Blockchain security research: theorizing through bibliographic-coupling analysis

Article *in* Journal of Advances in Management Research · August 2020

DOI: 10.1108/JAMR-04-2020-0051

2 authors:

Lurdes Patrício
Universidade da Beira Interior
5 PUBLICATIONS **18** CITATIONS
SEE PROFILE

João J. M. Ferreira
Universidade da Beira Interior
434 PUBLICATIONS **8,390** CITATIONS
SEE PROFILE

Blockchain security research: theorizing through bibliographic-coupling analysis

Lurdes D. Patrício and João J. Ferreira
Faculdade de Ciências Sociais e Humanas and NECE – Research Unit in Business Sciences, Universidade da Beira Interior, Covilha, Portugal

Received 7 April 2020
Revised 14 July 2020
Accepted 16 July 2020

Abstract

Purpose – The continuous presence and intensity of the Internet of things (IoT) in our lives and the risk of security breaches in traditional transactional and financial platforms are the major cause of personal and organizational data losses. Blockchain emerges as a promised technology to ensure higher levels of data encryption and security. Thus, this study aims to develop a systematic literature review analyzing the previous literature and to purpose of a framework to better understand the process of blockchain security.

Design/methodology/approach – The 75 articles reviewed were obtained through the Scopus database and a bibliographic-coupling analysis was developed to identify the main themes of this research area, via VOSviewer software.

Findings – The results enable the categorization of the existing literature revealing four clusters: 1) feasibility, 2) fintech and cryptocurrency, 3) data trust and share and 4) applicability. Blockchain technology is still in its early stage of development and counting on researchers in security and cryptography to take it further to new highs, to allow its applicability to different areas and in long-term scenarios.

Originality/value – This systematic literature creates a base to reduce the blockchain security literature gap. In addition, it provides a framework that enables the scientific community to access the main subjects discussed and the articulation between concepts. Furthermore, it enhances the state-of-the-art literature on blockchain security and proposes a future research agenda.

Keywords Systematic literature review, Blockchain, Blockchain technology, Security, Blockchain security, Bibliographic-coupling analysis

Paper type Literature review

1. Introduction

The Internet of things (IoT) is growing at an exponential rate and thus generating still unexplored privacy and security areas. There are estimates that 2020 shall see more "things" than people on Earth and with security problems becoming a still greater concern for IoT networks as humans simply cannot control the large amount of data available while ensuring its security and integrity (Ghadekar *et al.*, 2019). The security breaches in traditional transactional and financial platforms represent the major cause of personal and organizational data losses (Taleb, 2019). In turn, blockchain technology has recently evolved into applications serving as a means of security in peer-to-peer (P2P) networks (Ghadekar *et al.*, 2019). Due to the importance of privacy and the integrity of data, the deployment of blockchain now extends to ensuring the security of cloud environments, systems highly prone to malicious attacks that may compromise data, (Veena *et al.*, 2019). Blockchain differs from other technologies which secure transactions by centralized databases. Instead, blockchain technology decentralizes data transactions into different nodes. The information in all the nodes then forms a block with all these transaction blocks interlinked and with no scope for deleting the information held in those blocks. Whenever

This work is financed by national funds through FCT - Fundação para a Ciência e a Tecnologia, I. P., under the project "UIDB/04630/2020".

Journal of Advances in Management Research
© Emerald Publishing Limited
0972-7981
DOI 10.1108/JAMR-04-2020-0051

there are attempts to delete the block, the information is in any case available in another block. Another difference to traditional approaches stems from the access that differs between customers and users. Due to these security features, there are many trading firms, insurance companies, hospitals and other organizations shifting their focus to blockchain technology on the expectation that blockchain ensures IoT reliability, scalability, reusability and responsibility (Venkateswara *et al.*, 2018).

Blockchain technology remains at an early stage of its development and requiring security and cryptography researchers to further deepen the progress thus far made. The expectations are for blockchain to ensure the reliability, scalability, reusability and responsibility of the IoT (Kumar *et al.*, 2019a, b). The IoT is itself now a popular field of research. Due to the sheer importance and extent of computerization and smart objects, certain security issues have emerged related to the gathering of private information, uncertain interfaces and unencrypted communications. According to Bathula and Basha (2019), the most common attacks are (1) port sweep assaults that do not damage the framework or server but rather find dynamic ports to render the machine vulnerable; (2) man-in-the-middle (MITM) assaults in which the aggressor discovers a correspondence between two gatherings with the respective participants believing they are having a private discussion even while the assailant oversees all their correspondence; (3) refusal of service assaults that shut down machines/ applications/ networks for a period of time; (4) conveyed denial of service assaults in which the assailant identifies weaknesses in the framework, normally through malware and then takes control of it; (5) sniffing assaults that commonly target wired remote networks to allow their perpetrators to acquire, gather and adjust data and (6) crypto graphical assaults normally involving key disclosure. In this context, the blockchain technology emerges with great expectations in terms of enhancing security and privacy. Nevertheless, blockchain features remain unsuitable for the majority of IoT gadgets (Bathula and Basha, 2019).

According to Lemieux (2016), the trustworthiness of records arises from the capacity to establish their reliability and authenticity. From the outset, reliability stems from record creation, who does this and how. The current standards for record management are defined by the International Organization for Standardization (ISO). In turn, authenticity encapsulates both the creation and maintenance of the identity and integrity of records both before and after their creation.

Umarovich *et al.* (2017) sustain that due to the dynamics of the digital economy and the increasing integration of information and financial technologies, financial markets are especially sensitive to financial and technological (fintech) innovations that drive increases in transaction speeds, changes in financial contracts and better cost management.

Figure 1 details and analyses just how the blockchain technology works.

The applicability of blockchain directly interconnects with the development of smart contracts (Umarovich *et al.*, 2017), thus the computerized transaction protocols which execute the terms of a contract (Giancaspro, 2017). Recourse to smart contracts encourages, confirms and authorizes execution of an understanding or exchange between at least two parties (Kanimozhi and Akila, 2019), enabling the mechanization of certain, advanced and executable procedures among the participant parties (Poluri *et al.*, 2019).

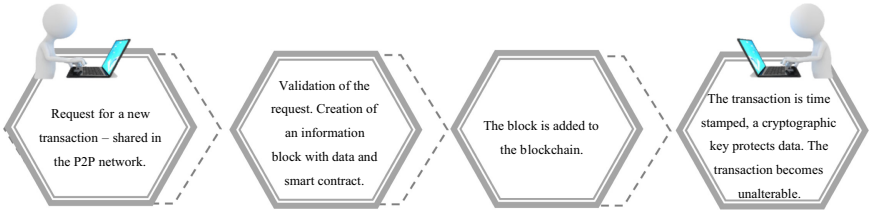

Figure 1.
How blockchain works in peer-to-peer networks, adapted from Cole *et al.* (2019)

Umarovich *et al.* (2017) state that the changes in contract speeds shape the effective evaluation parameters prevailing in the real economic sector and influence the dynamics of investments due to shifts in investor expectations and requirements. According to Hoxha and Sadiku (2019), smart contracts enable the elimination of the need for third parties thereby bringing about reductions in transactions cost due to the removal of intermediaries and greater process speed and efficiency. The major focus becomes the effectiveness of the system in ensuring economic security to all entities, especially business firms, considering their responsibilities for maintaining harmony and stability in investment and financial markets (Umarovich *et al.*, 2017).

With the objective of identifying clusters in the literature and presenting a future research agenda, we approached the new trends in research on industry 4.0 and, as a result, were able to identify a gap in the findings on blockchain (Xu *et al.*, 2018), specifically in the relationship between blockchain technology and its security aspects (Hoxha and Sadiku, 2019). To address this existing gap, the purpose of this research is to analyze the articles existing on blockchain and security, systematizing the existing studies and addressing the need for a systematic literature review that approaches both concepts simultaneously. A search of the Scopus database returned the 75 articles reviewed in accordance with bibliographic-coupling analysis made by the VOSviewer software. This software brought about the identification of clusters containing 47 of the 75 documents included. This analysis classifies documents as bibliographic coupled whenever approaching the same item of reference (Kessler, 1963). We adopted a search protocol to ensure a systematic approach and with the results revealing four clusters, specific ç, (1) feasibility, (2) fintech and cryptocurrency, (3) data trust and sharing and (4) applicability, as well as underpinning the development of a framework to systematize the relationships between these clusters.

This article contains the following structure: Section 2 presents a literature review emphasizing the major themes emerging from this systematic literature review, Section 3 describes the research method, Section 4 sets out the VOSviewer software results and systematizes the core concepts of the clusters before Section 5 puts forward the conclusions, implications and future research agenda.

2. Method

This paper carried out a systematic literature review characterized by applying an objective and rigorous research protocol within the scope of minimizing researcher bias (Tranfield *et al.*, 2003) . As the purpose of this study involves identifying clusters in the literature and presenting a future research agenda, we opted to apply the Tranfield *et al.* (2003) methodology. Figure 2 displays the research protocol complemented by Table 1 that presents the article inclusion and exclusion criteria.

This study aims to systematize the literature, identify research paths and present the emerging aspects interrelated with blockchain security. The Scopus database selection corresponded to its scope and relevance in the management field. The search of the database made recourse to the keywords blockchain and security. The research was refined by specifying the business, management and accounting areas, only English language works and with articles as the exclusive document type. The search took place on November 15th 2019 and returned 75 articles.

This research project applied version 1.6.13 of the VOSviewer software to generate the bibliometric maps and identify the bibliographic coupling in the document references. Kessler (1963) describes the bibliographic-coupling method in which two documents classify as bibliographic coupled whenever using the same item of reference.

Figure 2 provides details on the search protocol.

