Telematics and Informatics 60 (2021) 101593

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Blockchain technology as an enabler of consumer trust: A text mining literature analysis

Catarina Ferreira da Silva [a,b,*], Sérgio Moro [a,*]

[a] Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR, Lisboa, Portugal
[b] Center for Informatics and Systems of the University of Coimbra (CISUC), Portugal

ARTICLE INFO

Keywords:
Blockchain
Consumer trust
Consumer transparency
Privacy
Literature analysis
Topic modelling

ABSTRACT

Blockchain (BC) technology is gaining momentum in a variety of application domains, beyond finance. We present a text mining literature analysis of a body of published articles queried in the Scopus database, regarding BC technology and consumer trust. We applied a semiautomated text mining and topic modelling approach: we mix top-down and bottom-up procedures to align the existing literature on BC taxonomies with the gathered articles' list of keywords; we then feed automatically the latent Dirichlet allocation (LDA) algorithm to uncover relevant topics enabling to analyse the existing body of knowledge. Our analysis highlights the multidisciplinary nature of BC research within consumer trust. Among others, findings show pertinent aspects to consumer trust, such as traceability and privacy, are receiving only marginal attention from scholars. Our analysis also reveals the marketing, social and economic sciences' researchers should devote efforts to the application of BC and its impact to consumer trust. We provide future research trends we deem crucial to be addressed regarding sustainable blockchain trustability.

1. Introduction

Blockchain technology is gaining momentum, since its start in 2009 (Nakamoto, 2009) and can be one of the elements of the ongoing digital transformation, which has the potential to bring on modifications to business processes (Baiyere et al., 2020). A blockchain (BC) is a ledger of continuously growing list of records, named blocks, which are connect between themselves and secured using cryptographic mechanisms. This ledger registers processed transactions made between users, stores value information, allowing the user's computer to check the validity of the transaction (Yaga et al., 2018). The transaction authentication is protected by the digital cryptographic signature of the sending address. The first and mostly widely known usages of BC are in the cryptocurrencies' markets (Li and Whinston, 2020) and Internet-based finance (Guo and Liang, 2016). By securing transactions between untrusting parties, BC disrupts traditional transactions as it facilitates rule out of the trusted third party, hence avoiding this single point of failure (Nofer et al., 2017).

Consumer trust is a key construct in Marketing models (McKnight et al., 2002; Pappas, 2016). Marketing literature acknowledges the influence of consumer trust in consumer behaviour (Sirdeshmukh et al., 2002), purchase intention (McKnight et al., 2002), and consumer loyalty (Delgado-Ballester et al., 2001). Therefore, the recognition of BC technology as an enabler of trust by marketers across industries is leading to a wide range of BC applications beyond the narrower cryptocurrency scope from where it emerged (Hughes et al., 2019). Trust can be perceived by consumers as a synonym of quality regarding the final product offered at the end of a

* Corresponding authors.
E-mail addresses: Catarina.Ferreira.Silva@iscte-iul.pt, alvescatarina@yahoo.com (C. Ferreira da Silva), scmoro@gmail.com (S. Moro).

https://doi.org/10.1016/j.tele.2021.101593
Received 1 June 2020; Received in revised form 28 December 2020; Accepted 15 February 2021
Available online 21 February 2021

supply chain (Van Rijswijk and Frewer, 2012), by assuring the information regarding the product is reliable, increasing transparency. Additionally, in current times when large web platforms hosted by a few global-wide companies such as Google, Amazon, and Facebook dominate the online landscape and take advantage of individuals' personal data, perceived privacy and security are also playing a key role in consumers' trust (Ayaburi and Treku, 2020). These factors contribute to the increased perceived value of BC, given its premises.

Whether there is currently a hype around BC or not, BC research has recently flourished across many directions. As such, a refreshed literature analysis on BC body of knowledge is important to highlight current trends and gaps, helping to offer a holistic view and guide future efforts. Hawlitschek et al. (2018) focused specifically on trust-free systems based in BC in the sharing economy by analysing 45 sharing economy articles together with 17 BC articles. From another perspective, Seebacher and Schüritz (2017) analysed 32 articles to identify the characteristics that enable trust and decentralization within the context of service systems. Casino et al. (2019) conducted a broad systematic literature review of BC-based applications following a thorough manual screening of 260 articles published until April 2018. They developed a taxonomy of the different types of BC applications. In contrast, we focus specifically on studies which highlight trust/transparency from the consumer perspective. We adopt a mixed approach by including a top-down procedure based on existing literature on BC taxonomies and a bottom-up procedure drawn from each article's list of keywords extracted from 432 gathered articles published until November 2019. Such approach enriches existing BC taxonomies by benefiting from a passive crowdsourcing effect, given the articles keywords were defined by the authors, who considered them as important for indexing purposes. The articles are then automatically analysed by using text mining and topic modelling to unveil interesting topics that summarize the existing body of knowledge. The use of text mining to conduct literature analyses is becoming mainstream as science keeps developing grounded on Internet media (Feng et al., 2019a, 2018). By adopting text mining, it is possible to cover a vast body of knowledge which otherwise would render infeasible only at the expense of computational power (Moro et al., 2019). Through such an approach, we aim to contribute to a better understanding of BC from the important consumer trust perspective. We raise the following research questions (RQ) which help in guiding our analysis:

