



# Cryptocurrencies, Systematic Literature Review on Their Current Context and Challenges

Yeray Mezquita<sup>(✉)</sup>, Marta Plaza-Hernández, Mahmoud Abbasi,  
and Javier Prieto

BISITE Research Group, University of Salamanca, Edificio Multiusos I+D+i, Calle  
Espejo 2, 37007 Salamanca, Spain

yeraymm@usal.es martaplaza@usal.es Mahmoud.abbasi@ieee.org javierp@usal.es

**Abstract.** The financial crisis of 2008 breached society's trust in banks and centralized financial institutions. Bitcoin appeared as a response to those transgressions, proving that the blockchain technology it implements is reliable. Since then, this technology has become widespread in the form of new cryptocurrencies and an increasing number of people have begun to invest in them. In the absence of a body to regulate the cryptocurrency market, users play with and encourage the fluctuations in their price, causing them to be treated as investment assets rather than transaction assets. This work carries out and then discusses a systematic study of the state of the art and of the general challenges faced by cryptocurrencies.

**Keywords:** Cryptocurrencies · Systematic review · Challenges

## 1 Introduction

The 2008 financial crisis breached the society's trust in banks and centralized financial institutions; these entities led to the crisis by lending large sums of money while keeping very little in reserve [11, 18]. Bitcoin emerged in 2009, in response to those transgressions. Its solution was a currency that could operate without a central authority [41]. Bitcoin comprises a series of cryptographic protocols that completely transform the process of making transactions. Thus, these protocols have brought the financial system one step closer to a truly democratic economy constructed by the community [8, 22, 26, 36, 51].

Due to the relative immaturity of blockchain technology, cryptocurrencies face technical issues such as network latency, network governance, transaction load, etc. Besides, while the appearance of a truly democratic economy is one of the strengths of using cryptocurrencies, it can also become the biggest problem for their adoption. In the absence of a body to regulate cryptocurrencies, users play with and encourage the fluctuations in their price, causing them to be treated as investment assets rather than transaction ones [14, 19, 29, 43, 49, 55].

This article provides a systematic review of the general challenges faced by cryptocurrencies and their underlying technologies, which helps in organizing the works previously done in the literature. Everyone interested in using cryptocurrencies, in any kind of way, will find this work useful, because it will help them to understand the challenges, at any level, that cryptocurrencies are facing.

Following the introduction, Sect. 2 presents the methodology used for the systematic literature review. In each of its subsections, it is presented the discussion on each of the research questions that have arise in this study. Finally, Sect. 3 concludes this work.

## 2 Proposed Framework

In this work, a systematic review of the literature [2,42] is carried out regarding the use of cryptocurrencies, the general vulnerabilities they face, and the cryptocurrency-related crimes that it is possible to commit with them. To achieve our goals, we have proposed the following questions to be answered during our study:

- **Q1:** What research has been carried out previously in the literature regarding the use of cryptocurrencies?
- **Q2:** What are the vulnerabilities that affect the adoption of cryptocurrencies?
- **Q3:** How are crimes committed with crypto affecting the global socio-economic ecosystem?

For the purpose of this study, we have used the following scientific databases to search for articles: ScienceDirect, IEEE Explore, ACM Digital Library, and Springer-Link. Given that the Google Scholar results consisted mostly of articles that had not been peer-reviewed and that were not related to our study, this source has not been considered.

We have identified 4 keywords that are relevant to the topic of our study: Blockchain, Cryptocurrency, Challenge, and Adoption; each of these keywords is represented by the following search strings:

- **Blockchain:** (“distributed ledger technology” OR blockchain\*)
- **Cryptocurrency:** (crypto\* OR cryptocurrency\*)
- **Challenge:** challenge\*
- **Adoption:** adopt\*

To obtain relevant works stored in each database, four queries have been carried out with the combination of the above keywords and search strings:

- **SS1:** Blockchain AND Cryptocurrency AND Challenge
- **SS2:** Blockchain AND Cryptocurrency AND Challenge AND Adoption
- **SS3:** Cryptocurrency AND Challenge
- **SS4:** Cryptocurrency AND Challenge AND Adoption

All publications available in the databases that matched the search criteria and had been published no later than May 2020, were included in this study.