3. Results

3.1 Descriptive data

Figure 3 portrays the annual trends in the number of publications and citations for the 75 articles published between 2016 and 2019. Analyzing the number of publications, the first

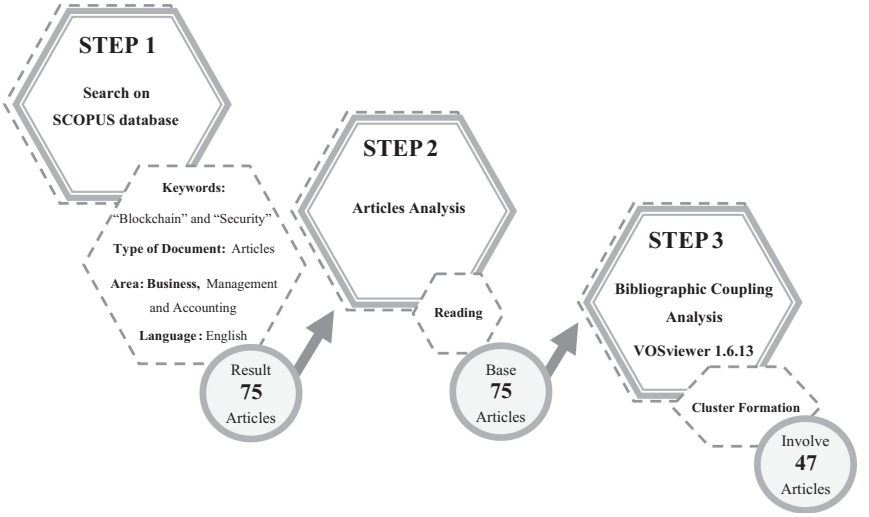

Figure 2.
Search protocol

Inclusion Criteria	*Exclusion Criteria*
• Published in the period: before 15th November 2019 • Present in Scopus database • Included in business, management and accounting subject areas • Peer-reviewed scientific articles published in English • Referring explicitly to blockchain security in the title, abstract or keywords	• The Scopus database search excluded books, book chapters, conference reviews, conference papers, notes, letters, editorials, notes and erratum • The VOSviewer software bibliographic coupling, with a full counting of the document under analysis, set a minimum number of one document citation and a minimum cluster size of 5 authors

Table 1.
Criteria for SLR inclusion and exclusion of publications

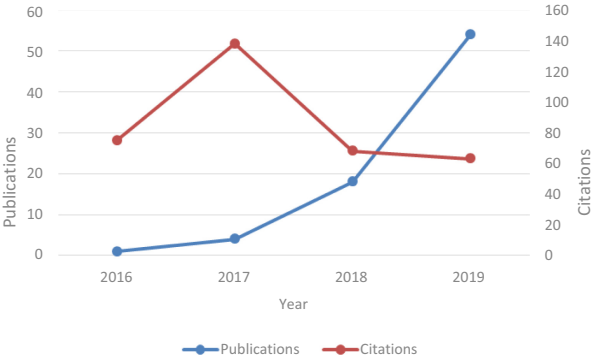

Figure 3.
Total publications and citations by year

article underwent publication in 2016 and with the number of articles published since increasing to peak in 2019 with the publication of 48 articles. Hence, this field is very recent with every article coming out within the last four years. The total of citations reached its maximum in 2017 with 138 incidences.

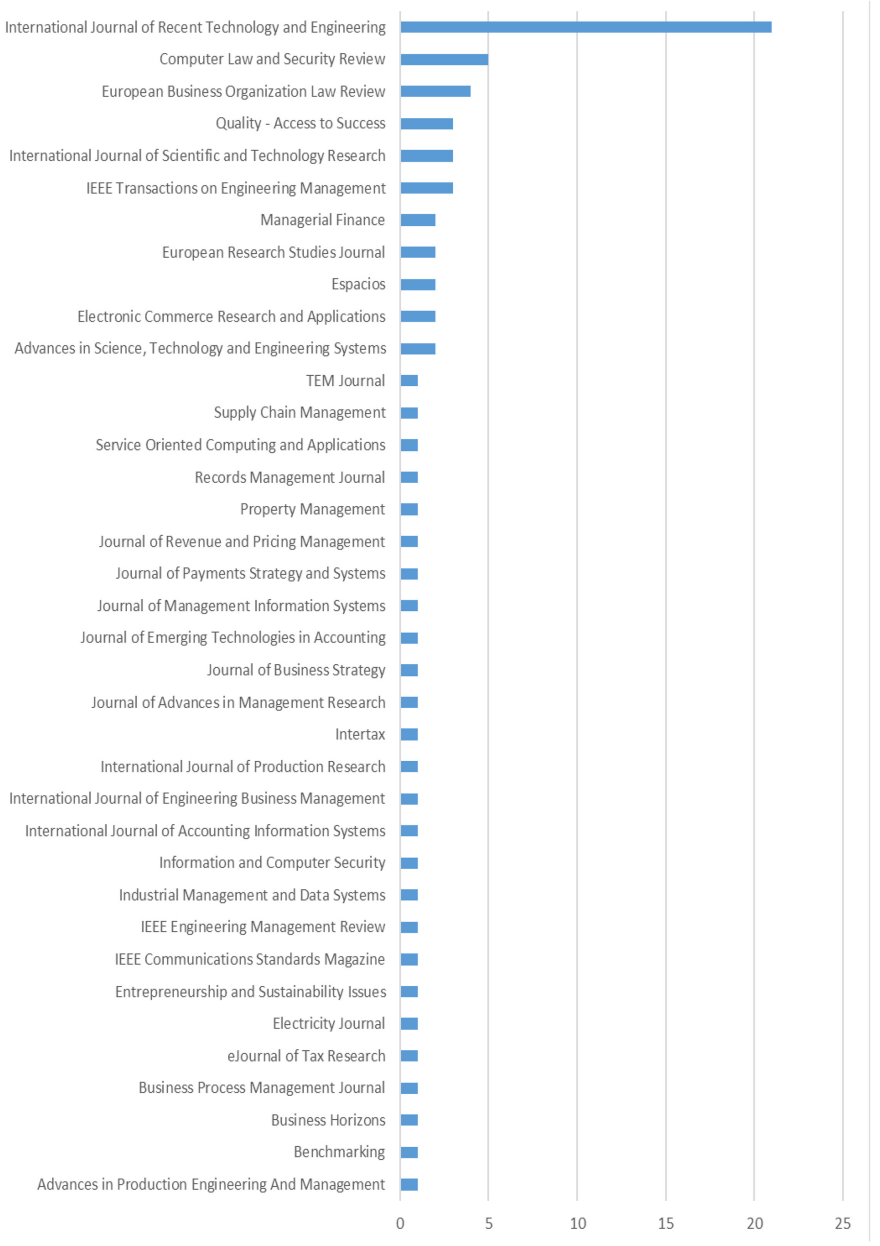

Figure 4.
Number of articles published

Article	Authors | year	Journal	Citations	Methodology
Trusting records: is blockchain technology the answer?	Lemieux (2016)	Records Management Journal	75	*Qualitative* Using requirements and digital preservations standards as a general evaluative framework for risk based in land register
Blockchain technology and its relationships to sustainable supply chain management	Saberi *et al.* (2019)	International Journal of Production Research	43	*Qualitative* Literature review to address blockchain barriers
Toward open manufacturing; a cross-enterprises knowledge and services exchange framework based on blockchain and edge computing	Li *et al.* (2018)	Managerial Finance	39	*Qualitative* Literature review based on the development of the emerging open manufacturing
Is a "smart contract" really a smart idea? Insights from a legal perspective	Giancaspro (2017)	Computer Law and Security Review	29	*Qualitative* Literature review to address potential issues with legal and practical implications in the use of smart contracts
Can blockchains serve an accounting purpose?	Coyne and McMickle (2017)	Journal of Emerging Technologies in Accounting	16	*Qualitative* Analyze, in context of the Byzantine generals problem, if blockchain could become a more secure alternative to current accounting ledgers
Blockchain and financial controlling in the system of technological provision of large corporations' economic security	Umarovich *et al.* (2017)	European Research Studies Journal	14	*Qualitative* Analyze the advantages and risks of the blockchain technology on the different levels of the economic system
Blockchain technology for providing an architecture model of decentralized personal health information	Rahmadika and Rhee (2018)	International Journal of Engineering Business Management	8	*Mixed* Address blockchain technology and several protocols embedded using data from health-care providers to propose an architectural model to manage personal health information
Blockchain and law: Incompatible codes?	Millard (2018)	Computer Law and Security Review	7	*Qualitative* Literature review analyzing the context of wider historical debates about new technologies versus law

Table 2.
Top ten most cited articles

(*continued*)

Of the 75 articles researched, 47 (62.67%) do not contain any citations and only 6 (8%) have ten or more citations.

The 75 articles received their publication in 37 different journals with the titles of these journals and the number of the articles published available in Figure 4.

Table 2 briefly presents the top ten most cited articles.

Article	Authors | year	Journal	Citations	Methodology
Blockchain technology, supply chain information and strategic product deletion management	Zhu and Kouhizadeh (2019)	IEEE Engineering Management Review	4	*Qualitative* Literature review on decision making processes of product deletion, rationalization or discontinuation using blockchain technology
Blockchain based DNS and PKI solutions	Karaarslan and Adiguzel (2018)	IEEE Communications Standards Magazine	4	*Qualitative* Analyze security and trust problems in the implementation of domain name systems and certificate authority systems and the possibility to use blockchain-based decentralized solutions

Table 2.

