International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

http://ijpsat.ijsht-journals.org
Vol. 27 No. 1 June 2021, pp.391-401

The Recent Advances, Opportunities and Challenges in the Cryptocurrencies Research field from Cybersecurity Approach

Luis Daniel LÓPEZ-ROBLES[1], Mariano Alberto CASAS-VALADEZ[2], Cecilia MONJARAZ-FRAUSTO[3], José Israel AYALA AGUILERA[4], Rubén ALVAREZ DIEZ[5], José Ricardo LÓPEZ-ROBLES[6]

[1,2,3,5,6]Academic Unit of Accounting and Administration
Universidad Autónoma de Zacatecas
Zacatecas, Mexico

[4]Academic Unit of Nursing
Universidad Autónoma de Zacatecas
Zacatecas, Mexico

***Abstract*—The convergence of new technologies and environments transform markets and sectors. Additionally, the digitization of the world represents a radical change in the way of doing business. The cryptocurrencies are one of the drivers in this change because the new finance and economic models will be one of the priorities of the developed countries and organizations. In this way, the cryptocurrencies are an unknown to everyone in general, a situation that does not help their development, deployment and use as a common element in markets and commercial relations. To resolve the above, it is necessary for professionals, academics and scientists to know what is being researched on this subject, bearing in mind aspects such as safety. This article links the concept of cryptocurrencies with that of cybersecurity, it focuses on the discussion of trends, challenges, opportunities and technologies that the mining sector requires to successfully face them using bibliometric techniques and methodologies. To do that, all the publications related to cryptocurrencies and cybersecurity hosted in Scopus from 2017 to 2021 were analyzed using VOSviewer. From the first publication since lasted one were downloaded and analyzed to identify the following aspects: most relevant research themes, most productive authors, most productive organizations, most productive countries, most relevant sources and subject, among others. These analysis establishes the first research framework related to both themes and could be used to promote the new knowledge creation.**

Keywords—cryptocurrencies, cybersecurity, financial technology, business intelligence, competitive intelligence, strategic intelligence, foresight.

I. INTRODUCTION

Cryptocurrencies are exclusively electronic money, i.e. they only exist in the digital medium. Cryptocurrencies allow buying and selling as with any ordinary currency but taking advantage of the digital world [1-5].

People could use cryptocurrencies to make quick payments and to avoid transaction fees. Some people might purchase cryptocurrencies as an investment, in the hope that it will increase in value. Cryptocurrencies can be purchased with a credit card or, in some cases, through a process called "mining." Cryptocurrencies are stored in a digital wallet or purse, either online, on your computer or other physical medium [6-10].

However, although cryptocurrencies have gone through ups and downs in their short history, they have managed to establish

Corresponding Author: José Ricardo López-Robles

themselves and grow. There are important institutions that are studying the launch of their own cryptocurrency. This gives an idea of the projection and potential of these virtual currencies, but there are still many doubts about their operation, evolution and adaptation to the real world [11-14].

The popularity and value of cryptocurrencies has made them an object of desire for many users. As a result, an increasing number of fraud attempts are hidden behind cryptocurrency transactions that never take place. The goal of these frauds is always the same: data theft. If these attacks occur on a company's computers or its employees, the organization's cybersecurity could be seriously affected [15-17].

Cyber-attacks for financial reward have also learned to take advantage of the cryptocurrency environment. Without measures in place to prevent it, it doesn't take much to compromise a company's physical cyber network and demand payment in cryptocurrencies in exchange for fixing the problem. In addition, tracing cryptocurrency transactions is virtually impossible, making the job of computer forensics very difficult [18-25].

Taking into account the above, it is necessary to understand cryptocurrencies from an integral approach, taking into account the aspects that refer to the cryptocurrencies themselves, but also those that have to do with the security of the digital world. It is clear that if the security issues associated with this type of elements are not clarified, their growth, evolution and adaptation will be affected, despite being a booming trend with strong roots in high-value sectors [26-32].

Finally, the following research shows an analysis of bibliometric networks to identify the intellectual structure of the cryptocurrencies and cybersecurity research field. Bibliometric studies provide value information about the scientific articles published in different countries, cities, institutions, and also in an individual level these studies allow to compare the scientific productivity in terms of the identification of trending subjects, the most productive researchers and institutions, and publication profiles such as scientific journals where they are published, language, publication year, type of study, associated institutions, among others [33-40].

II. Methodology and Dataset

Bibliometrics is defined as the set of methods and tools for evaluating and analyzing the evolution of the scientific and academic publications and their citations. Its aim is to analyze its impact and evaluate how these contribute to the progress of science in the main subject areas. In addition, bibliometrics allows the measurement of scientific and academic productive quality of the research field [41-50].