- RQ1: What are the main aspects of BC technologies and how are these becoming mainstream within consumer trust?
- RQ2: What are the aspects of BC technologies mostly addressed by the more prominent application domains, beyond the finance area?
- RQ3: What are the relations between BC application domains and the aspects of BC technologies and how can these associations be useful to the research BC community?

The remainder of the paper is as follows. We address BC technology inception and related concepts, as well as consumer trust and its relationship with BC technology in section 2. Section 3 presents the materials and methods we apply in our work, in particular our mixed approach comprising top-down and bottom-up procedures to connect the existing taxonomies of BC concepts with the gathered article's list of keywords. We then use this alignment to support the analysis of our results, which are obtained automatically by using text mining and topic modelling approach and discuss our research questions (section 4). Section 5 closes with conclusions and perspectives.

2. Background

2.1. Blockchain inception and evolution

According to Iansiti and Lakhani (2107), the level of transformation and also of complexity brought by BC technology is unprecedented. Being based on the consensus power of a network of nodes, it eliminates the need for an outside authority. However, BC is based on previous technological developments. Before BC, digital cash (Chaum, 1983) was conceptualized using cryptographic protocols for enabling transactions between mutually untrusting parties. The current enhancement of BC and its particular application in cryptocurrencies over Chaum's proposal is the decentralized architecture of the payment system permitted by the BC technology, hence leading to a state of affairs that goes further the crypto-economy (Pilkington, 2016), extending to transactions and ledger records in any application field benefiting from traceability, transparency and decentralized transactions between untrusting parties, such as healthcare and energy. Application of BC is being investigated in a variety of sectors (Casino et al., 2019).

A BC is a shared distributed ledger of cryptographically hashed blocks. These blocks contain published transactions or information, cryptographically signed by the sender, which are validated after a consensus and decision process among the network nodes or a set of them. The chain of blocks grows as new blocks are added, making it more difficult to modify older blocks. New published blocks are duplicated among the publishing nodes. These characteristics along with the cryptographic mechanisms make any attempt to modify a ledger of published blocks difficult to go unnoticed (Yaga et al., 2018).

Different approaches to reach consensus in a BC network are compared by Yaga et al. (2018), e.g., the Proof of Work (PoW), Proof of Stake (PoS), Delegated PoS, Round Robin, Proof of Authority/Identity, Proof of Elapsed Time (PoET). For instance, PoET is less computationally intensive than PoW, however it provides less security guarantees. PoET (Chen et al., 2017) is used in some permissioned networks, where nodes membership is validated by other nodes. In such a private network, one can consider security is not so critical when compared with a typical public permissionless network, such as Bitcoin, which applies PoW consensus.

2.2. Smart contracts

Smart contracts are the BC technology next level by enabling the execution of the terms of a contract on computer nodes running a BC. The smart contract concept was firstly introduced by Nick Szabo in 1994 and is currently applied by Ethereum, as well as by Hyperledger Fabric's chaincode (Dinh et al., 2018). A smart contract can, for instance, execute calculations, perform a service, store information, send funds to other accounts automatically or execute a multi-party transaction. This can provide transparency to business processes, enable data verifiability and improve trust. A smart contract action is automatically triggered when a specific condition in met, hence the encoded algorithm replaces the traditional third-party escrow. This algorithm has to be verified and validated before implementation, knowing that law is code (De Filippi and Hassan, 2018) in a smart contract context.

2.3. Consumer trust and the importance of blockchain

Consumer trust underpins loyalty, commitment, product acceptance and their good long-term relationships with firms and brands (Bozic, 2017). Transparency (Morey et al., 2015) is also related with trust-building (Nilashi et al., 2016), as explicit protection measures of consumers' data (Morey et al., 2015), production transparency, labour conditions and social responsibility (Kang and Hustvedt, 2014) reinforce trust. We have witnessed several organizational transgressions, such as the Volkswagen emissions scandal, the Cambridge Analytica scandal and the 2007′s global financial crisis, leading to breaches in trust (Currie et al., 2018; Gillespie et al., 2014; Kramer and Pittinsky, 2012). A centralized data system can harm trust and confidence of users (Moura and Gomes, 2017) as the central entity can be a single point of failure.