## 2.1 Q1: What Research Has Been Carried Out Previously in the Literature Regarding the Use of Cryptocurrencies?

This question has been asked to motivate the study of this work. We propose two new questions associated:

- RQ1.1: Has the possibility of mass adoption of cryptocurrencies been sufficiently studied?
- RQ1.2: Is it justified to carry out this study despite what has been done previously?

To find an answer to RQ1, a study has been made from papers that have addressed the topic of the use of cryptocurrencies from different perspectives. All the works that do not make a review of the challenges of the cryptocurrencies or a study of the value that their features provide have been excluded from this section.

In [10] and [53] a review of the fundamentals of cryptocurrencies is shown. These reviews indicate that the risks of buying cryptocurrencies lie in the absence of a legal basis, which prevents the excessive price fluctuations to which they are subjected daily. It also shows how the possibility of wallet theft is real, and that cryptocurrencies are often used for money laundering and illegal activities. In [35] it has been studied the frameworks proposed in the literature for the prediction of cryptocurrency prices. The conclusion reached by the study is that the prices are still dependent on the opinion of influencers that can manipulate the prices and the regulation of the governments.

In [30] a review has been made, although only on Bitcoin, of the most relevant aspects that affect the confidence of the users in that cryptocurrency. It is stated that cryptocurrencies rely on three technological elements: blockchain networks, cryptocurrency wallets, and exchange platforms. From those three constructs, 11 attributes have been detected as capable of building trust in investors, from which there are three that are the most relevant: the number of transfers made, the immutability of the blockchain, and the openness of the platform. The transfers made with a cryptocurrency are related to the usability given in its economic ecosystem. The other two attributes are related only to the technology used: openness creates transparency and immutability creates accountability.

Eyal [13] has studied the challenges that cryptocurrencies face in terms of resources spent, user privacy, and the risks of using smart contracts. To optimize the number of resources spent, a small review of the alternatives in the consensus algorithms is made, also addressed in works such as [49]. In addition, it has been studied the options of working off-chain and using a layer of software that works over a blockchain network. Regarding the improvement of the users' privacy, it is proposed the mixing of transactions to avoid their traceability (e.g. through token ring signatures), and the use of cryptographic keys called Zero-Knowledge Proofs (ZKP) [45]. In [15] the alternatives that exist when dealing with the privacy of the identity of users and the transactions carried out have been studied also. This study concludes that the methods have limitations, for example, ZKPs

require a lot of computing power. Besides, the possibility of complete privacy carries the risk of users abusing it and committing crimes that states cannot punish.

From this sub-section, it can be summarized that the biggest disadvantage cryptocurrencies face is the fluctuation in their price, which prevents them from being used daily. However, they are still being used in illegal activities, such as money laundering and drug dealing, a problem that the legislation must tackle through regulation [5, 50], as has been stated in numerous works of the literature [4, 46]. Besides, it has been studied how distributed networks challenge existing legal mechanisms of allocating responsibility, concluding that collaboration between legal scholars and technological developers is necessary [5], and answering RQ1.

Finally, regarding RQ1.1 it has been shown that there are works that study the cryptocurrencies' flaws and aspects that influence the mass adoption of this market. But, it is no work in the literature that put them all together, being the justification of this paper's study asked in RQ1.2.

## 2.2 Q2: What Are the Vulnerabilities that Affect the Adoption of Cryptocurrencies?

In the Sect. 2.1, it has been found the economic implications of the fluctuating nature of cryptocurrency prices. By answering Q2, we seek to identify what are the factors that allow those fluctuations and are harmful to the mass adoption of cryptocurrencies [52]. In this subsection, we will focus on the works whose studies point out types of vulnerabilities and problems that affect the use of cryptocurrencies as transactional assets.