In the bibliometric techniques categories, performance analysis and co-occurrence map can be highlighted. The performance analysis focuses on the impact of publications based on its production and citation evolution, while co-occurrences map represents how the main publications, research themes or authors are interrelated. This last category is widely used to understand, discover and visualize relationships that are difficult to see or that are hidden between core themes for the development of the field.

Based on a first review of the state of the art, scientific and academic production, it was decided to take as source *Scopus*. In this respect, the raw data has been retrieved from the using the following advanced query: *TITLE-ABS-KEY("Cryptocurren*") AND TITLE-ABS-KEY("Cybersecur*" OR "cyber-secur*").*

Finally, this search retrieved a total of 95 publications from 2017 to 2021 (June 15th, 2021). Once this was done, all publication abstracts were downloaded and reviewed.

III. Performance Analysis of Cryptocurrencies and Cybersecurity Research Field

In order to identify the recent advances, opportunities and challenges in the cryptocurrencies research field form cybersecurity approach and vice versa, the bibliometric performance of the research field has been analyzed using the following indicators: production, impact, more productive authors, more productive countries, more productive sources, more productive subjects, among others. Furthermore, the main research themes and its relationship is presented as science map using VOSviewer. It allows the visualization of the main research themes, its relationship and analyzes the performance of the main research themes within research field.

Bearing in mind it, Table I shows the cryptocurrencies and cybersecurity production and impact from 2017 to 2021 in terms of publications and citations, respectively. It is important to highlight the growing for the first publication in 2017.

TABLE I. CRYPTOCURRENCIES AND CYBERSECURITY PRODUCTION AND IMPACT FROM 2017 TO 2021

Year	Publication(s)	Citations
2017	1	0
2018	13	6
2019	32	141
2020	36	398
2021 (*)	13	303

In line with the above, the second indicator that was analyzed is most productive authors (Table II). Choo, K.K.R., Dehghantanha, A., Doerr, C., Jahankhani, H., Jamal, A., Javed Butt, U., Kethineni, S., Malluhi, Q., Nizamuddin, N., Oosthoek, K., Parizi, R.M. and Salah, K. are the most productive authors related to cryptocurrencies and cybersecurity, and they have two publications each. Moreover, the rest of the authors has only one publication.

TABLE II. MOST PRODUCTIVE AUTHORS FROM 2017 TO 2021

Publications	Author(s)
2	Choo, K.K.R.; Dehghantanha, A.; Doerr, C.; Jahankhani, H.; Jamal, A.; Javed Butt, U.; Kethineni, S.; Malluhi, Q.; Nizamuddin, N.; Oosthoek, K.; Parizi, R.M.; Salah, K.
1	146 authors

According to the results and expressed in Table II. Regarding the bibliography performance analysis on its third indicator, the Organizations that most participated in cryptocurrencies and cybersecurity research field are *Delft University of Technology* with 3 publications, and *The University of Texas at San Antonio, University of Northumbria, Prairie View A and M University, University of Guelph, Chinese Academy of Sciences, Kennesaw State University, Brunel University London, Taras Shevchenko National University of Kyiv, University of Chinese Academy of Sciences, Financial University under the Government of the Russian Federation, Qatar University, Amity University, Noida, Khalifa University of Science and Technology,* and *Hamad Bin Khalifa University* with 2 publications each.