Blockchain trust-free distributed network of nodes and tamper resistance characteristics can contribute to support consumer trust (Beck et al., 2016; Hawlitschek et al., 2018). The near zero possibility to alter previous published blocks without being noticed, digital cryptographic signature of each published information in the ledger and the transparency provided by tracking of information published in a decentralized chain of blocks put together are what bring about BC as a trust-free technology. Hawlitschek et al. (2018) argue that BC technology is able to replace trust in platform providers to some degree, however, raising the issue of trust in algorithms. Trust shifts from third parties to a BC system. Ma et al. (2020) provide a survey on BC trust mechanism applied to the specificities of crowdsourcing services. The trust by design feature of BC is analysed in the context of supply chain management by Imeri et al. (2019). Casino et al. (2019) propose a classification of BC applications based on a literature review of 260 articles and 54 reports. Their analysis classifies BC applications in business and industry, data management, financial, integrity verification, governance, Internet of Things (IoT), health, education, privacy and security. The surveys conducted by Sankar et al. (2017) and Zheng et al. (2017) compare a variety of consensus algorithms. Feng et al. (2019b) address privacy preservation mechanisms in BC. The integration of IoT (Internet of Things) and BC attracts a lot of interest, with several papers addressing, among other issues, the trustfulness of transactions (Dai et al., 2019; Thakore et al., 2019; Wu et al., 2019). Janssen et al. (2020) propose a framework for analysing BC technology adoption considering the relations between institutional, market and technical factors.

To the best of our knowledge none of the published papers address the analysis of the relation between BC technology and consumer trust and transparency. The work of Hawlitschek et al. (2018) is the most closely related to ours. However, they analyse BC technology and trust specifically in the sharing economy, whereas we sought to understand trust in BC from the marketing perspective.

3. Materials and methods

This study aims at answering the proposed research questions through a semi-automated literature analysis approach (Fig. 1). We chose the Scopus database to search for relevant studies, considering it is a well-known and highly reputed source among scholars and academic institutions (Singh et al., 2020). Additionally, publications indexed by the most reputed academic databases, including specialised ones such as the ACM (Association for Computing Machinery) and the IEEE[1] (Institute of Electrical and Electronics Engineers) are indexed in the Scopus database as well. As such, several other literature analysis studies have also adopted Scopus for querying for relevant publications (e.g., Cattelan and Elaine, 2017; Parlina et al., 2020). Additionally, Scopus covers a vaster range of outlets when compared to other scientific databases (e.g., Web of Science) (Abrizah et al., 2013), while at the same time it does not include non-peer reviewed material such as presentations and others as it does Google Scholar, for example. Since our focus is on consumer trust, based on our questions presented in the introduction section, we defined a query to find articles where both "consumer" and "trust" are mentioned, as well as "blockchain". We included other relevant synonyms from different contexts to account for a wider context-lexicon (e.g., "patients" for the case of health). Also, it should be noted that Scopus indexes the title, abstract and keywords from each article. By using those standard sections in scientific literature, it enables to narrow the search to relevant literature in comparison to Google Scholar, which indexes the full text, including the references, which may conceal non-relevant terms, leading to a huge number of hits (Harzing and Alakangas, 2016). Therefore, Scopus was queried (in November 2019) as follows:

TITLE-ABS-KEY ((customer OR consumer OR client OR user OR patient) AND (trust OR transparency) AND blockchain)

The result is a total of 432 articles, which were used for the subsequent steps illustrated in Fig. 1. Considering we aim to uncover trends from the consumer trust perspective, including Marketing application domains is of chief importance, hence we also included the word "marketing" as mandatory initially. However, the corresponding query resulted in just 13 articles, missing many important

[1] https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee_indexing_agreements.pdf