Cluster 1: $N = 17$	Cluster 2: $N = 13$	Cluster 3: $N = 9$	Cluster 4: $N = 8$
Bathula and Basha (2019)	Anand and Tanguturi (2019)	Hoxha and Sadiku (2019)	Coyne and McMickle (2017)
Dhagarra *et al.* (2019)	Cole *et al.* (2019)	Lemieux (2016)	Ferrer-Gomila *et al.* (2019)
Fu *et al.* (2019)	Deng *et al.* (2018)	Kumar *et al.* (2019a, b)	Mathew *et al.* (2019)
Gupta and Jose (2019)	Dimitropoulou *et al.* (2018)	Poluri *et al.* (2019)	McCallig *et al.* (2019)
Karaarslan and Adiguzel (2018)	Ghadekar *et al.* (2019)	Sehra *et al.* (2018)	Rindaşu (2019)
Limba *et al.* (2019)	Hu *et al.* (2019)	Van der Elst and Lafarre (2019)	Saberi *et al.* (2019)
Monika *et al.* (2019)	Lee (2019)	Li *et al.* (2018)	Smith and Dhillon (2019)
Kumar *et al.* (2019a, b)	Milian *et al.* (2019)	Li *et al.* (2019)	Yin *et al.* (2019)
Prabhakaran and Asha (2019)	Mohanta *et al.* (2019)	Zhu and Kouhizadeh (2019)	
Prasad *et al.* (2018)	Pramothini *et al.* (2018)		
Samsudeen *et al.* (2019)	Rahmadika and Rhee (2018)		
Scuderi *et al.* (2019)	Rane and Narvel (2019)		
Subramanian (2019)	Sushmetha and Vairamuthu (2019)		
Taleb (2019)			
Umarovich *et al.* (2017)			
Venkateswara *et al.* (2018)			
Vovchenko *et al.* (2018)			

Table 3.
Typology of clusters

The top ten most cited articles all feature qualitative studies, common when the literature base still remains very narrow. The topics approached are blockchain security in the supply chain (Saberi *et al.*, 2019; Zhu and Kouhizadeh, 2019), its applications to diverse areas such as accounting, finance and healthcare (Umarovich *et al.*, 2017; Coyne and McMickle, 2017; Rahmadika and Rhee, 2018), smart contracts and law (Giancaspro, 2017; Millard, 2018), blockchain trust (Lemieux, 2016) and domain name system (DNS) and public key infrastructures (PKIs) for connecting to a network service (Karaarslan and Adiguzel, 2018).

3.2 Bibliographic coupling of documents: main themes

To identify the trends in the literature on blockchain and security, we carried out the bibliographic coupling of document references, which resulted in the definition of four clusters accounting for forty-seven of these articles. Table 3 presents the cluster constitution.

We analyzed and named these clusters as (1) feasibility, (2) fintech and cryptocurrency, (3) data trust and sharing and (4) applicability.

Figure 5 conveys the visualization of the cluster network.

3.2.1 Cluster 1: feasibility. Seventeen studies contribute to understanding feasibility (Table 4).

Bathula and Basha (2019) approach the IoT as a popular research field. As regards computerization and smart objects, they identify several IoT related security issues, such as private information gathering, uncertain interfaces and unencrypted communications. In this context, blockchain appears with high expectations in terms of promoting security and privacy. However, certain features prevent the incorporation of blockchains into the majority of IoT gadgets because they are both computationally costly and involve high data transfer capacities. These issues emerge as crucial to healthcare service delivery, especially for addressing disparities in access to healthcare, particularly for the poor and disadvantaged. Dhagarra *et al.* (2019) propose an integrative healthcare framework anchored in big data and blockchain to provide timely and appropriate healthcare services for every citizen. The model allows for the secure, immutable and comprehensive access to medical records across every existing treatment center.

Fu *et al.* (2019) design the Bead Strand Model, a self-destructing mechanism that ensures users the capacity of defining what data would vanish on the expiry date. With the user in control of privacy and security, the model becomes more humanized and more acceptable than blockchain.

According to Gupta and Jose (2019), technology has touched our lives in every possible field with significant benefits in terms of time, money and human power. The Indian Police represents no exception and, following the "Digital India" campaign, they replaced the

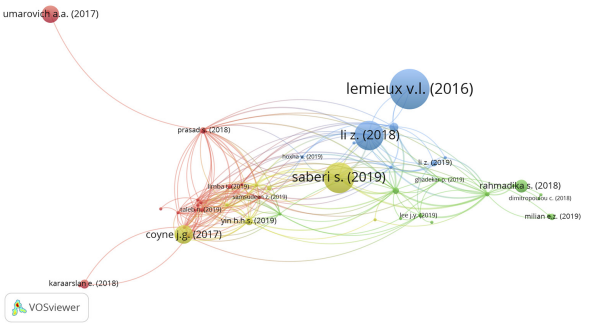

Figure 5.
Clusters network

Authors	Article	Objective	Methodology	Main findings
Bathula and Basha (2019)	Blockchain Technology with Internet of Things in the Real time Network Stream	Propose a Blockchain–based network for Internet of Things (IoT) maintaining a large portion of its security and privacy benefits	Qualitative	The research accomplished a Blockchain–based network for the internet of Things and found key data to blend IoT and Blockchain technology. Blockchain emerge as the best answer to the requirement for faster development of smart associated devices that search for a protected and dependable condition for information store
Dhagarra *et al.* (2019)	Big Data and blockchain supported conceptual model for enhanced healthcare coverage The Indian context	Present a framework to address disparities across gender, geography and socioeconomic status in access to healthcare service delivery using as key component the Big Data analytics-based framework that relays on a unique identification number (UID) system as formalized and implemented by the Government of India for identification of the patients and their cases	Qualitative	The authors presented a framework that provides easy access to secure, immutable and comprehensive medical records of patients across all treatment centers across India. The model ensures security and privacy of the medical records based on the incorporation of biometric authentication by the patients for access of their records to healthcare providers serving the pertinent stakeholders, from patients to healthcare services providers

(*continued*)

Table 4.
Authors in cluster 1: feasibility

Authors	Article	Objective	Methodology	Main findings
Fu *et al.* (2019)	Bead Strand Model: a high-efficiency storage structure for self-destructing data in cloud environment	Design a storage structure with a self-destructing mechanism that can provide high-efficiency concurrency to Blockchain, providing security to all the users and all types of data	Mixed Test of a Prototype system of Bead Strand ModelonJ2EE platform	Based on a user set option, named Bead Strand Model, the data would vanish after expiration. The humanization of the mechanism makes it more acceptable, by the people who are concerned with privacy and security in cloud environments, than Blockchain
Gupta and Jose (2019)	A Method to Secure FIR System using Blockchain	In a digitalization era, Indian Police Department replaced the manual system with a centralized online process to register the complaint. It is necessary to address the security using Blockchain technology	Qualitative	It is possible to provide a method to secure the First Investigation Reports (FIR) system using Blockchain technology and protect it from malfeasance
Karaarslan and Adiguzel (2018)	Blockchain Based DNS and PKI Solutions	Explain how a domain name system (DNS)s work and its principal security challenges and how Blockchain-based DNS are classified, what are the feasibility advantages. They questioned the possibility of a decentralized Internet	Qualitative	The paper explains how Blockchain works and present its strengths and how to use it to address DNS security challenges. Blockchain-based DNS solutions are classified and described according to their service, presenting its advantages and feasibility

Table 4. (*continued*)

Authors	Article	Objective	Methodology	Main findings
Limba *et al.* (2019)	Cryptocurrency as disruptive technology: Theoretical insights	Address the portencial disruptive power of criptocurrency in the financial sector, retail market or on global monetary policy	Qualitative	The combination of disruptive technologies with Internet, Mobile Internet and IoT is changing the world. Society gained comfort for a cheaper price but, on the other hand, many people lost their jobs. Based on this social and legal context definitions and principles are systematized, practical application tendencies are identified
Monika *et al.* (2019)	Beneficial P2P Storage Scheme with Privacy Protection	Approach purchaser's safety based on Blockchain technology applied to Peer-to-Peer networks	Qualitative	It is possible to reduce correspondence fee and make certain the purchasers protection within the P2P stockpiling plan and Blockchain
Kumar *et al.* (2019a, b)	A Secure Transaction Authentication Scheme using Blockchain based on IOT	Provide an overview of Blockchain architecture and compare some typical consensus algorithms used in different Blockchains	Qualitative	The authors sustain that Blockchain could be customized and tailored to fit multiple cases. They specifically analyzed banking transaction via IOT and various applications and proposed validating transactional information for secure transaction and authentication scheme for IoT. They also list technical challenges, recent advances and future trends for Blockchain

(*continued*)

Table 4.

Authors	Article	Objective	Methodology	Main findings
Prabhakaran and Asha (2019)	Enhancing Cyber Security in Power Sector Systems using Block chain	Address power plants threats (e.g. injection denial of service, phishing and Malware) and providing a method to protect data storage	Qualitative	The authors propose a secure and trustworthy method to protect power plant in which data is stored in Blockchain
Prasad *et al.* (2018)	A TISM modeling of critical success factors of blockchain based cloud services	Identify and analyze critical success factors that can facilitate success of Blockchain-based cloud services	Qualitative	Based on literature review and expert opinions emerged a hierarchical framework that identifies 19 critical success factors and how they are inter dependent
Samsudeen *et al.* (2019)	Behavioral Analysis of Bitcoin Users on Illegal Transactions	Address the problem of interconnected illegal transactions and identified behavioral patterns and significant facts among illegal incidents relaying on Bitcoin Blockchain process to overcome them	Qualitative	The paper identifies common patterns to obtain an evaluation based on previous findings allowing the recognition of common spending patterns and popular exchanges

Table 4. (*continued*)

manual criminal record system with a centralized online process that deployed blockchain to protect the system from malfeasance.

Karaarslan and Adiguzel (2018) approach the violation of neutrality, censorship and privacy problems that menace Internet freedom and usability and capable of disrupting online services. The solutions for this might lie in decentralized blockchain technologies.

According to Monika *et al.* (2019), ever since the advent of web cloud storage (WCS), businesses have been unable to assure purchaser data security through P2P data collects without complex server techniques. Through blockchain, it would be feasible to properly secure client records.

In turn, Kumar *et al.* (2019a, b) state that blockchain technology still remains at an early stage of development, counting on researchers in security and cryptography to further advance and deepen this field. They therefore expect blockchain to develop and ensure the reliability, scalability, reusability and responsibility of the IoT.

Prabhakaran and Asha (2019) maintain that data storage in blockchains rather than distributed blocks provides a more secure and trustworthy method of overcoming threats to data privacy.