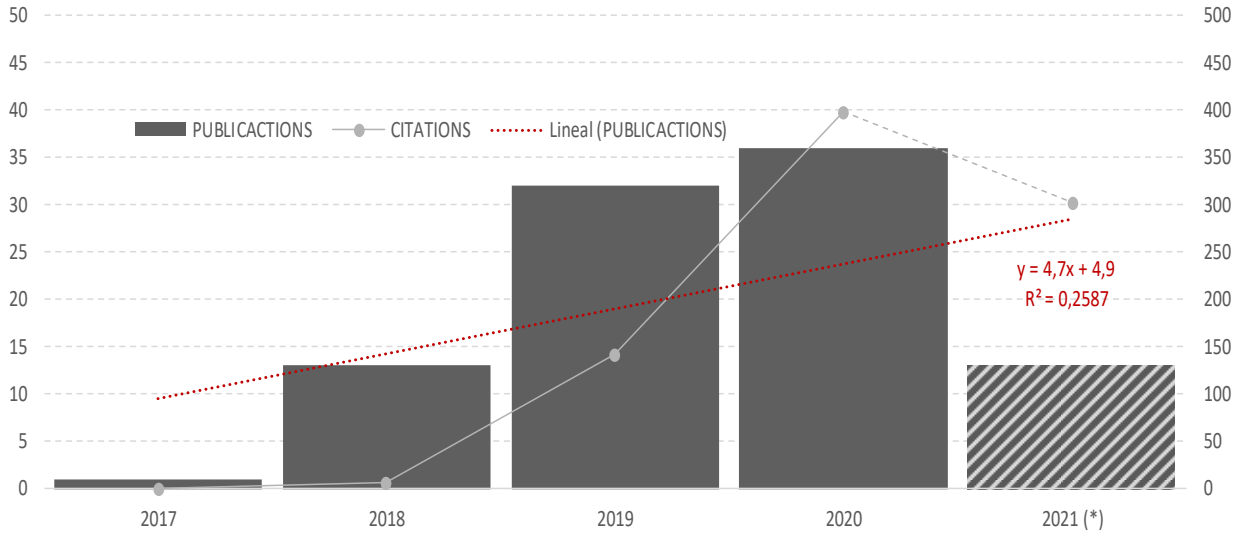


Figure 1. Distribution of publications of Cryptocurrencies and Cybersecurity from 2017 to 2021

TABLE III. MOST PRODUCTIVE ORGANIZATIONS FROM 2017 TO 2021

Publications	Organization(s)
3	Delft University of Technology
2	The University of Texas at San Antonio; University of Northumbria; Prairie View A and M University; University of Guelph; Chinese Academy of Sciences; Kennesaw State University; Brunel University London; Taras Shevchenko National University of Kyiv; University of Chinese Academy of Sciences; Financial University under the Government of the Russian Federation; Qatar University; Amity University, Noida; Khalifa University of Science and Technology; Hamad Bin Khalifa University
1	131 organizations

A fourth indicator that was considered to identify the recent advances, challenges and opportunities of the cryptocurrencies and cybersecurity research field is the geographical distribution of the publications, in order to know which countries carry out more research on this topic. The data obtained from the analysis are shown in Table IV. Highlighting United States with 23 publications, India with 12 publications, United Kingdom with 7 publications, Russia with 5 publications and China with 5 publications.

TABLE IV. MOST PRODUCTIVE COUNTRIES FROM 2017 TO 2021

Publications	Country(ies)
23	United States
12	India
7	United Kingdom
6	Russia
>=5	37 countries

Another indicator is to know the sources that handle more research on cryptocurrencies and cybersecurity, according to the data obtained and expressed in Table V, it finds that the most prominent sources are *ACM International Conference Proceeding Series* and *Advances in Intelligent Systems and Computing* with 4 publications each, and *IEEE Access* and *Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics* with 3 publications each, respectively.

TABLE V. MOST PRODUCTIVE SOURCES FROM 2017 TO 2021

Publications	Source(s)
4	ACM International Conference Proceeding Series; Advances In Intelligent Systems And Computing
3	IEEE Access; Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics
2	Advances In Information Security; Applied Network Science; Communications In Computer And Information Science; Sustainability Switzerland
1	41 sources

The last indicator considered is to know the research areas where cryptocurrencies and cybersecurity are applied. The results are shown in Table VI, the most prominent area are Computer Science, Engineering, Social Sciences, and Decision Sciences with 67, 39, 19 and 15 publications, respectively.

Finally, in order to effectively analyze to identify the main research themes related to cryptocurrencies and cybersecurity research field and its relationship in recent years are determined in the following section using *VOSviewer*.

TABLE VI. MOST PRODUCTIVE SUBJECTS FROM 2017 TO 2021

Publications	Subject(s)
67	Computer Science
39	Engineering
19	Social Sciences
15	Decision Sciences
>=13	14 subjects

IV. SCIENCE MAPPING ANALYSIS

The co-occurrence map tool enables the analysis of scientific and academic papers, and can be used to visualize and evaluate complex research topics. In Figure 1, the co-occurrence map of the main research themes related to cryptocurrencies and cybersecurity research field and its relationship is shown. It is based on information retrieved from *Scopus*, covering publications from 2017 to 2021.