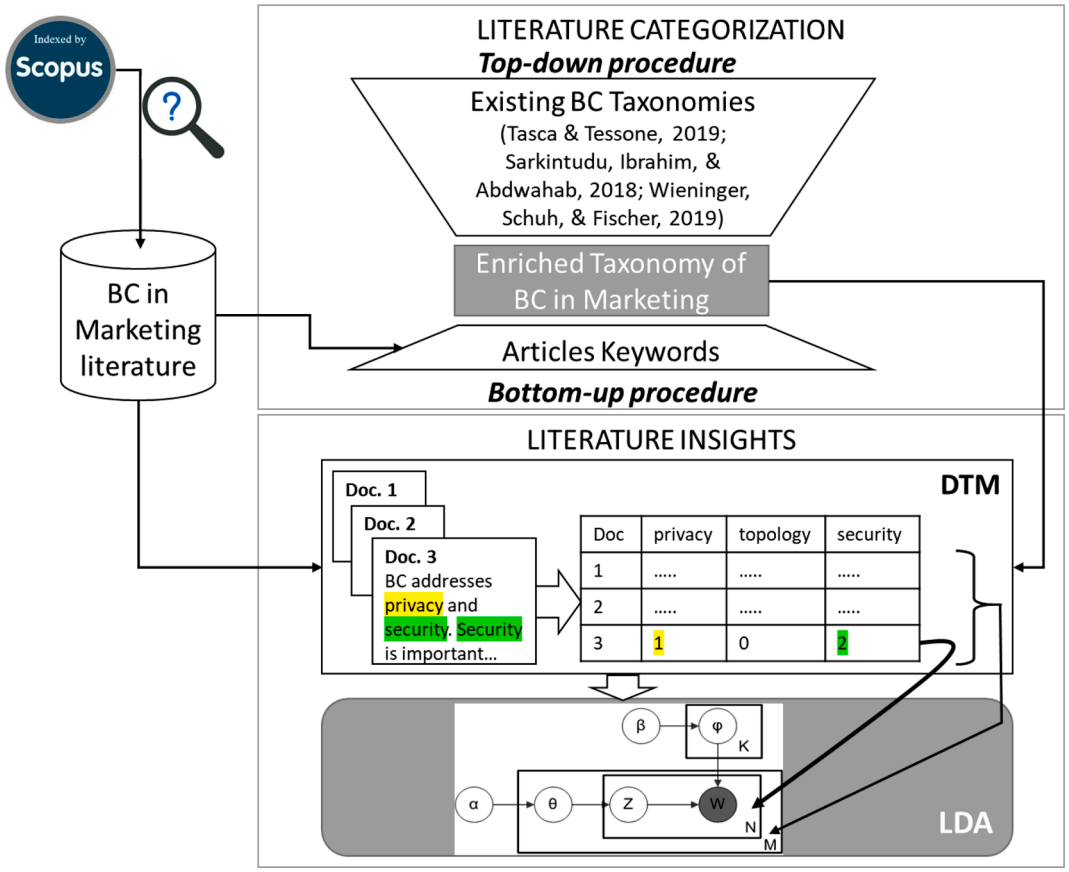

Fig. 1. Experimental approach.

studies (e.g., Grover et al., 2019; Zhao et al., 2019). As so, we then excluded the word "marketing" from our query, in order to cover a wider body of knowledge.

In the first step, the goal is to categorize existing literature using two procedures (Fig. 1). The first is a top-down procedure where key studies in which the authors developed taxonomies for BC are scrutinized. Xu et al. (2017) present a taxonomy categorizing the software architectural characteristics of BC and the impact of the associated design decisions. Our top categorization is partially inspired on the top relevant BC concepts from the existing BC taxonomies (Sarkintudu et al., 2018; Tasca and Tessone, 2019; Wieninger et al., 2019) such as Access Type and Access Control, Network Topology, Storage and Consensus Protocol. We sought to align existing concepts described in the analysed taxonomies from a top-down procedure with the articles gathered. Therefore, we began by gathering all keywords defined by the authors from the collected articles. Then, we organized those keywords according to the relevant categories gathered from the existing BC taxonomies. When the keywords were not related with the available concept taxonomies, we created new categories. This was the case of the following ones: Transaction related, Cryptography/Cryptology/Encryption, Fund raising, Reputation, Autonomy, Auditability. Finally, we pruned the set of BC concepts by defining a dictionary of related terms, that facilitate the process in the next step of organizing the literature we retrieved. Table 1 shows a subset of the resulting enriched taxonomy. To facilitate reading, we organized this table in two main domains: Applications, and Aspects of BC Technologies. We categorised in related terms associated with "other security vulnerabilities", the security aspects other than privacy, integrity and cryptography. Examples of other security vulnerabilities are cybersecurity, authentication, IoT security, reputation and security management, intrusion detection and general data protection regulation, as presented in Table 1. As another example, the category "network topology" includes the following keywords of the gather articles: decentralised, centralised, partially decentralised, peer-to-peer.