After analysis of the critical factors for success in blockchain-based services, Prasad *et al.* (2018) identify 19 critical factors, specifically; (1) user engagement, (2) industry collaboration, (3) rich ecosystem, (4) blockchain technology standardization, (5)regulatory clarity, (6) cost efficiency, (7) energy efficiency–wasted resources, (8) handling blockchain bloat, (9) miner

Authors	Article	Objective	Methodology	Main findings
Scuderi *et al.* (2019)	The Supply Chain Value of POD and PGI Food Products Through the Application of Blockchain	Approach the Blockchain Partnership Initiative in order to reduce information asymmetry, reducing the distance between producers and consumers	Qualitative	The research allows the reorganization of Blockchain system of an organization of the supply chain of POD and PGI quality food products. The use of the Blockchain in the agri-food has vantages for supply chain, allowing the consumers to verify the origin of the raw material and obtain information on the production (e.g. packaging operations, distribution). There is always the risk of fraudulent information insertion, representing a weakness very difficult to verify. However, Blockchain emerged as a shared certified tool of control and valorization that protects manufacturers, packers, traders and the final consumer
Subramanian (2019)	Security tokens: architecture, smart contract applications and illustrations using SAFE	Describe the security token architecture as an application of smart contracts and analyze the implementation and design of an instrument, Simple Agreement for Future Equity (SAFE) based on a security token architecture and smart contracts	Qualitative	The authors concluded that there are models using relational algebra and models based on utility maximization. Reducing information asymmetry between the investors and SAFE users is positive if smart contract-based security tokens developed accordingly to each state in the SAFE contract

(*continued*)

Table 4.

Authors	Article	Objective	Methodology	Main findings
Taleb (2019)	Prospective applications of blockchain and bitcoin cryptocurrency technology	Literature review of Blockchain and Bitcoin technology and its future applications	Qualitative	The authors presents a systematization of Blockchain advantages and disadvantages
Umarovich *et al.* (2017)	Block Chain and Financial Controlling in the System of Technological Provision of Large Corporations' Economic Security	Research trends and priorities for the Blockchain technology use in order to ensure the economic security of large corporate entities	Qualitative	Highlights the need of institutional, legal, information and technology preparation of economic agents to the Blockchain technology implication to solve definite economic problems
Venkateswara *et al.* (2018)	Blockchain Technology–A Sturdy Protective Shield	Provide an overview of Blockchain technology	Qualitative	The paper allows the analisis of Blockchain architecture listing security and technical challenges, identifying future trends
Vovchenko *et al.* (2018)	Conceptual approach to the development of financial technologies in the context of digitalization of economic processes	Approach the lack in confidence and stability on financial institutions and instruments and the existing legal mechanisms, witch do not create the ideal framework to new financial instruments and technologies, considering emerging problems that occur with digitization of social and economic processes in the Russian economy	Qualitative	The authors concluded that the development of the digital economy, in the special case of Russia, is due to the need to ensure the information and economic security of the state and that the introduction of innovative communication and financial technologies is a way to improve the living standards and national well-being through

Table 4.

incentives, (10) the business case alignment with blockchain's capabilities, (11) sidechains development, (12) the availability of a blockchain talent pool, (13) leadership readiness for a decentralized consensus-based technology, (14) technology investment and maturity, (15) trust in blockchain networks, (16) integration with other cloud services, (17) robust and mature smart contracts platforms, (18) blockchain security and (19) user control over data privacy. These factors might allow researchers and industries to strategically focus on the specific drivers able to extract the maximum benefits from this disruptive technology.

Meanwhile, Samsudeen *et al.* (2019) describe how the features of bitcoin, namely anonymity, security and decentralization, also create opportunities for illegal and fraudulent activities with the conclusion stressing the importance of automating the process to detect illegal transactions.

Scuderi *et al.* (2019) analyzed one of the most valuable, largest and complex industries, the agri-food sector. Its complexity makes the agri-food industry an excellent candidate for blockchain-based projects especially for countering fraud and counterfeiting and to make the relationship between small farmers and big buyers fairer. This might be possible through reducing information asymmetries and ensuring greater proximity between producers and consumers. The difficulties arise in the phases of the supply chain process that are not yet subject to codification.

According to Taleb (2019), blockchain and bitcoin platform data are highly encrypted and secure and the losses in personal and organizational data stem primarily from security breaches in the transactional and financial platforms.

Umarovich *et al.* (2017) studies applications of the blockchain technology to address security and minimize the risk by large corporations operating in the digital economy. This blockchain technology carries with it new threats to economic security with the decomposition of the risks enforcing auditing and control as a proactive approach.

Meanwhile, Venkateswara *et al.* (2018) describe how the success of bitcoin provides power to blockchain technology and underpins its presence in the most different areas, particularly financial services, reputation systems and the IoT. However, its applicability still faces many technical challenges for overcoming issues related to its scalability, security, reliability, accessibility and regulation

Furthermore, Vovchenko *et al.* (2018) describe the importance in Russia of addressing the emerging problems that occur following the digitization of social and economic processes in accordance with the new economic paradigm. The lack of confidence and stability in financial institutions and their instruments and the existing legal mechanisms do not generate a framework ideal for launching new financial instruments and technologies. To develop digital economies, the state therefore needs to ensure information and economic security to achieve a greater standard of living and national well-being.

3.2.2 Cluster 2: fintech and cryptocurrency. Table 5 presents the thirteen articles contained in cluster 2, fintech and cryptocurrency.

Cole *et al.* (2019) identify a set of eight attributes in the blockchain technology (e.g. enhancing product safety and security, improving quality management, reducing illegal counterfeiting, improving sustainable supply chain management, advancing inventory management and replenishment, reducing the need for intermediaries, impacting on new product design and development and reducing the cost of supply chain transactions) that might transform operations and supply chain management. To obtain the maximum rewards from blockchain, organizations should build up their human capital expertise.

Following comparative analysis of some advanced economies (e.g. the United States, Canada, Australia, Singapore, Hong Kong, the United Kingdom and Europe), Deng *et al.* (2018) propose a regulatory framework for Initial Coin Offerings in China. This maintains how Initial Coin Offerings might class as financial securities and thus be subject to securities laws.

Dimitropoulou *et al.* (2018) consider the need for improvement in international tax dispute resolution. The European Union and the United Nations have taken measures to prevent and diminish the resolution times for tax treaty-related disputes. Surprisingly, none of those resolution proposals incorporate technology. Disruptive technologies (e.g. artificial intelligence, shared-data platforms, cloud-based solutions and blockchain) might secure and support mutual agreement procedures and accelerate resolution times, reducing costs and establishing trust between tax administrations and taxpayers.

Authors	Article	Objective	Methodology	Main findings
Anand and Tanguturi (2019)	Blockchain Based Packet Delivery Mechanism for WSN	Implementation of an algorithm for combining the Ad Hoc On-Demand Distance Vector routing protocol and particle swarm optimization to produce trustable routing in every location through Blockchain	Mixed Application of a new algorithm combining the AODV (Ad Hoc On-Demand Distance Vector) routing protocol and particle swarm optimization (PSO)	The authors analyzed the efficiency of the Ad Hoc On-Demand Distance Vector (AODV) when the nodes are interconnected by Blockchain with the particle swarm optimization (PSO), creating the base to know how the data will be secured using Blockchain in the various levels of networks using n number of nodes
Cole *et al.* (2019)	Blockchain technology: implications for operations and supply chain management	Analyze of Blockchain technology from an operations and supply chain management perspective	Qualitative	The article presents several ways in which Blockchain could transform operations and supply chain management (OSCM). To get the maximum reward it is important that managers examine their products and the supply chain to know if the Blockchain could be a benefit. Managers should have human capital expertise to exploit the technology possibilities
Deng *et al.* (2018)	The Regulation of Initial Coin Offerings in China: Problems, Prognoses and Prospects	Provide a non-exhaustive classification of the legal status of Initial Coin Offerings	Qualitative	The authors explore the difficulties in drawing a complete regulatory regime for ICOs to facilitate the development of FinTech in the ICO market and protect investors against fraudulent projects

Table 5.
Authors in cluster 2: fintech and cryptocurrency

(*continued*)

Authors	Article	Objective	Methodology	Main findings
Dimitropoulou *et al.* (2018)	Applying modern, disruptive technologies to improve the effectiveness of tax treaty dispute resolution: Part 2	Analyze the tax treaty dispute resolution process and how technologies can be used to improve the mutual agreement procedure and supplementary solutions	Qualitative	Tax treaty dispute resolution mechanisms are outdated and require substantial human and financial resources. It demands a global coordinated approach
Ghadekar *et al.* (2019)	Secure Access Control to IoT Devices using Blockchain	Propose a lightweight and secure architecture for IoT by using Ethereum Blockchain maintaining its security powers	Qualitative	The proposed architecture for IoT by using Ethereum Blockchain, being decentralized solves the single point of authentication common in IoT networks. Based on a Smart Home System case study and the considering temperature and intrusion detection the qualitative evaluation demonstrated it tackles various attacks
Hu *et al.* (2019)	A blockchain-based smart contract trading mechanism for energy power supply and demand network	Propose a trading mechanism for energy power supply and demand network (EPSDN) based on Blockchain smart contract based on the opening Chinese market	Mixed Application of efficient trading mechanism for energy power supply and demand network (EPSDN)	The proposed mechanism overcomes high cost, high risk and poor efficiency of traditional centralized electric energy trading method. Smart contracts achieve the desirable security and effectiveness and solve the problems in EPSDN
Lee (2019)	A decentralized token economy: How blockchain and cryptocurrency can revolutionize business	Analyze how Blockchain technology and cryptocurrencies are evolving and interconnected, creating a token economy through different business models	Qualitative	The author conclude that Blockchain improvements in transaction transparency and reliability are major and enable technology, innovation and social perspectives consensus

(*continued*)

Table 5.