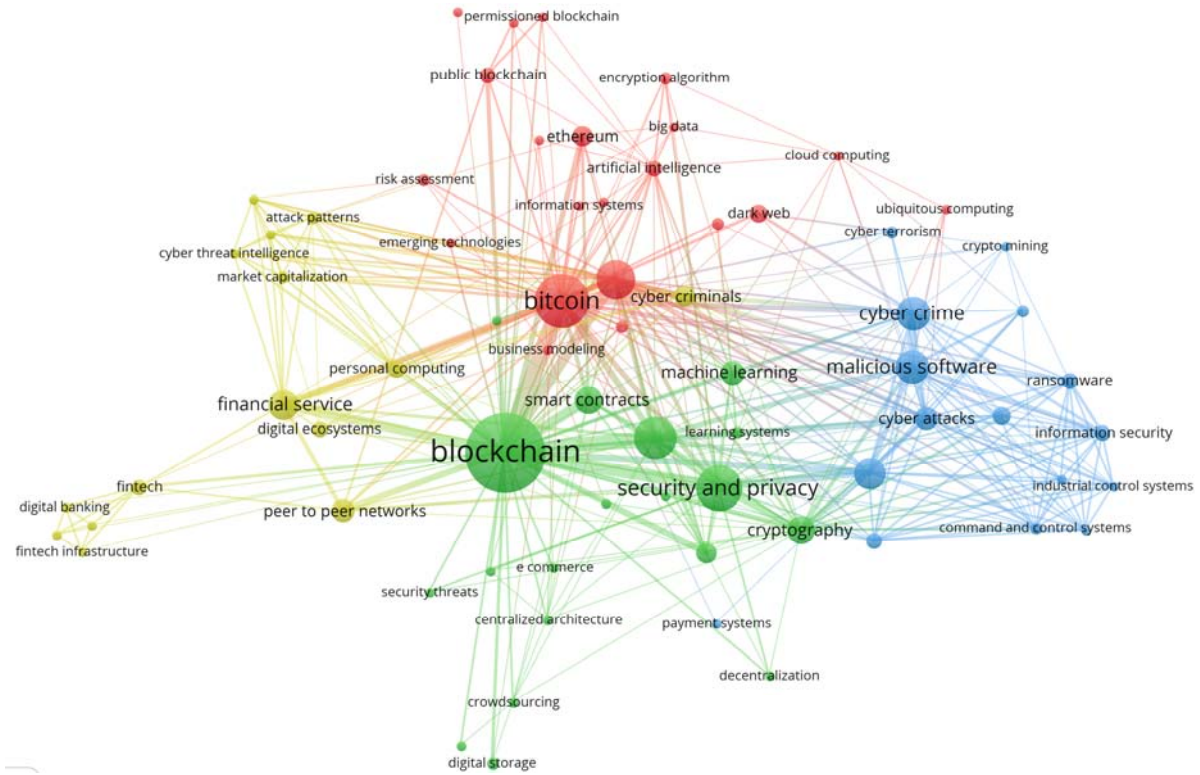
Taking into account the results of the science map presented below, four clusters were identified and analyzed according its structure and performance: Cryptocurrencies (21 research themes, 332 links and 96 occurrences), New technologies (19 research themes, 335 links and 147 occurrences), Cybersecurity (16 research themes, 308 links and 81 occurrences), and New environments (15 research themes, 235 links and 57 occurrences).

In terms of occurrences and link the most relevant clusters are New technologies and Cryptocurrencies, respectively. These themes cover the main research themes of the research field and are the link to the rest of clusters.

The New technologies cluster is the second one in terms of themes, but it is the most relevant in terms of links and occurrences. The New technologies cluster is structured by the following research themes: blockchain, internet of things, security and privacy, cryptography, smart contracts, machine learning, consensus algorithms, learning systems, security challenges, centralized architecture, data mining, processing capability, e commerce, crowdsourcing, learning algorithms, security threats, decentralization, digital storage, and fog computing.

The Cryptocurrencies cluster is the first one in terms of themes, but is the second one in terms of occurrences and links. The Cryptocurrencies cluster is structured by the following research themes: security of data, bitcoin, ethereum, artificial intelligence, intelligent computing, risk assessment, private key, public blockchain, dark web, encryption algorithm, permissioned blockchain, private blockchain, business modeling, information systems, information use, cloud computing, emerging technologies, forecasting technologies, big data, supply chain management, and ubiquitous computing.

The Cybersecurity cluster is the third one in terms of research themes, occurrences and links. The Cryptocurrencies cluster is structured by the following research themes: network security, malicious software, cyber attacks, cyber crime, sustainable development, intrusion detection systems, ransomware, information security, command and control systems, social media, industrial control systems, scada systems, supervisory control and data acquisition, cyber terrorism, crypto mining, and payment systems.