As highlighted in Fig. 1, the second step is the extraction of knowledge from the set of articles in the form of a summarized perspective that enables a direct interpretation of the main trends and gaps. Considering the main input is textual contents, we adopted topic modelling. This technique belongs to the text mining umbrella which encompasses approaches and procedures to handle the specificities of textual data (Aggarwal and Zhai, 2012). One of the most commonly used structures within text mining is the document-term matrix (DTM) (Voorhees, 1986). It counts how many times each considered word or term occurs within each document (thus, it is a matrix where each row accounts for each document while each column accounts for each word/term). In our case, each document corresponds to the title and abstract merged together as retrieved from Scopus. Since we aimed specifically at summarizing BC in

Table 1
Subset of the enriched taxonomy.

	Term	Related terms (from the articles keywords)
BC Applications	food	agriculture, farming, food transparency
	finance	cryptocurrency, currency, wallet, ICO, fintech, cryptosystem, authcoin, roamcoin
	health	clinical, medicine
	public administration	public services, governments
	supply chain	supply chain management, cold chain
	transportation	road traffic, vehicle
	tourism	hospitality, hotels
Aspects of BC Technologies	blockchain type	Bitcoin, Ethereum, Hyperledger, Decentralized Autonomous Organizations
	access type and access control	permissionless, permissioned, consortium, attribute access control, access management
	network topology	decentralised, centralised, partially decentralised, peer-to-peer
	transaction related	smart contracts, off-chain transaction
	cryptography, cryptology, encryption	advanced encryption standard, pki, attribute-based signature, cp-abe, cross-domain authentication
	privacy	anonymity, data masking, anonymous credential, privacy-awareness, confidentiality, obfuscation, personal data, data hiding
	integrity	integrity verification, data integrity, data protection, anonymous reputation, piracy
	other security vulnerabilities	cybersecurity, authentication, IoT security, reputation and security management, intrusion detection, general data protection regulation
	traceability	license verification, certificate, verified claims, performance evaluation, verifiability

consumer trust literature, we did not consider all words from all documents. Instead, we used the taxonomy of relevant categories identified in the previous step (Table 1) and the corresponding related terms, in a procedure like the one adopted by Moro et al. (2019). Such procedure also addresses the limitations inherent to having a sparse matrix (Shepherd, 2007), by enabling a concise DTM with 16 columns corresponding to the categories highlighted in Table 1. The DTM is then given as input to the topic modelling algorithm. We adopted the popular latent Dirichlet allocation (LDA) algorithm since it has already been used in similar literature analysis with interesting results (Cheng and Hung, 2018; Evangelopoulos et al., 2012; Müller et al., 2016; Santos et al., 2020). The LDA is a three-level hierarchical Bayesian model, which gathers a set of documents into topics defined by terms (Canito et al., 2018). Fig. 2 shows the mathematical model of LDA, where M denotes the documents, N is the words in a given document, α is the parameter of the Dirichlet prior on the per-document topic distributions, β is the parameter of the Dirichlet prior on the per-topic word distribution, θ_i is the topic distribution for document i, φ_k is the word distribution for topic k, z_{ij} is the topic for the *j*-th word in document i, and w_{ij} is the specific word. Fig. 3 depicts an example of how LDA computes the topics based on the textual contents of a set of documents (Bastani et al., 2019). Additionally, the scheme from Fig. 1 shows how the DTM is computed and then its results are used from the text mining procedure by the LDA. Only the relevant terms selected during the literature categorization procedure are considered. In the example in Fig. 1, for illustration purposes, three terms are identified: privacy, topology, and security. Thus, the DTM contains in each cell the number of occurrences of each term for document (doc.) 3. This structure of term frequency is used by the LDA, with the N parameter consisting in each line of the DTM, and the M in the terms' frequency for the whole documents, as highlighted in Fig. 1.

All the experimental procedure was conducted using the R statistical tool, which is specifically suited for data analysis tasks (Cortez, 2014). Specifically, we adopted the "tm" package for developing the DTM, the "ldatuning" to tune the number of topics which is a given input to LDA, and "topicmodels" to build the topic model.

4. Results and discussion

The 432 articles collected were published in by a total of 73 different publishers. Table 2 shows the publishers that contributed with ten or more articles for the retrieved body of knowledge. Interestingly, specific technology-related publishers such as the IEEE and the ACM are the ones where most of the papers have been published. Such result is an evidence that, even though the search focused specifically on consumer trust, most of the published research so far has been adopting more the technological innovation approach, relegating to a second plan the managerial and social perspectives of trust related adoption of BC.