Because of the fluctuating nature of the cryptocurrencies' price, there have been numerous articles that have tried to find a pattern in it [35]. In [44] it is mapped the change in features on users and network activities to understand the dynamics of the Bitcoin cryptocurrency. To analyze the results it has been proposed a machine learning model to predict the changes in the prices. This model is based on the computed correlation between features such as hash rate, number of users, transaction rate, the total number of bitcoins, and price. Following that trend, in [1] has done an analysis of the factors that impact the adoption decision of a cryptocurrency, along with the impact of those factors based on the quantification of users' judgments. That manuscript suggests that the users of cryptocurrencies are influenced by economic, technical, social, and personal factors. From the defined factors, it was found that the top criteria used by the investors were the investment opportunity, subjective norms, business acceptance, privacy, and global attention. Being the economic and social factors as the general rules.

However, the problem observed from the review carried out is the little information that society has about how to use cryptocurrencies and the technology on which they rely. Most of the attacks are due because users are not careful enough with their passwords for their wallets, and how to store them, not because of the technology [16]. E.g. some of the recommendations on how to anticipate

this kind of problem are not to reuse wallet addresses, to introduce new address types using stronger hashing and signature schemes, etc.

There have been cases of coin theft via smart contracts, like in the case of the DAO attack [32]. Due to a vulnerability in the code of the smart contract, it was stolen millions of dollars in Ether. As for this kind of problem, users must make sure that these smart contracts had been previously audited correctly, before being deployed in the corresponding blockchain network [7, 31, 33–35, 37–40, 40].

Exchanges are the most widely used gateway to bring users closer to the main cryptocurrencies and the great risks users are facing when investing in them. Attacks on exchanges created a strong alarm in the community, as they have been the main gateway for users (although mostly speculative investors). Because of that, [23] has proposed an economic model to capture the short-term incentives of cryptocurrency exchanges concerning making security investments and establishing transaction fees, which would help to build the trust of the users.

While blockchain technology has been created with the intention of replacing the current, centralized financial system, authors of [21] claim that blockchain technology is capable of replacing intermediaries while ensuring the security of other kinds of platforms. Although this technology offers resistance to traditional cyberattacks, hackers have developed new forms of cyberattacks, specifically targeted at blockchain technology [6, 17, 25, 27, 36].

There also exist vulnerabilities regarding the anonymity of the users that use cryptocurrencies. In [28] the issue is developed in terms of the regulation advantages and drawbacks that pseudo-anonymity currently has in the Bitcoin ecosystem. While studying also the risk that genuinely anonymous transactions, for example in terms of illegal activities, like money laundering or drug dealing, would entail.

From this subsection, it can be concluded that cryptocurrencies are seen by the users as investment instruments, and not as transactional ones. It has been shown that by using artificial intelligence models, patterns in price fluctuation can be predicted over a week, which helps speculation and avoid its mainstream adoption as a transactional asset. Another economic aspect is that investors tend to keep the social aspect in mind, what others think of a cryptocurrency, more than the technology behind it. On the other hand, it can be concluded that one of the ways to resist high speculation is a healthy economic ecosystem underlying a robust network of nodes [1, 44].

Many of the studied papers talk about the technology behind a cryptocurrency as one of the most important features to determine its price. The highlights in this respect are the network of nodes that ensures the immutability of the blockchain; the transparency that is obtained from a network of nodes governed in a distributed manner; and the cost of keeping the network operational [39]. However, the price also depends on the economic ecosystem surrounding a cryptocurrency. However, it has been found that most of the users are speculative investors and not people with real intentions to participate actively in those ecosystems. Therefore, factors such as visibility in social networks and the use given to a cryptocurrency are strongly related to its market capitalization [1, 35, 44].

### 2.3 Q3: How Are Crimes with Crypto Affecting the Socio-economic Ecosystem in the World?

Due to the pseudo-anonymous character of crypto, many illegal activities take advantage of it in the dark web [3, 48]: money laundering, purchase of weapons and drugs. This is a characteristic of cryptocurrencies that makes them be targeted by states and has caused the prohibition of their use in some of them.