Cluster	Themes (the most productive)	Weight	Total link strength	Occurrences
Cryptocurrencies	security of data	48	102	16
	bitcoin	47	114	27
	ethereum	20	29	6
	artificial intelligence	19	25	4
	intelligent computing	17	20	3
	risk assessment	17	18	3
	private key	16	16	2
	public blockchain	16	23	4
	dark web	15	20	5
	encryption algorithm	15	17	3
New technologies	blockchain	58	179	48
	internet of things	45	88	18
	security and privacy	39	84	21
	cryptography	34	64	10
	smart contracts	22	42	10
	machine learning	20	31	8
	consensus algorithms	14	26	6
	learning systems	11	13	3
	security challenges	11	13	2
	centralized architecture	10	11	2
Cybersecurity	network security	31	71	12
	malicious software	30	73	13
	cyber attacks	28	52	7
	cyber crime	27	54	13
	sustainable development	23	35	4

		intrusion detection systems	20	24	3
		ransomware	20	35	4
		information security	19	37	4
		command and control systems	18	30	3
		social media	18	23	5
	New environments	cyber criminals	30	50	6
		financial service	29	60	11
		digital ecosystems	25	28	4
		personal computing	23	36	5
		peer to peer networks	21	36	7
		attack patterns	14	24	3
		market capitalization	13	23	3
		cryptocurrency exchanges	12	21	2
		cyber threat intelligence	12	21	2
		fintech	12	20	4

Figure 2. Science map of cryptocurrencies and cybersecurity. The main research themes included in each research field.

The New environments cluster is the fourth one in terms of research themes, occurrences and links. The New environments cluster is structured by the following research themes: cyber criminals, financial service, digital ecosystems, personal computing, peer to peer networks, attack patterns, market capitalization, cryptocurrency exchanges, cyber threat intelligence, fintech, industry standards, digital banking, fintech business models, fintech infrastructure, and fintech landscape.

Therefore, and taking into consideration the clusters, four baseline research lines are identified. These lines of research are related to cybersecurity, new technologies related to digital environments, application of these researches and the fintech environment. Finally, these clusters establish the main research framework related to cryptocurrencies and cybersecurity research and the links to other knowledge areas that are pushing these topics.

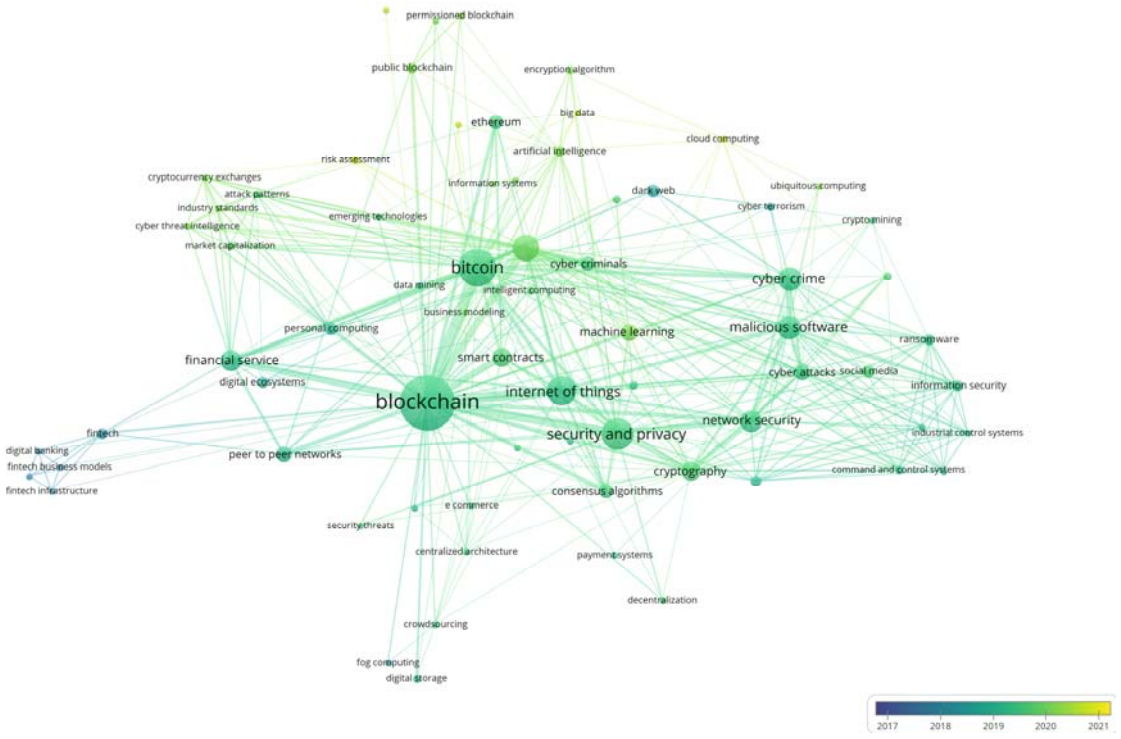


Figure 3. Evolution of the cryptocurrencies and cybersecurity research field

V. Conclusions

In terms of bibliometric performance, the size of literature related to cryptocurrencies and cybersecurity showed a noteworthy increase in the last years (2017–2021).