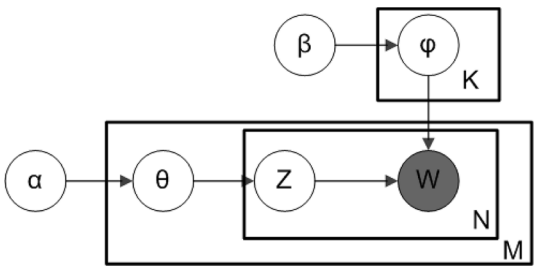

Fig. 2. LDA mathematical model.

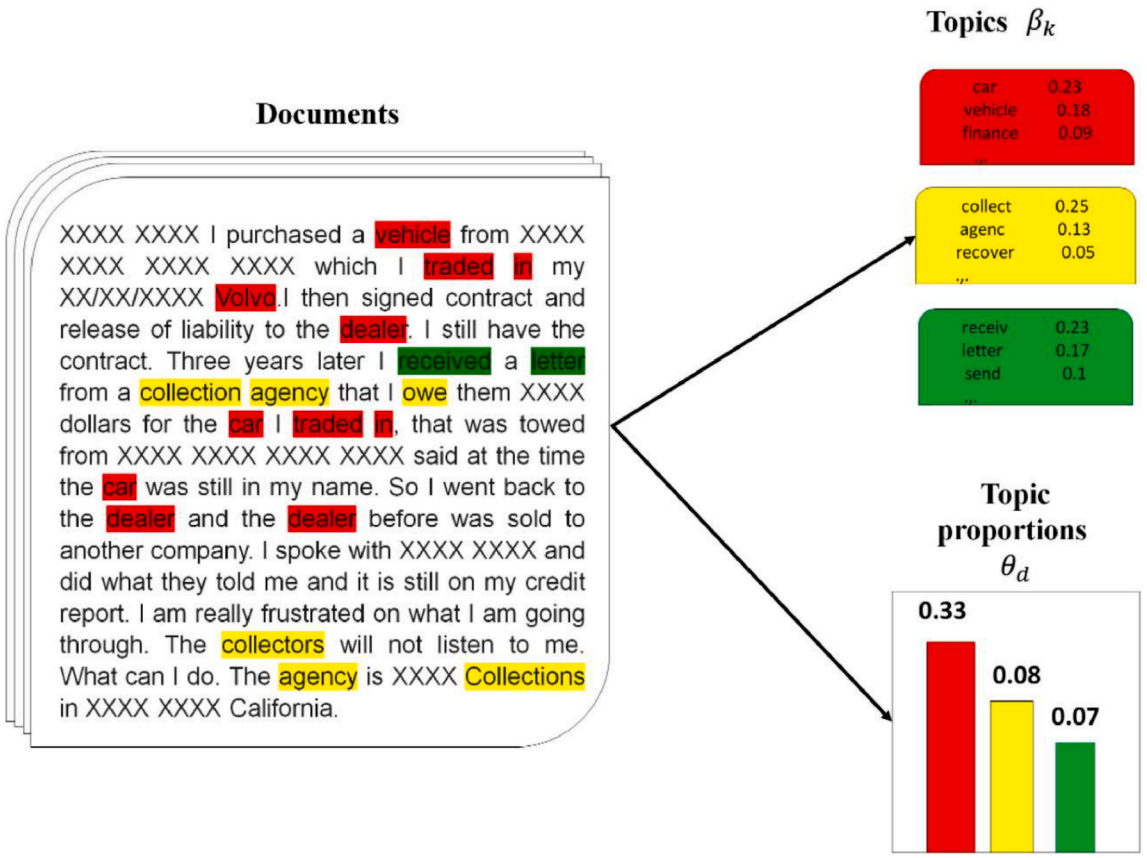

Fig. 3. Illustrative example of LDA components.
Source: Bastani et al., 2019Fig. 4

Table 2
Top contributing publishers.

Publisher		Total
IEEE	176	322
Springer	83	
ACM	30	
Elsevier	22	
MDPI	11	
Others		110
		432

Table 3
Sources with five or more articles.

Source	Total
Lecture Notes in Computer Science	42
Advances in Intelligent Systems and Computing	12
ACM International Conference Proceeding Series	11
IEEE Access	11
Communications in Computer and Information Science	7
IEEE International Conference on Blockchain and Cryptocurrency	6
Lecture Notes in Business Information Processing	6
International Journal of Innovative Technology and Exploring Engineering	5
Studies in Health Technology and Informatics	5
CEUR Workshop Proceedings	5
International Journal of Advanced Computer Science and Applications	5

Table 3 exhibits all sources contributing with five or more articles. The first is the Springer published Lecture Notes in Computer Science, which is a compilation series of conferences articles in computer science and related subjects. Likewise, the second source is also a compilation series of conference proceedings in intelligent systems published by Springer. Only in fourth appears the first journal, IEEE Access, a multidisciplinary journal published by IEEE. In overall, Table 3 confirms the results of Table 2 by highlighting that the focus is being given to the technological innovation, rather than the application of the technology. This is an interesting gap that reveals the marketing, social and economic sciences' researchers are still not devoting noteworthy efforts to the application of BC and its impact to consumer trust.