Authors	Article	Objective	Methodology	Main findings
Milian *et al.* (2019)	Fintechs: A literature review and research agenda	Investigate the concept of fintech	Qualitative	The article identifies a set of FinTechs definitions and creates a map of the evolution of key topics and trends on FinTechs literature
Mohanta *et al.* (2019)	Trust Management in IOT Enable Healthcare System using Ethereum based Smart Contract	Approach security and privacy issues in IoT enabled applications based on decentralized Blockchain	Qualitative	The article identified and explained security challenges related with privacy on IoT applications. Using an Ethereum virtual machine, it was possible to implement Blockchain distributed network and healthcare insurance claims is used to test the technique, showing that it provides trust and addresses some of the security and privacy problems in the healthcare insurance sector
Pramothini *et al.* (2018)	Securing Images with Fingerprint Data using Steganography and Blockchain	Address the problems of privacy of legitimate users considering Blockchain and Steganography	Qualitative	Medical images storage and distribution could be protected by a combination of Steganography and digital watermarking techniques to assure confidentiality and Blockchain to assure non-repudiation. The detailed experimentation reveals enhancing in security when compared with other schemes

Table 5. (*continued*)

Authors	Article	Objective	Methodology	Main findings
Rahmadika and Rhee (2018)	Blockchain technology for providing an architecture model of decentralized personal health information	Address Blockchain technology and several protocols embedded using data from health-care providers to propose an architectural model to manage personal health information	Qualitative	The personal health information (PHI) could rely on Blockchain immutability of data record without having to trust a third party
Rane and Narvel (2019)	Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future Industry 4.0	Discuss the redesign of business for innovations based on Blockchain–IoT architecture that helps organizations to improve operations agility due to the emergence of disruptive technologies	Qualitative	Blockchain features, such as increasing the capacity of decentralization, trust-less transactions, security and allowing autonomous coordination of the IoT devices will improve agility in Industry 4.0. Blockchain and IoT merge gives industries (e.g. manufacturing, oil and gas, engineering and construction) a possibility to re-design business organization in a more agile way
Sushmetha and Vairamuthu (2019)	Message Authentication using Threshold Blockchain in VANET	Addresses Blockchain technology with an additional layer of cryptography to ensure security as a possible solution to infrastructure less environments	Mixed Based in secondary data of real time values of three out of eight pollutants monitored by Indian government	The results reveal that the usage of a threshold scheme suits ad hoc environments. The decentralized and distributed nature of Blockchain technology facilitates authentication of a new node in ad hoc environment where the new node could decide the threshold or verify the share of private key. The user anonymity confers threshold Block chain flexibility, confidentiality and scalability

Table 5.

Blockchain has recently served to provide security for P2P networks. Computationally expensive and heavyweight, blockchain is not inherently suitable for IoT architectures. However, there are emerging lightweight and secure architecture for the IoT that deploy Ethereum blockchain while maintaining its security power (Ghadekar *et al.*, 2019)

In addition, Hu *et al.* (2019) approach smart blockchain contracts as a means of reducing costs, risks and improving on poor levels of efficiency and transparency in energy power supply and demand networks in China. This concludes in favor of the scope for improved transaction efficiency based on a secure and efficient power trading environment.

According to Lee (2019), there are many expectations that blockchain will remodel the economic system and the way we communicate via the Internet. The great expectations of the blockchain technology derive from its promise of the trust and security that would in the future allow for the establishment of a token economy.

Milian *et al.* (2019) define fintech in accordance with the ways innovative financial companies make use of the availability and automatization of communication, the ubiquity of the Internet and the means by which companies deal with financial industry regulation and local legislation or the financial system globally. Blockchain emerges in the literature as interrelated with financial service operations with a great emphasis on security and the ways companies deal with financial losses.

Mohanta *et al.* (2019) approach one of the most promising research areas of the last decade: the IoT. With the increasing number of enabled devices, the IoT has established its presence across the insurance sector, smart environment monitoring, smart city, healthcare sector, smart transportation and agriculture sectors, etc. facing challenges out of the need of confidentiality, integrity, authentication, authorization, trust, verification, information storage and management availability. Deploying an Ethereum virtual machine does enable the implementation of a blockchain distributed network that provides for the management of trust and some of the security and privacy issues.

According to Pramothini *et al.* (2018), following innovations in technology and the Internet, the information distribution is now fast, easy and economical worldwide. However, the value of data makes it very attractive for theft and tampering. Through recourse to blockchain and steganography, it is possible to ensure confidentiality and security for data storage and distribution.

Rahmadika and Rhee (2018) conceptualize a model that makes recourse to blockchain to manage the personal health information derived from several healthcare providers while bestowing a guarantee of data integrity to the patients and access to the providers. Thus, blockchain offers trusted data without having to trust any third party; an important feature due to the sensitivity of personal health information data.

Anand and Tanguturi (2019) approach the importance of blockchain to securing wireless sensor networks. Cryptographic systems and routing protocols are useful but do not indicate the optimal network path and hence rendering it impossible to prevent attacks by unauthorized nodes. Combining blockchain and particle swarm optimization make it possible to ensure the security of every node used to identify the best path.

Rane and Narvel (2019) consider that the recent interest in Industry 4.0 has arisen due to the emergence of disruptive technologies and the consequent redesign of businesses based on IoT blockchain-based innovations in order to pursue agility in the future business environment.

Sushmetha and Vairamuthu (2019) take into consideration the usages of blockchain in infrastructure-less environments and conclude that the decentralized nature of blockchains facilitates the authentication of a new node in ad hoc environments but might become more secure when complemented with a cryptography scheme.

Authors	Article	Objective	Methodology	Main findings
Hoxha and Sadiku (2019)	Study of factors influencing the decision to adopt the blockchain technology in real estate transactions in Kosovo	Explore, from the point of view of Kosovo real estate buyers and sellers, how transparency, security and cost reduction affect Blockchain technology adoption	Quantitative Factor analysis of close-ended questionnaire applied to a 1.000 people stratified sample	Real estate buyers and sellers perceived transparency and cost reduction as major influencers in Blockchain technology adoption, followed by the security of transactions. Blockchain technology provides a transparent and errorless interaction. The cost reduction relies on smart contracts to eliminate intermediaries in real estate transactions, conducing to significant cost reduction giving speed and efficiency to the process
Kumar *et al.* (2019a, b)	Challenges Potential and Future of Internet of Things Integrated with Blockchain	Analyze the correlation between IoT enormous information quantities and its restrictions and how Blockchain could change the way we work in IoT	Qualitative	IoT relies on self-governing of regular gadgets, a path that is being achieved through innovation but there are some challenges like security and information dependability that needed to be addressed. Blockchain technology presents a trusted new way of sharing information that does not require hi-tech specialists

(*continued*)

Table 6.
Authors in cluster 3: data trust and share

Authors	Article	Objective	Methodology	Main findings
Lemieux (2016)	Trusting records: is Blockchain technology the answer?	Analyze value, limitations, risk and opportunities of Blockchain technology as a solution to create and preserve trustworthy digital records	Qualitative	The analysis suggests that Blockchain technology addresses data in present and in the short term, revealing several limitations as a long-term solution for maintaining trustworthiness
Li *et al.* (2018)	Toward open manufacturing a cross-enterprises knowledge and services exchange framework based on blockchain and edge computing	Definition of a cross-enterprises framework to achieve a higher level of sharing of knowledge and services in manufacturing ecosystems	Qualitative	Development of a framework that incorporates the recent development in Blockchain and edge computing to address secure and distributed requirements for the sharing of knowledge and services in manufacturing ecosystems
Li *et al.* (2019)	Blockchain for decentralized transactive energy management system in networked microgrids	Explore the possibility of customizing Blockchain technologies to meet socioeconomic requirements of transactive energy management at the power distribution level and considers additional smart contract measures for securing optimal energy transactions	Qualitative	The article proposed a Blockchain-based framework for decentralized transactive energy management, creating the base to better financial flows towards active distribution networks

Table 6. (*continued*)

Authors	Article	Objective	Methodology	Main findings
Poluri *et al.* (2019)	IOT Ecosystem with Blockchain and Smart Contracts	Addresses smart contracts to achieve a complete exploration of its concept, which indirectly relies on Blockchain technology, to map and explore the smart contract concept	Qualitative	Blockchain technology allows smart contracts to execute continually and to promote authorization and understanding between unknown entities without the concept of trust of a third party. IoT digital communications gained more security using smart contracts. The research identifies four key issues, namely systematizing, security, protection, and execution issues
Sehra *et al.* (2018)	On Cryptocurrencies, Digital Assets and Private Money	Review technical, economic and legal aspects related to cryptocurrencies to provide an interpretation of this complex and emerging field	Qualitative	The authors discuss the use of Blockchain and secondary tokens in issue, register and settle digital assets that could represent various property rights. The analysis of viability, complexity and limitations of the existing models intends to provide the reader a strong base to explore this field

(*continued*)

Table 6.

Authors	Article	Objective	Methodology	Main findings
Van der Elst and Lafarre (2019)	Blockchain and Smart Contracting for the Shareholder Community	Approach the use of permissioned Blockchain to increase the transparency and verifiability of shareholder engagement	Qualitative	The paper concludes that the use of permissioned Blockchain could address classical inefficiencies in shareholders engagement systems. The large chains of intermediaries in the current securities models involves high transaction costs and shareholders votes are not always correctly transmitted. The information asymmetry creates inequalities and hindering shareholder democracy. Blockchain technology has emerged in the last two years with prototypes and legislative initiatives that show its use merits. It is important that Europe Union incorporates Blockchain technology in its legislation
Zhu and Kouhizadeh (2019)	Blockchain Technology, Supply Chain Information, and Strategic Product Deletion Management	Applicability of Blockchain technology to supply chain namely application recommendations and managerial insights into product deletion decision-making processes with Blockchain technology	Qualitative	Development of a framework of strategic product deletion management and Blockchain technology, to support supply chain information system

Table 6.

3.2.3 Cluster 3: data trust and sharing. Table 6 depicts the nine articles in cluster 3, data trust and sharing.

Hoxha and Sadiku (2019) advance with an analysis of the relationship between blockchain technology and aspects such as transparency, security and cost reduction from the perspective of real estate buyers and sellers. After surveying 1,000 people, they infer that real estate buyers and sellers attribute higher importance to transparency and cost reductions in their intentions toward adopting blockchain technology, followed by the security of transactions. Smart blockchain contracts enable the elimination of intermediaries that ensure cost reductions and faster and more efficient processes. Additionally, increasing trust between sellers and buyers might also act as a way to fight corruption in real estate investments.

According to Kumar *et al.* (2019a, b) the upcoming advances in the IoT field will make regular gadgets savvy and self-governing. This raises new challenges, especially in terms of security and information dependability. However, blockchain will not require specialists because the hi-tech development will profoundly alter numerous enterprises.

Lemieux (2016) explores the value of blockchain as a possible solution for creating and maintaining trustworthy digital records. Considering implementations of blockchain technology led to the proposition of an evaluative framework for a risk-based assessment of developing country land registry systems. Blockchain technology might thus serve to address information integrity and reliability in a short-term scenario; however, there are limitations in terms of maintaining trustworthy digital records as a long-term solution.