Given the large volume of publications and citations received in this field, it is expected that the interest will continue to grow and serve as a support to other knowledge areas such as information and communication technologies, finance technologies, entrepreneurship and new business models.

The present research presents the first bibliometric study about cryptocurrencies and cybersecurity, identifying the main research themes and related knowledge areas. More than 95 original research articles have been analyzed and processed using *VOSviewer*.

The most productive organizations are *Delft University of Technology*, *The University of Texas at San Antonio, University of Northumbria, Prairie View A and M University, University of Guelph, Chinese Academy of Sciences, Kennesaw State University, Brunel University London, Taras Shevchenko National University of Kyiv, University of Chinese Academy of Sciences, Financial University under the Government of the Russian Federation, Qatar University, Amity University, Noida, Khalifa University of Science and Technology,* and *Hamad Bin Khalifa University*. In this way, the most productive countries are United States, India, United Kingdom and Russia. The correspondence between the most productive organizations and countries reflects the balance and quality of the publications covered by this research field.

According to the science mapping analysis developed using VOSviewer tool, four base research themes cluster were identified. The main themes covered by these cluster are: security of data, artificial intelligence, blockchain, internet of things, security and privacy, cryptography, machine learning, learning systems, security challenges, malicious software, cyber attacks, cyber crime, cyber criminals, financial service, digital ecosystems, cryptocurrency exchanges, cyber threat intelligence, and fintech.

Finally, we would like to address some future works. First, a global analysis could be carried out taking into account a wider time span and enriching the query with more search terms. Second, the evolution of the research themes could be studied across the consecutive time periods for the main sectors in the finance and business field.

Acknowledgment

The authors acknowledge the support by the CONACYT-Consejo Nacional de Ciencia y Tecnología (Mexico), DGRI-Dirección General de Relaciones Exteriores (Mexico) and COZCYT- Consejo Zacatecano de Ciencia Tecnología e innovación to carry out this study.

References

[1] C. Alexander, and M. Dakos, “A critical investigation of cryptocurrency data and analysis,” *Quantitative Finance,* vol. 20, no. 2, pp. 173-188, 2020.

[2] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto, and J. M. Corchado, "Blockchain technology: a review of the current challenges of cryptocurrency." pp. 153-160.

[3] Y. Sovbetov, “Factors influencing cryptocurrency prices: Evidence from bitcoin, ethereum, dash, litcoin, and monero,” *Journal of Economics and Financial Analysis,* vol. 2, no. 2, pp. 1-27, 2018.

[4] R. N.-U.-D. Jalal, I. Alon, and A. Paltrinieri, “A bibliometric review of cryptocurrencies as a financial asset,” *Technology Analysis & Strategic Management*, pp. 1-16, 2021.

[5] M. S. Hossain, “What do we know about cryptocurrency? Past, present, future,” *China Finance Review International*, 2021.

[6] P. P. Momtaz, “The pricing and performance of cryptocurrency,” *The European Journal of Finance*, pp. 1-14, 2019.

[7] K.-C. Yen, and H.-P. Cheng, “Economic policy uncertainty and cryptocurrency volatility,” *Finance Research Letters,* vol. 38, pp. 101428, 2021.

[8] S. Qureshi, M. Aftab, E. Bouri, and T. Saeed, “Dynamic interdependence of cryptocurrency markets: An analysis across time and frequency,” *Physica A: Statistical Mechanics and its Applications,* vol. 559, pp. 125077, 2020.

[9] K. Grobys, S. Ahmed, and N. Sapkota, "Technical trading rules in the cryptocurrency market," *Finance Research Letters,* vol. 32, pp. 101396, 2020.

[10] G. Tepe, and U. B. Geyikçi, "FinTech Companies: A Bibliometric Analysis," 2020.

[11] J. Liang, L. Li, and D. Zeng, "Evolutionary dynamics of cryptocurrency transaction networks: An empirical study," *PloS one,* vol. 13, no. 8, pp. e0202202, 2018.

[12] J. Liu, and A. Serletis, "Volatility in the cryptocurrency market," *Open Economies Review,* vol. 30, no. 4, pp. 779-811, 2019.

[13] B. M. Lucey, S. A. Vigne, L. Yarovaya, and Y. Wang, "The cryptocurrency uncertainty index," *Finance Research Letters*, pp. 102147, 2021.

[14] M. A. Nasir, T. L. D. Huynh, S. P. Nguyen, and D. Duong, "Forecasting cryptocurrency returns and volume using search engines," *Financial Innovation,* vol. 5, no. 1, pp. 1-13, 2019.