In the literature, studies have been carried out on the social ecosystem of the dark web in the market for illegal substances. In [50], it has been made an exploratory study on how New psychoactive substances (NPS) are being sold with the help of cryptocurrencies. Another legal problem arises when financial scams appear in the cryptocurrency market. It is demonstrated in [24], with a proposed detection system, that the pump-and-dump schemes happen and may be detected by examining real-world use cases. Given that this kind of scams should be penalized by law to help protect investors.

To tackle the previously mentioned problems, cryptocurrencies as structures that are designed to circumvent the regulation can always be prohibited. To avoid prohibitory solutions, a combination of established and novel concepts for regulating new technological phenomena could be implemented [12]. That's the case of Gibraltar, which is regulating DLTs also as a competitive tool and a means for creating new public value. The study carried out in [46] contributes to the emerging view of smart regulation as an enabler and protector rather than an inhibitor and obstacle in areas of rapid innovation.

Right now it is unclear whether or not regulatory approaches based on principles rather than hard rules, like in the case of Gibraltar, would be practical only for small and highly agile jurisdictions. In [54] it is stated that a mix of soft law and hard law tools is needed for a successful regulatory framework. Those tools will help install sandbox regimes for a transitional period and at the same time inform about the legal consequences of participating in distributed ledger technologies that lack clear structures of responsibility. As another example, in [20] is stated that virtual currencies pose a serious threat to be used for money laundering, and by so, weakening the European Union's financial system. That's why directive (EU) 2018/843 (the fifth anti-money laundering Directive) intends to mitigate these risks by introducing a definition of virtual currencies within Union law.

Regulating, not only helps protect investors from fraudulent token issuers but also helps to fulfill other worthwhile goals, such as providing additional funding for small to medium-sized enterprises and financial inclusion [47]. In the Initial Coin Offering (ICO) area, [9] has stated that ICOs must be regulated, because a ban in that area, may stifle the innovation and is not conducive to the development of FinTech and blockchain technology.

According to [5], it is stated that current General Data Protection Laws are a challenge to distributed networks. Nodes of a blockchain network, according to article 26 of the General Data Protection Regulation (GDPR), are obliged to determine their respective responsibilities. Therefore, a solution to allocating responsibility for data protection in distributed networks lies outside the GDPR.

Using the Bitcoin network as an example, the transfers stored constitute personal data within the meaning of Article 4(1) GDPR, because the users behind these transfers are identifiable via their Bitcoin address(es). Also, full nodes qualify as establishments under Article 3(1) GDPR and the Bitcoin network provides a service within the meaning of Article 3(2)(a) GDPR to data subjects in the EU. Therefore, it is concluded that the data processing carried out within the Bitcoin blockchain, and therefore in the rest of the cryptocurrency blockchains, falls within the material and the territorial scope of the GDPR.

By answering Q3, it has been found that the most effective way to tackle the challenges posed by crypto and DLTs is by applying a sandbox of a mix of soft laws and hard laws to the legal framework of a country. This way it is possible to regulate the activities carried out, protecting investors and impeding crimes like laundering fraud, while allowing innovation in the area. Which could lead to a potential replacement of the current financial system.

### 3 Conclusion

The capitalization boom of the cryptocurrency market has contributed to the increase in the number of them. Each one of the cryptocurrencies is supported by a DLT platform, whose technology builds user trust in the cryptocurrency and therefore contributes greatly to its value. This work provides a systematic review of the general challenges faced by cryptocurrencies and their underlying technologies. Focusing on answering three research questions: (Q1) What research has been carried out previously in the literature regarding the use of cryptocurrencies? (Q2) What are the vulnerabilities that affect the adoption of cryptocurrencies? (Q3) What crimes are being carried out with crypto that poses a threat to its adoption?

From the studies related to Q1, it can be summarized that it has been stated in numerous works that cryptocurrencies need some kind of regulation. Because although they face great fluctuations in their price, they are still being used in illegal activities, such as money laundering and drug dealing. Besides, it has pointed out how distributed networks challenge existing legal mechanisms of allocating responsibility, concluding that collaboration between legal scholars and technological developers is necessary.