Fig. 4 shows the trends in the publications of conference and journal articles. We chose these two types of publications because are the ones most represented, in a total of 412 from the 432 articles. It can be observed a steep increase in conference publications between 2016 and 2018, appearing to reach a plateau during 2019. Nevertheless, this result does not mean that conference organizers are paying less attention to BC. For example, the results witness the emergence of the IEEE International Conference on Blockchain and Cryptocurrency, which had its first edition in 2019 and contributed with six articles to our set. The journal publications, with an inherently larger lag of publication, as a result of a generally more demanding peer-review process, and without imposed deadlines as it happens on conferences, only very recently have begun to catch up on BC publications. Yet, the observed increase in 2018 and 2019 suggest the output will continue to increase in the forthcoming years. The results also emphasize the importance of the undertaken literature analysis now that the theme is becoming mainstream.

As previously stated, by tuning the LDA number of topics using the "ldatuning" package, we defined that number to be equal to 15. The execution of the LDA algorithm results in a structure characterized by three dimensions: the topics, the terms that characterize each topic, and the articles (title plus abstract). The relations between topics and articles can be measured by an αdistribution value, while the relations between topics and taxonomy terms is characterized by a βdistribution value. The βrepresents the document-topic density. Thus, a higher αindicates that a document is related to more topics, while a lower αlinks the document to fewer topics. We used the function "topic" from "topicmodels" package to retrieve the topic most closely related to each article. The βrepresents topic-word density, i.e., words with low βin relation to a topic are strongly linked to that topic. We obtained the βs through the "term" function from "topicmodels".

Fig. 5 shows the 15 unveiled topics. The topics are represented by a squared rectangle in the middle of the figure, being numbered from #1 to #15 for referencing purposes. For an easier visual representation of the results, we consider that an article is associated with the topic to which it is best matched to. Thus, within each topic rectangle, we show also the number of articles best matched to that topic. The taxonomy terms that best characterize each topic are represented on the left inside rounded rectangles for the case of the domains of applications, and on the right for the case of aspects of BC technologies. Also, for an easier depicting, we chose to show only the BC technologies' categories with a βbelow or equal to 2.5. For the case of the domains of applications, and since some topics are not so closely related to a domain of application as they are with the BC technologies, we considered only the two domains more closely related to each topic. Also, due to this fact, we included in the figure the most relevant β values so that the reader can see if it is a weaker (higher β value) or a stronger relation (lower β value, i.e., closer to 0). All β values are also presented in Table 4. Thus, as an example, topic #1 has 55 articles that are more closely related to it than to any of the remaining topics. The two most relevant domains of application for topic #1 are "finance" and "supply chain", while the aspects of the BC technologies that best characterize such topic are "BC type" and "access type/control" (Table 1).

Since Fig. 5 became dense due to information richness, to further clarify it, we also detail in Table 4 the terms and values for each of the 15 uncovered topics. Additionally, we show the distribution of articles per topic over the 2014–2019 period. Furthermore, we include word clouds per topic in Fig. 6 to increase readability and interpretability of the results.

Table 5 shows two randomly selected articles that match each of the topics identified in Table 4. For instance, regarding the paper (Dobler et al., 2019) automatically associated with topic #1, where the authors address trust and blockchain in supply chains, we can find the "BC type" term *Bitcoin* (Table 1) mentioned 8 times and the term *Ethereum* 5 times, excluding its references' list. Regarding the

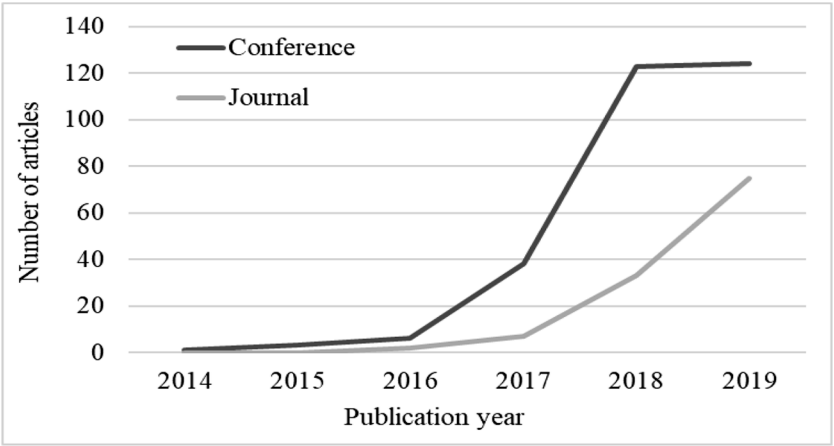

Fig. 4. Publication of articles over the years.