[15] N. A. Kyriazis, "A survey on efficiency and profitable trading opportunities in cryptocurrency markets," *Journal of Risk and Financial Management,* vol. 12, no. 2, pp. 67, 2019.

[16] M. H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Transactions on Engineering Management,* vol. 67, no. 4, pp. 1196-1212, 2019.

[17] A. Mikhaylov, M. S. S. Danish, and T. Senjyu, "A New Stage in the Evolution of Cryptocurrency Markets: Analysis by Hurst Method," *Strategic Outlook in Business and Finance Innovation: Multidimensional Policies for Emerging Economies*: Emerald Publishing Limited, 2021.

[18] J. Kubicek, "Complications of Cryptocurrency: Financial and Cybersecurity Risk in the Age of Bitcoin," Utica College, 2018.

[19] C. Gurdgiev, and A. Fleming, "Informational efficiency and cybersecurity threats: A Social Impact Finance perspective of the systemic threats to blockchain applications," 2021.

[20] G. Kabanda, "Cybersecurity risk management plan for a blockchain application model," *Trans Eng Comput Sci,* vol. 2, no. 1, pp. 221, 2021.

[21] G.-L. Schipor, "Risks and Opportunities in the Cryptocurrency Market," *Ovidius University Annals, Economic Sciences Series,* vol. 19, no. 2, pp. 879-883, 2019.

[22] K.-K. R. Choo, A. Dehghantanha, and R. M. Parizi, *Blockchain cybersecurity, trust and privacy*: Springer, 2020.

[23] A. Serapiglia, "Cybersecurity and cryptocurrencies: introducing ecosystem vulnerabilities through current events," *EDSIG ISSN,* vol. 2473, pp. 3857, 2019.

[24] P. Bansal, R. Panchal, S. Bassi, and A. Kumar, "Blockchain for Cybersecurity: A Comprehensive Survey." pp. 260-265.

[25] R. M. Parizi, A. Dehghantanha, A. Azmoodeh, and K.-K. R. Choo, "Blockchain in Cybersecurity Realm: An Overview," *Blockchain Cybersecurity, Trust and Privacy*, pp. 1-5, 2020.

[26] R. Lombardi, C. de Villiers, N. Moscariello, and M. Pizzo, "The disruption of blockchain in auditing–a systematic literature review and an agenda for future research," *Accounting, Auditing & Accountability Journal*, 2021.

[27] R. Duan, and L. Guo, "Application of Blockchain for Internet of Things: A Bibliometric Analysis," *Mathematical Problems in Engineering,* vol. 2021, 2021.

[28] A. Firdaus, M. F. Ab Razak, A. Feizollah, I. A. T. Hashem, M. Hazim, and N. B. Anuar, "The rise of "blockchain": bibliometric analysis of blockchain study," *Scientometrics,* vol. 120, no. 3, pp. 1289-1331, 2019.

[29] L. Ante, "Smart Contracts on the Blockchain–A Bibliometric Analysis and Review," *Telematics and Informatics*, pp. 101519, 2020.

[30] F. Z. Chentouf, and S. Bouchkaren, "Blockchain for Cybersecurity in IoT," *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, pp. 61.

[31] P. Bhaskar, C. K. Tiwari, and A. Joshi, “Blockchain in education management: present and future applications,” *Interactive Technology and Smart Education*, 2020.

[32] S. Jiang, X. Li, and S. Wang, “Exploring evolution trends in cryptocurrency study: From underlying technology to economic applications,” *Finance Research Letters,* vol. 38, pp. 101532, 2021.

[33] J. R. López-Robles, J. R. Otegi-Olaso, I. Porto-Gómez, and M. J. Cobo, “30 years of intelligence models in management and business: A bibliometric review,” *International Journal of Information Management,* vol. 48, pp. 22-38, 2019.

[34] J. R. López-Robles, J. Guallar, J. R. Otegi-Olaso, and N. K. Gamboa-Rosales, “El profesional de la información (EPI): bibliometric and thematic analysis (2006-2017),” *El profesional de la información,* vol. 28, no. 4, pp. e280417, 2019.

[35] E. Herrera-Viedma, J.-R. López-Robles, J. Guallar, and M.-J. Cobo, “Global trends in coronavirus research at the time of Covid-19: A general bibliometric approach and content analysis using SciMAT,” *El Profesional de la Información, 2020, vol. 29, num. 3*, 2020.

[36] L. B. Furstenau, M. K. Sott, L. M. Kipper, Ê. L. Machado, J. R. López-Robles, M. S. Dohan, M. J. Cobo, A. Zahid, Q. H. Abbasi, and M. A. Imran, “Link between sustainability and industry 4.0: trends, challenges and new perspectives,” *IEEE Access,* vol. 8, pp. 140079-140096, 2020.