Li *et al.* (2018) set out a framework for achieving a higher level of shared knowledge and services in manufacturing ecosystems. The basis of study was the emerging open manufacturing sector and the debate around manufacturer knowledge creation processes. This framework involves six layers, specifically, a customer layer, an enterprise layer, an application layer, an intelligence layer, a data layer and an infrastructure layer. The framework applications, based on blockchain and edge computing, reveal a system change from integrated and centralized to shared and distributed. With blockchain standards and protocols, implementing a framework for sharing knowledge and services becomes secure.

Li *et al.* (2019) analyze a scheme developed for blockchain-based networked microgrids and deployed in power distribution systems to optimize financial and physical operations. The authors explore how customizing blockchain to address the economic requirements of transactive energy management at the power distribution level through utilization of networked microgrids to transact energy may apply blockchain technology to optimize management of the efficiency, reliability, resilience, security and sustainability of electricity power services. The application of smart blockchain contracts increases the credibility and security of energy transactions and enables the transition from a traditional power distribution system to active distribution networks.

Poluri *et al.* (2019) approach smart contracts as a piece of code that continuously runs over the blockchain to detect any unauthorized entry of entities lacking the concept of trust and third party intrusions. 26 publications with different database origins identify how smart contracts address systematizing, security, protection and execution issues in communications.

Sehra *et al.* (2018) address the technical, economic and legal issues of cryptocurrencies. Blockchain might serve to define digital assets for securities, private forms of money or other property rights.

Van der Elst and Lafarre (2019) deal with the high transaction costs due to the number of intermediaries in current security models. This problem, when regulated to serve modern technologies, increases transparency and enables the verification of shareholder engagement.

After shareholder engagement, the system enables different opportunities for different types of shareholders and only possible through blockchain technology customized for the purpose.

Zhu and Kouhizadeh (2019) maintain the supply chain performance influences product management. Decisions over product deletion, rationalization or discontinuation must be well-structured processes that encompass recognition, analysis and revitalization, evaluation and decision formation and implementation. Blockchain features (e.g. traceability, transparency, security, accuracy and smart execution) may prove fundamental to rationalizing product deletion decisions.

3.2.4 Cluster 4: applicability. Table 7 presents the eight articles belonging to cluster 4; applicability.

According to Coyne and McMickle (2017), blockchain technology enabled the successful creation of decentralized digital currency networks. This success promptly instigated other potential applications in other business areas, particularly in accounting. While it is not feasible to apply blockchain as a financial reporting tool because blockchain digital currencies only exist within the blockchain, furthermore there are economic transactions that exist outside the accounting records rendering blockchain neither fully available nor even reliable for accounting purposes. On the other hand, McCallig *et al.* (2019) developed an information system applied to financial reporting information that enables the aggregation and reporting of private company data. This derived from how other departments already hold this information to provide for reporting and audit processes. Such reporting and audit processes, public keys and the accounting recordkeeping developed enable public access with the benefit of blockchain privacy guaranteeing the faithfulness of the respective financial reporting.

Ferrer-Gomila *et al.* (2019) analyze 40 proposals for electronically signing contracts, the basis of e-commerce transactions. Normally, the solutions available must achieve fairness of exchange even if not one of proposals studied met this requirement. The authors present a feasible protocol for blockchain-based contract signing that satisfies the necessary security requirements: fairness, timeliness and non-repudiation. This solution is both more reliable than other blockchain-based options and the most efficient in terms of cost, efficiency and security.

Mathew *et al.* (2019) describe how blockchain often serves to prevent illegal access to networks. The security and privacy features make blockchain very attractive to banking, credit card transaction, trading and online applications. The authors propose a blockchain and IoT based smart-home design that monitors the home and traps the intruder.

For Saberi *et al.* (2019), blockchain technology ensures supply chain transparency, traceability and security and promises the easier management of supply chain problems. Blockchain is still in its early stages and the existing barriers need categorizing (e.g. inter-organizational, intra-organizational, technical and external to barriers) and provide insights into how to overcome them.

Yin *et al.* (2019) approach the bitcoin blockchain where entity identities remain hidden behind a pseudonym labeled address and thereby retaining a high degree of anonymity. This anonymity feature leads to its frequent utilization in illicit activities. However, addressing this problem might involve the creation of supervised machine learning to analyze the type of still-unidentified entities. The method has many potential applications in society, organizational regulation and compliance.

4. Conclusions, implications and future research agenda

The articles reviewed enabled the development of a framework for better understanding the blockchain security process (Figure 6).

Authors	Article	Objective	Methodology	Main findings
Coyne and McMickle (2017)	Can blockchains serve an accounting purpose?	Analyze the implementation of the Blockchain as a financial reporting tool	Qualitative	Considering that economic transactions exist outside of accounting records, Blockchain model is not fully available or reliable in an accounting setting
Ferrer-Gomila *et al.* (2019)	A fair contract signing protocol with blockchain support	Present a protocol for smart contract signing based on Blockchain that does not require trusted third party (TTP) and compare the new protocol to previous solutions for contract signing based on Blockchain in terms of cost, efficiency and security	Qualitative	Analyze the existing protocols contract signing are divided in those that have a trusted third party (TTP) to achieve fairness and those that do not. The existing published proposals (40), based on Blockchain, hane not yet been recognized and applied in the market
Mathew *et al.* (2019)	Assimilation of Blockchain for Augmenting the Security and Coziness in IoT Based Smart Home	Design a Blockchain Integrated IOT Based Smart Home that monitors the home and effectively prevent the entry of harmful users	Qualitative	It was possible to achieve a system prototype Blockchain Integrated IOT Based Smart Home Based with the implementation of Ethereum Private Blockchain network. It needs to enhance the sensors and its prediction performances
McCallig *et al.* (2019)	Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a Blockchain	Define an accounting information system to enhance the representational faithfulness of financial reporting information	Qualitative	Define the simultaneous use public key cryptography and network analysis and define accounting recordkeeping techniques based on Blockchain to balance public access and privacy

(*continued*)

Table 7.
Authors in cluster 4: applicability cluster

Authors	Article	Objective	Methodology	Main findings
Rîndaşu (2019)	Blockchain in Accounting: Trick or Treat?	Investigate the benefit contexts of Blockchain technology to accounting practitioners, addressing companies' actual needs	Qualitative	Providing a practical point of view on the main challenges and advantages in daily impact, eliminating the redundant activities and offering a better level of the data security
Saberi *et al.* (2019)	Blockchain technology and its relationships to sustainable supply chain management	Examination of Blockchain technology and smart contracts and possible applicability to supply chain management	Qualitative	Categorization of the Blockchain barriers and future research agenda to provide insights into overcoming barriers and adopt Blockchain technology in supply chain management
Smith and Dhillon (2019)	Assessing blockchain potential for improving the cybersecurity of financial transactions	Understand how financial sector organizations address the problem of cybersecurity and utilizing Keeney's (1992) multi-objective decision analytics technique, termed value-focused thinking (VFT), to demonstrate how organizations can analyze Blockchain as a potential solution	Qualitative	Prove to be viable the use of Keeney's VTF (1992) as a multi-criteria decision analysis tool for assessing Blockchain technology and how it can be extended and adapted for individual organizations
Yin *et al.* (2019)	Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain	Explore a de-anonymizing approach to Bitcoin Blockchain by using Supervised Machine Learning to predict the type of yet-unidentified entities	Quantitative Based on a sample of 957 entities (with ≈385 million transactions)	Definition of a model to predict the type of a yet-unidentified entity using the Gradient Boosting algorithm

Table 7.

The framework presented arises out of the articles reviewed and explains blockchain technology security in accordance with four clusters in the literature, specifically, (1) feasibility, (2) fintech and cryptocurrency, (3) data trust and sharing and (4) applicability. Feasibility results from a process that balances advantages and disadvantages (Table, 2019). According to (Umarovich *et al.*, 2017), economic agents need to undergo institutional, legal, information and technological preparation to effectively solve economic problems. Prasad *et al.* (2018) identifies a set of 19 CSFs to facilitate success in blockchain-based cloud services.

In the second cluster, fintech and cryptocurrency, progress is important on the need to establish a regulatory regime that protects ICO investors (Deng *et al.*, 2018), to combine