Works related to Q2 point out how the technology behind a cryptocurrency is one of the most important features to determine a cryptocurrency price. The highlights in this respect are the network of nodes that ensures the immutability of the blockchain; the transparency that is obtained from a network of nodes governed in a distributed manner; and the cost of keeping the network operational. However, the price also depends on the economic ecosystem surrounding a cryptocurrency. Therefore, factors such as visibility in social networks and the use given to a cryptocurrency are strongly related to its market capitalization. In addition, through this study it has been found that the illegal activities contracted with cryptocurrencies are not only related to money laundering: procurement of illicit services such as distributed denial of service attacks; malware

binaries; botnets; and the purchase of illegal products including weapons, drugs, and falsified or stolen documents.

By answering Q3, it has been found that the most effective way to tackle the challenges posed by crypto and DLTs is by applying a sandbox of a mix of soft laws and hard laws to the legal framework of a country. This way it is possible to regulate the activities carried out, protecting investors and impeding crimes like laundering fraud, while allowing innovation in the area. Which could lead to a potential replacement of the current financial system.

**Acknowledgements.** The research of Yeray Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and co-funded by Banco Santander. This research was also partially supported by the project “Technological Consortium TO develop sustainability of underwater Cultural heritage (TECTONIC)”. Authors declare no conflicts of interest.

## References

1. Alzahrani, S., Daim, T.U.: Evaluation of the cryptocurrency adoption decision using hierarchical decision modeling (HDM). In: 2019 Portland International Conference on Management of Engineering and Technology (PICMET), pp. 1–7. IEEE (2019)
2. Barn, B., Barat, S., Clark, T.: Conducting systematic literature reviews and systematic mapping studies. In: Proceedings of the 10th Innovations in Software Engineering Conference, pp. 212–213 (2017)
3. Barone, R., Masciandaro, D.: Cryptocurrency or usury? Crime and alternative money laundering techniques. *Eur. J. Law Econ.* **47**(2), 233–254 (2019)
4. Bortnikov, S.: The state sovereignty in questions of issue of cryptocurrency. In: International Scientific Conference Digital Transformation of the Economy: Challenges, Trends, New Opportunities, pp. 564–573. Springer, Berlin (2019)
5. Buocz, T., Ehrke-Rabel, T., Hödl, E., Eisenberger, I.: Bitcoin and the GDPR: allocating responsibility in distributed networks. *Comput. Law Secur. Rev.* **35**(2), 182–198 (2019)
6. Casado-Vara, R., Novais, P., Gil, A.B., Prieto, J., Corchado, J.M.: Distributed continuous-time fault estimation control for multiple devices in IoT networks. *IEEE Access* **7**, 11972–11984 (2019)
7. Castellanos-Garzón, J.A., Mezquita Martín, Y., José Luis Jaimes, S., López, S.M.: A data mining approach applied to wireless sensor networks in greenhouses. In: International Symposium on Distributed Computing and Artificial Intelligence, pp. 431–436. Springer, Berlin (2018)
8. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al.: Blockchain technology: beyond bitcoin. *Appl. Innov.* **2**(6–10), 71 (2016)
9. Deng, H., Huang, R.H., Wu, Q.: The regulation of initial coin offerings in China: problems, prognoses and prospects. *Eur. Bus. Organ. Law Rev.* **19**(3), 465–502 (2018)
10. Dilek, S.: Cryptocurrencies in the digital era: the role of technological trust and its international effects. In: Blockchain Economics and Financial Market Innovation, pp. 453–474. Springer, Berlin (2019)
11. Earle, T.C.: Trust, confidence, and the 2008 global financial crisis. *Risk Anal. Int. J.* **29**(6), 785–792 (2009)