[37] J. R. López-Robles, M. J. Cobo, N. K. Gamboa-Rosales, and E. Herrera-Viedma, "Mapping the Intellectual Structure of the International Journal of Computers Communications and Control: A Content Analysis from 2015 to 2019." pp. 296-303.

[38] J. R. López-Robles, J. R. Otegi-Olaso, R. Arcos, N. K. Gamboa-Rosales, and H. Gamboa-Rosales, “Mapping the structure and evolution of JISIB: A bibliometric analysis of articles published in the Journal of Intelligence Studies in Business between 2011 and 2017,” *Journal of Intelligence Studies in Business,* vol. 8, no. 3, 2018.

[39] M. K. Sott, L. B. Furstenau, L. M. Kipper, Y. P. R. Rodrigues, J. R. López-Robles, F. D. Giraldo, and M. J. Cobo, “Process modeling for smart factories: using science mapping to understand the strategic themes, main challenges and future trends,” *Business Process Management Journal*, 2021.

[40] J. R. López-Robles, J. R. Otegi-Olaso, I. Porto-Gomez, H. Gamboa-Rosales, and N. K. Gamboa-Rosales, “Understanding the intellectual structure and evolution of Competitive Intelligence: A bibliometric analysis from 1984 to 2017,” *Technology Analysis & Strategic Management,* vol. 32, no. 5, pp. 604-619, 2020.

[41] A. Faz-Mendoza, N. K. Gamboa-Rosales, C. Medina-Rodríguez, M. A. Casas-Valadez, A. Castorena-Robles, and J. R. López-Robles, "Intelligent processes in the context of Mining 4.0: Trends, research challenges and opportunities." pp. 480-484.

[42] C. E. Medina-Rodríguez, M. A. Casas-Valadez, A. Faz-Mendoza, R. Castañeda-Miranda, N. K. Gamboa-Rosales, and J. R. López-Robles, "The cyber security in the age of telework: A descriptive research framework through science mapping." pp. 1-5.

[43] M. A. Casas-Valadez, A. Faz-Mendoza, C. E. Medina-Rodriguez, M. Cobo, N. K. Gamboa-Rosales, and J. R. López-Robles, "Research trends in Sentiment Analysis and Opinion Mining from Knowledge Management approach: A science mapping from 2007 to 2020." pp. 1-6.

[44] C. E. Medina-Rodríguez, M. Casas-Valadez, A. Faz-Mendoza, A. Castorena-Robles, N. Gamboa-Rosales, and J. R. López-Robles, "Decision Management in the telework context: Trends, challenges and implications." pp. 307-311.

[45] J.-R. López-Robles, M.-A. Casas-Valadez, A. Guzmán-Fernández, C. Monjaraz-Frausto, A. Castorena-Robles, and N.-K. Gamboa-Rosales, "Understanding the relationship between e-learning and web 2.0: A bibliometric and thematic analysis from 2006 to 2020." pp. 290-295.

[46] A. Castorena-Robles, N.-K. Gamboa-Rosales, A. Faz-Mendoza, M.-A. Casas-Valadez, C.-E. Medina-Rodríguez, and J.-R. López-Robles, "Exploring the role of Medical Decision Making in Biotechnology field through science mapping." pp. 403-407.

[47] M. A. Casas-Valadez, A. Faz-Mendoza, C. E. Medina-Rodríguez, A. Castorena-Robles, N. K. Gamboa-Rosales, and J. R. López-Robles, "Decision Models in Marketing: The role of Sentiment Analysis from bibliometric analysis." pp. 561-565.

[48] N.-K. Gamboa-Rosales, A. Castorena-Robles, M.-A. Casas-Valadez, M.-J. Cobo, R. Castañeda-Miranda, and J.-R. López-Robles, "Decision Making using Internet of Things and Machine Learning: A bibliometric approach to tracking main research themes." pp. 1-6.

[49] M. A. Casas-Valadez, A. Faz-Mendoza, C. E. Medina-Rodríguez, R. Castañeda-Miranda, N. K. Gamboa-Rosales, and J. R. López-Robles, "The synergic relationship between e-commerce and Sentiment Analysis: A content analysis of published articles between 2007 and 2020." pp. 1-5.

[50] M. K. Sott, L. B. Furstenau, L. M. Kipper, Y. P. R. Rodrigues, J. R. López-Robles, F. D. Giraldo, and M. J. Cobo, “Process modeling for smart factories: using science mapping to understand the strategic themes, main challenges and future trends,” Business Process Management Journal, 2021.