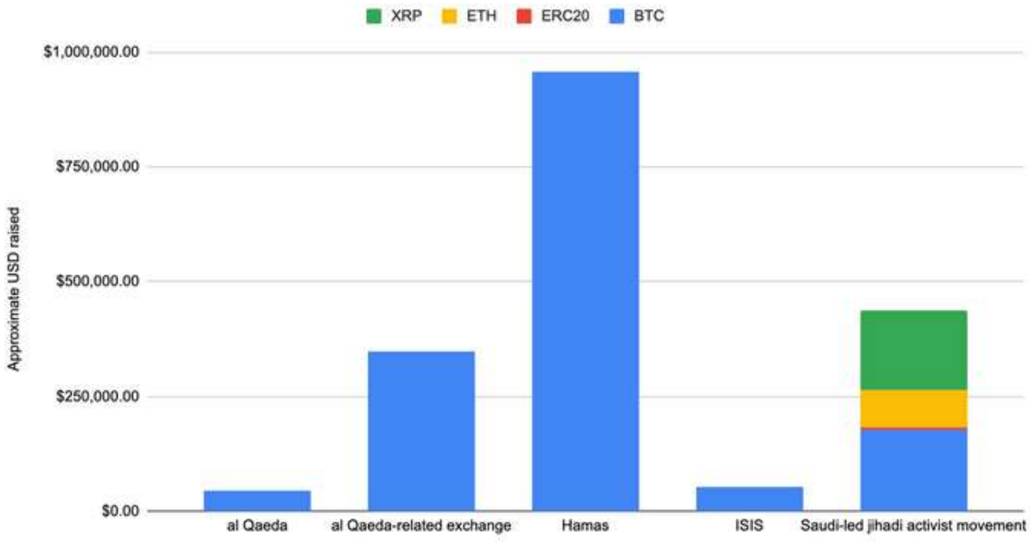

Fig. 4. Coinbase monitor on cryptocurrency fundraising for terrorism related organizations [17]

3 Using Blockchain Technology to Counter Threats and Limit Security Risks

The fast evolution of emerging and disruptive technologies such as Machine Learning, 5G, Artificial Intelligence, Blockchain will lead to significant changes in fundamental areas (economic, financial, security, education) that can both be beneficial to society by streamlining common processes and increasing comfort levels through technology, but also malicious through the abuse of technology carried out in order to commit actions that generate security risks (cyber-attacks, parallel financial systems, money laundering, dissemination of disinformation, deep fake operations, botnets etc.).

As the blockchain technology is currently linked to an economic component, the focus of criminal actors in developing this area is raising, and there is a possibility that the level of expertise of criminal groups in this field will increase in order to identify other opportunities to use blockchain technology to commit illicit actions with an impact on the international security and economic environment (management of botnet infrastructures based on blockchain [18], development of encrypted peer-to-peer communication systems [19] for the conspiracy of criminal activities, etc.).

This advantage can only be exploited by researching this technology at an early stage, as the fast rate of digital development leads to continuous mutations that can result in threats, especially in the field of cyber security.

At the same time, there are approaches to use blockchain technology to facilitate other key areas in the security enforcement process, such as combating and preventing disinformation and propaganda or optimizing the forensic evidence management process through blockchain systems.

3.1 Using Blockchain Technology to Establish the Traceability of Illicit Funds Used by Criminal Organizations

Even if cryptocurrency based on blockchain is used for committing risk-generating actions, the emergence of this technology is an advantage for law enforcement agencies as blockchain's public architecture allows for open-source monitoring and investigation of illegal items. In this sense, the identification or assignment of a block to a criminal entity can facilitate the traceability of the entire organization and all the blockchain resources used, making it possible to perform cluster analysis of the entire ecosystem used to commit security risk-generating actions [20].

Tools developed by private companies such as Chainalysis, CipherTrace or Eliptic exploit the exploits the public component of the blockchain to establish patterns and labels assigned to crypto wallets so as to determine the traceability of certain funds and allow their de-anonymization by assigning specific identifiers to each user.

In this sense, the public nature of the blockchain can allow investigators to develop ecosystems based on the traceability of cryptocurrencies used for illegal purposes, creating an overview of the networks involved.

3.2 Prevent and Counter Disinformation using Blockchain Technology

As for the concept of using blockchain technology to prevent and combat disinformation and propaganda carried out through deep fake processes, it involves the implementation of a decentralized register that must be confirmed and re-verified so that subsequent alteration of online content is impossible. At the same time, the implementation of a checking system in the virtual informational environment based on blockchain will allow Internet users to trace the information and the data sources could to be monitored and validated in the blockchain so that the authenticity of online content can be certified as being reliable [21].