12. Eisenberger, I.: Innovation im recht (2016)
13. Eyal, I.: Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer* **50**(9), 38–49 (2017)
14. Fatima, N.: Enhancing performance of a deep neural network by comparing optimizers experimentally. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J. Salamanca* **9**(2), 79–90 (2020). ISSN: 2255-2863
15. Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N.: A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **126**, 45–58 (2019)
16. Giechaskiel, I., Cremers, C., Rasmussen, K.B.: When the crypto in cryptocurrencies breaks: bitcoin security under broken primitives. *IEEE Secur. Priv.* **16**(4), 46–56 (2018)
17. González-Briones, A., Castellanos-Garzón, J.A., Mezquita Martín, Y., Prieto, J., Corchado, J.M.: A framework for knowledge discovery from wireless sensor networks in rural environments: a crop irrigation systems case study. *Wirel. Commun. Mobile Comput.* **2018** (2018)
18. Gros, D., Roth, F.: The financial crisis and citizen trust in the European central bank. *CEPs working document* (334) (2010)
19. Gupta, S., Meena, J., Gupta, O., et al.: Neural network based epileptic EEG detection and classification (2020)
20. Haffke, L., Fromberger, M., Zimmermann, P.: Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML directive (EU) and how to address them. *J. Bank. Regul.* 1–14 (2019)
21. Hawlitschek, F., Notheisen, B., Teubner, T.: The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.* **29**, 50–63 (2018)
22. Hussain, A., Hussain, T., Ali, I., Khan, M.R., et al.: Impact of sparse and dense deployment of nodes under different propagation models in manets (2020)
23. Johnson, B., Laszka, A., Grossklags, J., Moore, T.: Economic analyses of security investments on cryptocurrency exchanges. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1253–1262. IEEE (2018)
24. Kamps, J., Kleinberg, B.: To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Sci.* **7**(1), 1–18 (2018). <https://doi.org/10.1186/s40163-018-0093-5>
25. Lazarenko, A., Avdoshin, S.: Financial risks of the blockchain industry: a survey of cyberattacks. In: *Proceedings of the Future Technologies Conference*, pp. 368–384. Springer, Berlin (2018)
26. Li, T., Chen, H., Sun, S., Corchado, J.M.: Joint smoothing and tracking based on continuous-time target trajectory function fitting. *IEEE Trans. Autom. Sci. Eng.* **16**(3), 1476–1483 (2018)
27. Li, T., Corchado, J.M., Sun, S.: Partial consensus and conservative fusion of Gaussian mixtures for distributed PHD fusion. *IEEE Trans. Aerosp. Electron. Syst.* **55**(5), 2150–2163 (2018)
28. Li, Y., Susilo, W., Yang, G., Yu, Y., Du, X., Liu, D., Guizani, N.: Toward privacy and regulation in blockchain-based cryptocurrencies. *IEEE Netw.* **33**(5), 111–117 (2019)
29. López, A.B.: Deep learning in biometrics: a survey. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.* **8**(4), 19–32 (2019)
30. Marella, V., Upreti, B., Merikivi, J., Tuunainen, V.K.: Understanding the creation of trust in cryptocurrencies: the case of bitcoin. *Electron. Markets* 1–13 (2020)