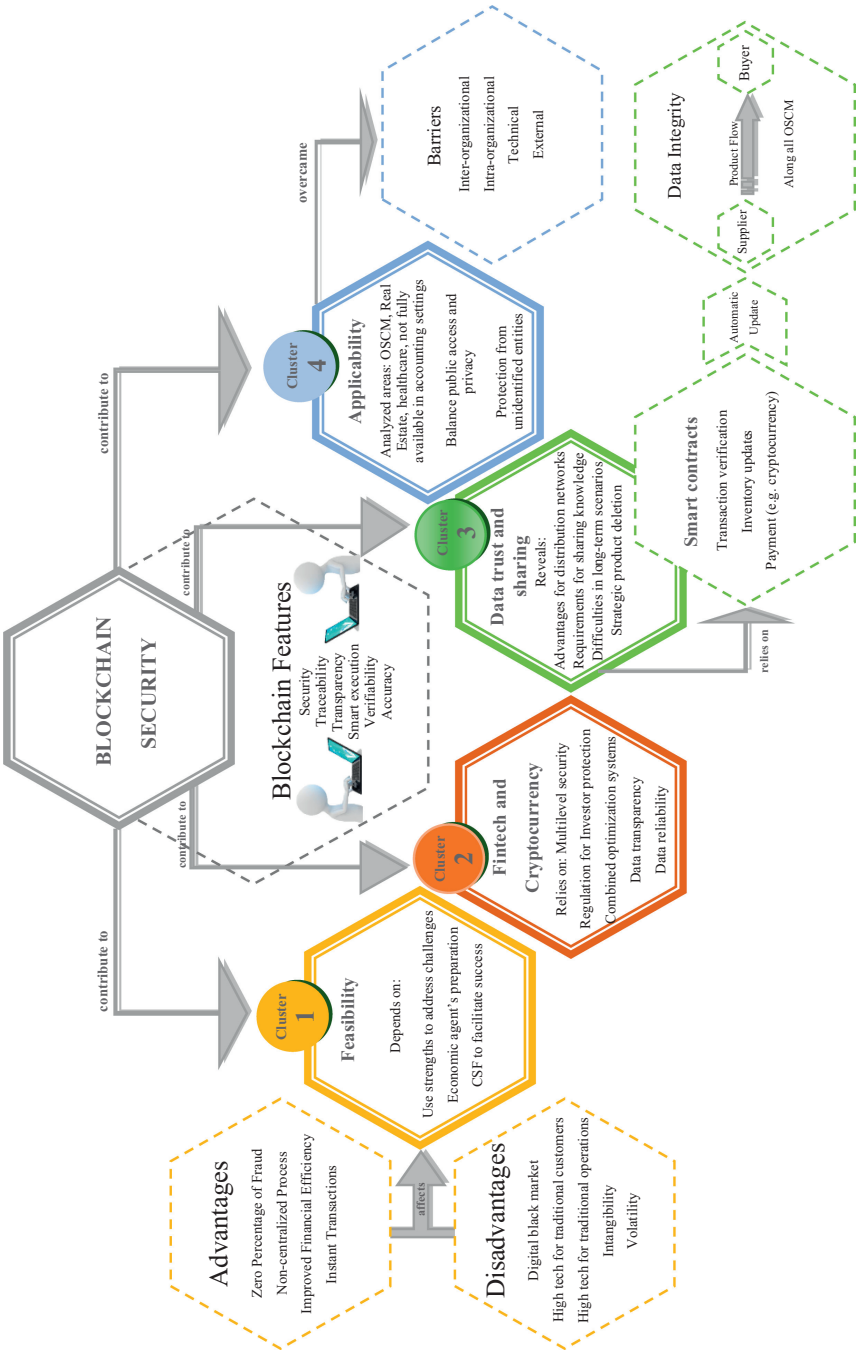

Figure 6.
Framework for blockchain security analyzes

optimization systems to prevent unauthorized nodes (Anand and Tanguturi, 2019) and guarantee multilevel security based on data transparency and data reliability (Lee, 2019).

In the third cluster, data trust and sharing, the framework emphasizes the emergence of advantages to distribution networks (Li *et al.*, 2019) but also points out several difficulties to blockchain security in long-term scenarios (Lemieux, 2016) and identify directions such as strategic product deletion (Zhu and Kouhizadeh, 2019). To guarantee security, traceability, transparency, verifiability, accuracy and smart execution features, blockchain relies on smart contracts (Cole *et al.*, 2019). Correspondingly, smart contracts allow for the automatic updating of validated data along all the Operations and Supply Chain Management (OSCM) within the ultimate intent of blockchain security (Cole *et al.*, 2019).

The fourth cluster, applicability, presents several different areas of application (e.g. OSCM, healthcare, finance, accounting, real estate, etc.), enhancing the need for a correct balance between public access and privacy (McCallig *et al.*, 2019) and reinforcing the need for protection from unidentified entities (Yin *et al.*, 2019). Applicability deals with several barriers, namely; intra-organizational, inter-organizational, technical and external (Saberi *et al.*, 2019).

In keeping with the articles revised, we may identify several research gaps.

Table 8 summarizes the aspects to consider in future research on the adoption and implementation of blockchain technology.

According to Cole *et al.* (2019), it is too early to make any large-scale survey of the impact of blockchain technology. However, there is broad scope for enriching the theoretical knowledge on the adoption of blockchain technology.

The first cluster, feasibility, directs us to a context where we have to balance the gains and the costs of adopting blockchain. Given its current success, research importantly needs to address the implementation phase to define who is paying the bill in establishing blockchain technology procedures. *Cole et al.* (2019) questioned ways to incentivize several

Table 8.
Summary of suggestions for future research

Cluster | area	Suggestions for future research
(1) Feasibility	Address the blockchain technology implementation phase to define who is paying the bill for establishing the procedures
	Consider the product and supply chain characteristics that might return sufficient payback in blockchain implementation
	Analyze the costs of blockchain adoption and implementation
	Analyze interactions with features of other models
(2) Fintech and cryptocurrency	Analyze blockchain technology development for OSCM based on the comparison with other successful or unsuccessful technologies
	Creation of a regulatory framework for FinTech technologies
(3) Data trust and sharing	Detail the CSF to clarify the importance of data trustworthiness and sharing
	Due to the importance of data security and privacy colliding with the existence of suspicious entities, it is important to explore the need for blockchain to prove that transactions are not interconnected with illicit activities
	Analyze the patterns of common attacks on blockchain transactions that might serve to detect illicit activities
(4) Applicability	Address the standardization of smart contracts as a means of cost reduction via fewer intermediaries and boosting both transparency and security (e.g. real estate, finance and logistics)
	Explore the creation of the standards required by blockchain specifications to enhance the IoT system to make their data interoperable and enable a wider range of devices
	Analyze the blockchain use in content streaming companies to enable secured data storage and interoperability

OSCM partners toward blockchain adoption and clarify just who should pay for its introduction given its achievements in terms of end-to-end transparency. Given the success of blockchain, it is important to analyze this technology with features from other emerging models. For example, Fu *et al.* (2019) present the Bead Strand Model with a self-destructing mechanism whereby users can define which data vanishes on the respective expiry date.

The second cluster, fintech and cryptocurrency, approaches the development of new financial technologies and the need for a regulatory framework for the functioning of financial technologies, addressing the legal barriers that may compromise the development of this market and the launching of new financial instruments. This also needs a harmonized legal and regulatory framework among different countries (Vovchenko *et al.*, 2018). In OSCM, this needs to address how blockchain technology might be enhanced by comparisons with other successful or unsuccessful technologies. The third cluster, data trust and sharing, sustains that blockchain emerged recently as one of the most disruptive technologies of the last few years. Prasad *et al.* (2018) presents a set of 19 CSFs that may influence the success of blockchain-based cloud services. After this initial identification and study, it would be important to access a detailed version of these CSFs to enrich the theoretical base clarifying the importance of data trustiness and sharing. In this scenario, there emerges the collision between data security and data privacy. Privacy assurances allow for the existence of suspicious entities and acknowledging whether blockchain might act to detect illicit activities or prove entities are not involved in illicit activities is particularly important (Bathula and Basha, 2019). In the fourth cluster, Applicability, research should focus on the generalization of blockchain technology areas of applicability. Li *et al.* (2019) sustains that blockchain technology represents a solution for addressing cybersecurity and mutual-trust via cryptography and smart contracts. The standardization of smart contracts does potential provide an effective cost reduction via fewer intermediates as well as a means of enhancing transparency and security (e.g. real estate, finance and logistics (Hoxha and Sadiku, 2019). Giancaspro (2017) approaches the smart contract potential for increasing commercial efficiency, reducing transactional and legal costs and facilitating transparent and anonymous transactions. However, several legal issues still hang over the legality of smart contracts. With the application of smart contracts, we can bypass intermediaries to achieve airtight agreements. The adoption of smart contracts in industries including finance, real estate, academia and logistics brings about a higher level of transparency and security. This issue gains special attention in content streaming companies due to the mandatory need of secured data storage and the provision of interoperability (Venkateswara *et al.*, 2018).

Blockchain technology success deeply interconnects with Bitcoin's success. The development of both blockchain and the IoT will bring about many changes for the creating, performing and securing of data. Blockchain emerged as a good solution for boosting information security and preventing assaults on devices. The forecast is for blockchain to ensure the reliability, scalability, reusability and responsibility of the IoT. Blockchain technology applications are already operational in areas such as healthcare, financial and real estate but still needs to tailor its features to adapt to P2P applications and become suitable for many other areas. There are also differences between its short-term performances, where it shows better guarantees, than that returned in long-term scenarios. However, blockchain achieves good results in supply-chain management operations as a means of cost reduction and raising transparency while noting an emphasis on the need for the standardization of smart contracts.

Only in 2019 did the first quantitative studies reveal a more solid theoretical basis to underpin the development of more specific and directed research. This study presents direct

implications for the literature on blockchain security, systematizing the existing studies and addressing the need for a systematic literature review that approaches both concepts simultaneously. It provides a framework that enables the scientific community to access the main subjects discussed and the articulations existing between these concepts. This also puts forward ideas for future research development.

The principal limitations of this paper relate to the broad scope of the existing literature published since the launch of blockchain, due to the variety of areas potentially benefiting from its application and in addition to recourse to but one database, Scopus, which may thus have overlooked some key articles.

References

Anand, S.R. and Tanguturi, R.C. (2019), "Blockchain based packet delivery mechanism for WSN", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 2, pp. 1112-1117.

Bathula, A. and Basha, S.K. (2019), "Blockchain technology with internet of things in the real time network stream", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 4, pp. 682-689.

Cole, R., Stevenson, M. and Aitken, J. (2019), "Blockchain technology: implications for operations and supply chain management", *Supply Chain Management*, Vol. 24 No. 4, pp. 469-483.

Coyne, J.G. and McMickle, P.L. (2017), "Can blockchains serve an accounting purpose?", *Journal of Emerging Technologies in Accounting*, Vol. 14 No. 2, pp. 101-111.

Deng, H., Huang, R.H. and Wu, Q. (2018), "The regulation of initial coin offerings in China: problems, prognoses, and prospects", *European Business Organization Law Review*, Vol. 19, pp. 465-502.

Dhagarra, D., Goswami, M., Sarma, P.R.S. and Choudhury, A. (2019), "Big Data and blockchain supported conceptual model for enhanced healthcare coverage: the Indian context", *Business Process Management Journal*, Vol. 25 No. 7, pp. 1612-1632, doi: 10.1108/BPMJ-06-2018-0164.

Dimitropoulou, C., Govind, S. and Turcan, L. (2018), "Applying modern, disruptive technologies to improve the effectiveness of tax dispute resolution: part 1", *Intertax*, Vol. 46, No. 11, pp. 856-872.

Ferrer-Gomila, J.L., Francisca Hinarejos, M. and Isern-Deyà, A.P. (2019), "A fair contract signing protocol with blockchain support", *Electronic Commerce Research and Applications*, Vol. 36, January, 100869.