Establishing a system to confirm the authenticity of certain information and to mark the credibility of the source would considerably limit the capacity to disseminate false information (e.g. fake news, deep fake) or propaganda, especially in the context of the increasing spread of this phenomenon in the virtual environment.

Therefore, both in terms of terrorist propaganda aimed at radicalizing sympathizers and other forms of ideologically, financially, geo-strategically etc. motivated disinformation, blockchain technology can be used to create societal resilience and counter current threats to democratic values.

3.3 Using Blockchain Technology in Digital Forensic Evidence Management

Blockchain technology can also facilitate the forensic evidence management process, as the issue of ensuring confidentiality, availability, authenticity and non-repudiation of this type of data is a challenge for all law enforcement and judicial institutions around the world, especially in the context of the growing awareness of the importance of digital evidence obtained through forensic procedures or through direct collection from entities/companies that manage such data (CCTV, email addresses, logs, cryptocurrency wallets etc.) [23]. The growth in the volume of digital evidence is also supported by the increasing number of requests for such data from law enforcement agencies (Figure 5) and the development of digital forensic types.

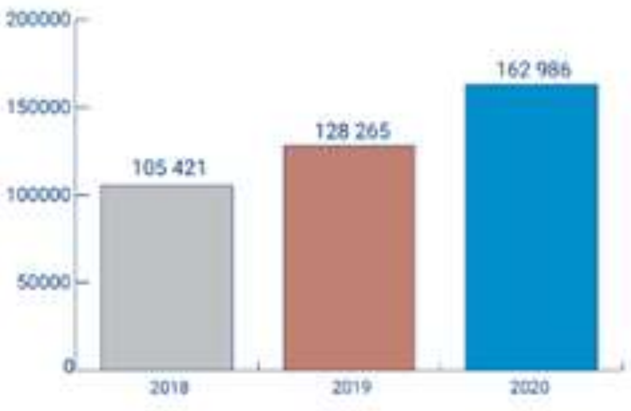

Fig. 5. EU Data requests to a number of Online Service Providers from 2018 to 2020 [24]

Using blockchain based system for maintaining chain of custody of digital evidence has the propriety to ensure traceability of the investigation and transfer process carried over the piece of evidence under trial. Apart from the conventional method where the human factor has an important role in claiming the authenticity of the evidence, the blockchain method is based on the transactions occurring on the electronic evidence. Every transaction gets logged in a distributed ledger and this entry is permanent, thus removing the need for reliance on trustworthiness of stakeholders involved [25].

4 Conclusions

In the perspective of digitization of modern societies, the concept of security should not be neglected as it is an essential part of the whole evolution process. Even though blockchain technology in used in illegal activities, its characteristics can be exploited to ensure a climate of security, but also to streamline vital activities within society and economic environment.

The broad spectrum of blockchain use should be exploited to streamline areas such as transport, finance, administration or security, and further research in the field may reveal other possible uses that could improve people's everyday activities.

In conclusion, the use of blockchain technology has advantages over its use by threat actors, and further research is needed to identify key sectors where it can be used.

References

[1] European Union Agency for Law Enforcement Cooperation, Europol (2019), “Do Criminals Dream of Electric Sheep? How technology shapes the future of crime and law enforcement” [Online].Available:https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf, 2019.

[2] European Union Agency for Law Enforcement Cooperation, Europol (2022, January 26), “Cryptocurrencies: tracing the evolution of criminal finances” [Online]. Available: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances#downloads

[3] Chainalysis (2022, January 6), “Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity” [Online]. Available: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction

[4] Kathleen E. Wegrzyn, Eugenia Wang (2021, August 19), “Types of Blockchain: Public, Private, or Something in Between”, Foley Insights [Online]. Available:https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

[5] Mike Orcutt (2019, August 2022), “Some crypto-criminals think jumping across blockchains covers their tracks. Big mistake”, MIT Technology Review, [Online]. Available: https://www.technologyreview.com/2019/08/22/133272/some-crypto-criminals-think-jumping-across-blockchains-covers-their-tracks-big-mistake

[6] John Bohannon (2016, March 9), [Online]. Available: “Why criminals can't hide behind Bitcoin”, Science, [Online]. Available: https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin

[7] Casey Murphy, Ethan Vera, Suzanne Kvilhaug (2022, February 8), “Beware of Cryptocurrency Scams”, Investopedia, [Online]. Available:https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp

[8] Francis Bignell (2021, June 26), “24,057% Increase in Crypto Crimes Since 2016 Finds Crypto Head”, The Finetech Times, [Online]. Available:https://thefintechtimes.com/24057-increase-in-crypto-crimes-since-2016-finds-crypto-head

[9] James Page (2021, December) “Crypto

Crimes - Comprehensive Overview", CryptoHead, [Online]. Available:https://cryptohead.com/wp-content/uploads/2021/12/cryptohead-io-research-crypto-crime-.pdf

[10] Chainalysis (2022, January 6), "Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity", [Online]. Available: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction

[11] Patrick Hansen (2021, December 1), "New Crypto Rules in the European Union – Gateway for Mass Adoption, or Excessive Regulation?", Standford Law School Blog, [Online]. Available: https://law.stanford.edu/2021/01/12/new-crypto-rules-in-the-eu-gateway-for-mass-adoption-or-excessive-regulation

[12] DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[13] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, "Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats", RAND National Security Reseach Division, pp. 9-16, 2019.

[14] Coinfirm (2021, May 2021), "Forensic Investigative Report: Terrorism Financing Blockchain Addresses", [Online]. Available:https://www.coinfirm.com/blog/terrorism-financing-blockchain-addresses

[15] U.S. Department of Justice (2020, October 1), "Report of the Attorney General's Cyber-Digital Task Force – Cryptocurrency", [Online]. Available:https://www.justice.gov/archives/ag/page/file/1326061/download

[16] Chainalysis (2020, January 17), "Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly", Chainalysis Blog, [Online]. Available: https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019

[17] Heidi Wilder (2021, September 21), "An overview of the use of cryptocurrencies in terrorist financing", The Coinbase Blog, [Online]. Available:https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7

[18] Leon Bock, Nikolaos Alexopoulos, Emine Saracoglu, Max Muhlhauser, Emmanouil Vasilomanolakis, "Assessing the Threat of Blockchain-based Botnets", APWG Symposium on Electronic Crime Research (eCrime), 2019, pp. 2-4.

[19] Kahina Khacef, Guy Pujolle, "Secure Peer-to-Peer communication based on Blockchain", HAL Archive, 2021, pp. 4-7.

[20] DataWalk (2020, November), "Cryptocurrency Investigations 101: What Every Analyst Should Know", [Online]. Available: https://datawalk.com/wp-content/uploads/2020/11/Cryptocurrency-Investigations-101-What-Every-Analyst-Should-Know-DataWalk-ebook.pdf;

[21] Kathryn Harrison, Amelia Leopold (2021, July 19), "How Blockchain Can Help Combat Disinformation", Harvard Business Review, [Online]. Available:https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation;

[22] Paula Fraga-Lamas, Tiago M. Fernandez-Carames, "Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality", IT Professional, vol. 22, no.2, 2020, pp. 2-5.

[23] Donghyo Kim, "Sun-Young Ihm, Yunsik Son, Two-Level Blockchain System for Digital Crime Evidence Management", Sensors, vol.1, 2021, pp. 3-7.

[24] Europol (2021, December 6), "SIRIUS EU Digital Evidence Situation Report 3rd Annual Report 2021", [Online].

Available: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_12_2021.pdf

[25] Yogita K. Borse, Deepti J. Patole, Gaurav Navnit Chawhan, Harsh Mukesh Parekh, Rishabh Rajmal Jain, "Advantages of Blockchain in Digital Forensic Evidence Management", 4th International Conference on Advances in Science & Technology (ICAST2021), 2021, pp. 4-6.

[26] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU;

[27] European Investment Bank, Arnold Verbeek, Maria Lundqvist (2021, October 18), "Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy Main Report", The European Commission (DG CONNECT), [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/fe087847-315d-11ec-bd8e-01aa75ed71a1/language-en;

[28] Strategy of the Ministry of Home Affairs for electronic information security (2021-2026), 172/2021;

[29] Stephen Ashurst, Stefano Tempesta, "Blockchain Applied Practical Technology and Use Cases of Enterprise Blockchain for the Real World", Productivity Press, pp. 265, 2021.

Vlad-Andrei ROTUNDU graduated the "Alexandru Ioan Cuza" Police Academy in Bucharest with a degree in law and military sciences, public order and national security. He has a master's degree in Diplomacy in International Economics from the Bucharest Academy of Economic Studies. He works in the field of cyber security and focuses his work on the study of emerging technologies from a security perspective and the development of the concept of cyber diplomacy.