31. Martín, Y.M., Parra, J., Pérez, E., Prieto, J., Corchado, J.M.: Blockchain-based systems in land registry, a survey of their use and economic implications. *CISIS* **2020**, 13–22 (2020)
32. Mehar, M.I., Shier, C.L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H.M., Laskowski, M.: Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack. *J. Cases Inf. Technol. (JCIT)* **21**(1), 19–32 (2019)
33. Mezquita, Y., Alonso, R.S., Casado-Vara, R., Prieto, J., Corchado, J.M.: A review of k-NN algorithm based on classical and quantum machine learning. In: *International Symposium on Distributed Computing and Artificial Intelligence*, pp. 189–198. Springer, Berlin (2020)
34. Mezquita, Y., Casado-Vara, R., González Briones, A., Prieto, J., Corchado, J.M.: Blockchain-based architecture for the control of logistics activities: pharmaceutical utilities case study. *Logic J. IGPL* **29**(6), 974–985 (2021)
35. Mezquita, Y., Gil-González, A.B., Prieto, J., Corchado, J.M.: Cryptocurrencies and price prediction: a survey. In: *International Congress on Blockchain and Applications*, pp. 339–346. Springer, Berlin (2021)
36. Mezquita, Y., Gil-González, A.B., Martíndel Rey, A., Prieto, J., Corchado, J.M.: Towards a blockchain-based peer-to-peer energy marketplace. *Energies* **15**(9), 3046 (2022)
37. Mezquita, Y., González-Briones, A., Casado-Vara, R., Chamoso, P., Prieto, J., Corchado, J.M.: Blockchain-based architecture: a mas proposal for efficient agri-food supply chains. In: *International Symposium on Ambient Intelligence*, pp. 89–96. Springer, Berlin (2019)
38. Mezquita, Y., González-Briones, A., Casado-Vara, R., Wolf, P., Prieta, F.D.L., Gil-González, A.B.: Review of privacy preservation with blockchain technology in the context of smart cities. In: *Sustainable Smart Cities and Territories International Conference*, pp. 68–77. Springer, Berlin (2021)
39. Mezquita, Y., Parra, J., Perez, E., Prieto, J., Corchado, J.M.: Blockchain-based systems in land registry, a survey of their use and economic implications. In: *Computational Intelligence in Security for Information Systems Conference*, pp. 13–22. Springer, Berlin (2019)
40. Mezquita, Y., Valdeolmillos, D., González-Briones, A., Prieto, J., Corchado, J.M.: Legal aspects and emerging risks in the use of smart contracts based on blockchain. In: *International Conference on Knowledge Management in Organizations*, pp. 525–535. Springer, Berlin (2019)
41. Nakamoto, S., et al.: Bitcoin: a peer-to-peer electronic cash system (2008)
42. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. In: *12th International Conference on Evaluation and Assessment in Software Engineering (EASE)*, vol. 12, pp. 1–10 (2008)
43. Pimpalkar, A.P., Raj, R.J.R.: Influence of pre-processing strategies on the performance of ml classifiers exploiting TF-IDF and bow features. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.* **9**(2), 49 (2020)
44. Saad, M., Choi, J., Nyang, D., Kim, J., Mohaisen, A.: Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions. *IEEE Syst. J.* **14**(1), 321–332 (2019)
45. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: decentralized anonymous payments from bitcoin. In: *2014 IEEE Symposium on Security and Privacy*, pp. 459–474. IEEE (2014)
46. Scholl, H.J., Bolívar, M.P.R.: Regulation as both enabler of technology use and global competitive tool: the Gibraltar case. *Gov. Inf. Q.* **36**(3), 601–613 (2019)

47. Tjio, H., Hu, Y.: Collective investment: land, crypto and coin schemes: regulatory ‘property’. *Eur. Bus. Organ. Law Rev.* 1–28 (2020)
48. Todorof, M.: Fintech on the dark web: the rise of cryptos. In: *Era Forum*, vol. 20, pp. 1–20. Springer, Berlin (2019)
49. Valdeolmillos, D., Mezquita, Y., González-Briones, A., Prieto, J., Corchado, J.M.: Blockchain technology: a review of the current challenges of cryptocurrency. In: *International Congress on Blockchain and Applications*, pp. 153–160. Springer, Berlin (2019)
50. Van Hout, M.C., Hearne, E.: New psychoactive substances (NPS) on cryptomarket fora: an exploratory study of characteristics of forum activity between NPS buyers and vendors. *Int. J. Drug Policy* **40**, 102–110 (2017)
51. Vergara, D., Extremera, J., Rubio, M.P., Dávila, L.P.: The proliferation of virtual laboratories in educational fields. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.* **9**(1), 85 (2020)
52. Weaver, N.: Risks of cryptocurrencies. *Commun. ACM* **61**(6), 20–24 (2018)
53. Wilson, C.: Cryptocurrencies: the future of finance? In: *Contemporary Issues in International Political Economy*, pp. 359–394. Springer, Berlin (2019)
54. Zetzsche, D.A., Buckley, R.P., Barberis, J.N., Arner, D.W.: Regulating a revolution: from regulatory sandboxes to smart regulation. *Fordham J. Corp. Fin. L.* **23**, 31 (2017)
55. Zubair, S., Al Sabri, M.A.: Hybrid measurement of the similarity value based on a genetic algorithm to improve prediction in a collaborative filtering recommendation system. *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.* **10**(2), 165–182 (2021)