Fu, X., Wang, Z., Chen, Y., Zhang, Y. and Wu, H. (2019), "Bead Strand Model: a high-efficiency storage structure for self-destructing data in cloud environment", *Service Oriented Computing and Applications*, Vol. 13 No. 2, pp. 95-103.

Ghadekar, P., Doke, N., Kaneri, S. and Jha, V. (2019), "Secure access control to IoT devices using blockchain", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 2, pp. 3064-3070.

Giancaspro, M. (2017), "Is a 'smart contract' really a smart idea? Insights from a legal perspective", *Computer Law and Security Review*, Vol. 33 No. 6, pp. 825-835.

Gupta, A. and Jose, D.V. (2019), "A method to secure FIR system using blockchain", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 1, pp. 626-629.

Hoxha, V. and Sadiku, S. (2019), "Study of factors influencing the decision to adopt the blockchain technology in real estate transactions in Kosovo", *Property Management*, Vol. 37 No. 5, pp. 684-700.

Hu, W., Hu, Y.W., Yao, W.H., Lu, W.Q., Li, H.H. and Lv, Z.W. (2019), "A blockchain-based smart contract trading mechanism for energy power supply and demand network", *Advances in Production Engineering and Management*, Vol. 14 No. 3, pp. 284-296.

Kanimozhi, E. and Akila, D. (2019), "Block chain smart contracts on Iot", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 2, pp. 105-110.

Karaarslan, E. and Adiguzel, E. (2018), "Blockchain based DNS and PKI solutions", *IEEE Communications Standards Magazine*, Vol. 2 No. 3, pp. 52-57, IEEE.

Keeney, R.L. (1992), *Value-Focused Thinking*, Harvard University Press, Cambridge, MA.

Kessler (1963), "Kessler-1963-American_Documentation", *American Documentation*, Vol. 14 No. 1, pp. 10-25.

Kumar, A., Jha, G., Sharma, L. and Khatri, S. (2019a), "Challenges potential and future of internet of things integrated with blockchain", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 2S7, pp. 530-536.

Kumar, A.N., Jegadeesan, R., Ravi, C.N. and Greeda, J. (2019b), "A secure transaction authentication scheme using blockchain based on Iot", *International Journal of Scientific and Technology Research*, Vol. 8 No. 10, pp. 2217-2221.

Lee, J.Y. (2019), "A decentralized token economy: how blockchain and cryptocurrency can revolutionize business", *Business Horizons*, Vol. 62 No. 6, pp. 773-784, doi: 10.1016/j.bushor.2019.08.003.

Lemieux, V.L. (2016), "Trusting records: is Blockchain technology the answer?", *Records Management Journal*, Vol. 26 No. 2, pp. 110-139.

Li, Z., Wang, W.M., Liu, G., Liu, L., He, J. and Huang, G.Q. (2018), "Toward open manufacturing a cross-enterprises knowledge and services exchange framework based on blockchain and edge computing", *Industrial Management and Data Systems*, Vol. 118 No. 1, pp. 303-320.

Li, Z., Bahramirad, S., Paaso, A., Yan, M. and Shahidehpour, M. (2019), "Blockchain for decentralized transactive energy management system in networked microgrids", *The Electricity Journal*, Vol. 32 No. 4, pp. 58-72.

Limba, T., Stankevičius, A. and Andrulevičius, A. (2019), "Towards sustainable cryptocurrency: risk mitigations from a perspective of national security", *Journal of Security and Sustainability Issues*, Vol. 9 No. 2, pp. 375-389.

Mathew, R.M., Suguna, R. and Devi, M.S. (2019), "Assimilation of blockchain for augmenting the security and coziness in IoT based smart home", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 2, pp. 2274-2279.

McCallig, J., Robb, A. and Rohde, F. (2019), "Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain", *International Journal of Accounting Information Systems*, Vol. 33, pp. 47-58.

Milian, E.Z., Spinola, M.de M. and Carvalho, M.M.d. (2019), "Fintechs: a literature review and research agenda", *Electronic Commerce Research and Applications*, Vol. 34, 100833.

Millard, C. (2018), "Blockchain and law: incompatible codes?", *Computer Law and Security Review*, Vol. 34 No. 4, pp. 843-846.

Mohanta, B.K., Jena, D. and Satapathy, U. (2019), "Trust management in IOT enable healthcare system using ethereum based smart contract", *International Journal of Scientific and Technology Research*, Vol. 8 No. 9, pp. 758-763.

Monika, G.S., Parthipan, V., Palaniappan, S. and Manikanta, S.D.S. (2019), "Beneficial P2P storage scheme with privacy protection", *International Journal of Recent Technology and Engineering*, Vol. 7 No. 6, pp. 472-476.

Poluri, M., Kumar, A., Allam, S. and Kiran, K.V.D. (2019), "IOT ecosystem with blockchain and smart contracts", *International Journal of Recent Technology and Engineering*, Vol. 7 No. 6, pp. 638-641.

Prabhakaran, R. and Asha, S. (2019), "Enhancing cyber security in power sector systems using block chain", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 1, pp. 58-62.

Pramothini, S., Sai Pavan, Y.V.V.S. and Harini, N. (2018), "Securing images with fingerprint data using steganography and blockchain", *International Journal of Recent Technology and Engineering*, Vol. 7 No. 4, pp. 82-85.

Prasad, S., Shankar, R., Gupta, R. and Roy, S. (2018), "A TISM modeling of critical success factors of blockchain based cloud services", *Journal of Advances in Management Research*, Vol. 15 No. 4, pp. 434-456.

Rahmadika, S. and Rhee, K.H. (2018), "Blockchain technology for providing an architecture model of decentralized personal health information", *International Journal of Engineering Business Management*, Vol. 10, pp. 1-12.

Rane, S.B. and Narvel, Y.A.M. (2019), "Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future Industry 4.0", *Benchmark*, doi: 10.1108/BIJ-12-2018-0445.

Rîndaşu, S. M. (2019), "Blockchain in accounting: trick or treat?", *Quality-Access to Success*, Vol. 20 No. 170, pp. 143-147.

Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L. (2019), "Blockchain technology and its relationships to sustainable supply chain management", *International Journal of Production Research*, Vol. 57 No. 7, pp. 2117-2135.

Samsudeen, Z., Perera, D. and Fernando, M. (2019), "Behavioral analysis of bitcoin users on illegal transactions", *Advances in Science, Technology and Engineering Systems Journal*, Vol. 4 No. 2, pp. 402-412.

Scuderi, A., Foti, V. and Timpanaro, G. (2019), "The supply chain value of pod and pgi food products through the application of blockchain", *Quality - Access to Success*, Vol. 20 No. S2, pp. 580-587.

Sehra, A., Cohen, R. and Arulchandran, V. (2018), "On cryptocurrencies, digital assets and private money", *Journal of Payments Strategy and Systems*, Vol. 12 No. 1, pp. 13-32.

Smith, K.J. and Dhillon, G. (2019), "Assessing blockchain potential for improving the cybersecurity of financial transactions", *Managerial Finance*, doi: 10.1108/MF-06-2019-0314.

Subramanian, H. (2019), "Security tokens: architecture, smart contract applications and illustrations using SAFE", *Managerial Finance*, doi: 10.1108/MF-09-2018-0467.

Sushmetha, N. and Vairamuthu, S. (2019), "Message authentication using threshold blockchain in VANET", *International Journal of Recent Technology and Engineering*, Vol. 7 No. 6, pp. 1464-1466.

Taleb, N. (2019), "Prospective applications of blockchain and bitcoin cryptocurrency technology", *TEM Journal*, Vol. 8 No. 1, pp. 48-55.

Tranfield, D., Denyer, D. and Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", *British Journal of Management*, Vol. 14 No. 3, pp. 207-222.

Umarovich, A.A., Gennadyevna, V.N., Vladimirovna, A.O. and Alexandrovich, S.R. (2017), "Block chain and financial controlling in the system of technological provision of large corporations' economic security", *European Research Studies Journal*, Vol. 20 No. 3, pp. 3-12.

Van der Elst, C. and Lafarre, A. (2019), "Blockchain and smart contracting for the shareholder community", *European Business Organization Law Review*, Vol. 20 No. 1, pp. 111-137.

Veena, A.M., Ananthi, V. and Sureka (2019), "Adopting blockchain technologies in cloud for efficient data storage and enhanced security", *International Journal of Recent Technology and Engineering*, Vol. 8 No. 2S8, pp. 1295-1297.

Venkateswara, K.L., Bala Dinakar, R. and Siva Prasad, P. (2018), "Blockchain technology - a sturdy protective shield", *International Journal of Recent Technology and Engineering*, Vol. 7 No. 4, pp. 269-272.

Vovchenko, N.G., Ivanova, O.B., Andreeva, O.V. and Kostoglodova, E.D. (2018), "Conceptual approach to the development of financial technologies in the context of digitalization of economic processes", *European Research Studies Journal*, Vol. 21 No. 2, pp. 11-20.

Xu, L. Da, Xu, E.L. and Li, L. (2018), "Industry 4.0: state of the art and future trends", *International Journal of Production Research*, Vol. 56 No. 8, pp. 2941-2962.

Yin, H.H.S., Langenheldt, K., Harlev, M., Mukkamala, R.R. and Vatrapu, R. (2019), "Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain", *Journal of Management Information Systems*, Vol. 36 No. 1, pp. 37-73.

Zhu, Q. and Kouhizadeh, M. (2019), "Blockchain technology, supply chain information, and strategic product deletion management", *IEEE Engineering Management Review*, Vol. 47 No. 1, pp. 36-44, IEEE.

About the authors

Lurdes D. Patrício is a PhD candidate in the University of Beira Interior, Portugal. Her research interests include strategy and technology.

João J. Ferreira is an Associate Professor at the University of Beira Interior (UBI) – Portugal. He holds a PhD in Entrepreneurship and Small Business Management from the Autonomous University of Barcelona (UAB), Spain. Currently, he is a Scientific Coordinator of NECE – Research Centre in Business Sciences. His research interests include: strategy, competitiveness and entrepreneurship. He is also an Editor and Reviewer Board of some International Journals, author of some books and he has published extensively in a variety of leading journals. João Ferreira is the corresponding author and can be contacted at: jjmf@ubi.pt