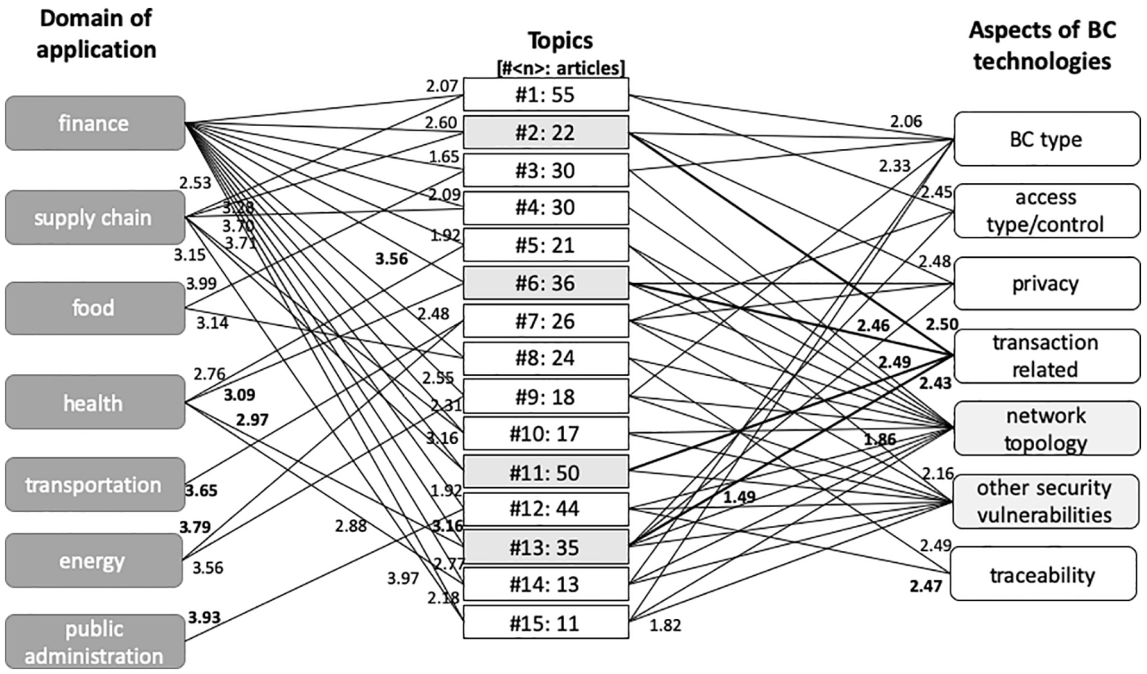

Fig. 5. Discovered topics.

aspect "Access type/control", which also classifies the topic #1, the term *Permissioned* is mentioned 5 times in (Dobler et al., 2019). The paper (Sadhya et al., 2018), where the authors analyse how bitcoin blockchain ensures trust in the technology, is associated with the topic #2. Consequently, going through this paper, we verify the "BC type" term *Bitcoin* is mentioned more than 100 times and the term *Decentralized Autonomous Organization* is detected once. When analysing why the taxonomy term "transaction related" also classifies this paper in the topic #2, we find the related term *Smart Contract* also present one time. Regarding the aspect privacy, the related term *Anonymity* is detected 2 times, while the term *Confidentiality* counts 7 times in (Sadhya et al., 2018). This paper also classifies in the finance domain, where the term *currency* appears 6 times and the word *wallet* is found 16 times.

The Fig. 5 depicts the mainstream aspects of BC technologies and domains of application we found when analysing our results, with the connecting lines between them and the topics helping to answer our research questions.

4.1. RQ1: What are the main aspects of BC technologies and how are these becoming mainstream within consumer trust?

Fig. 5 shows scholars are investing major efforts in two of the BC technological aspects, showing a high density of connecting lines: "network topology", and "other security vulnerabilities". With exception of the first two topics, all the remaining are connected to such aspects of BC technologies. On one hand, this result is natural, considering the category "network topology" includes all different types of network architectures mentioned in the gathered articles: decentralised, centralised, partially decentralised, peer-to-peer (Table 1). On the other hand, all of the reported application domains, except for food, are being concerned with "other security vulnerabilities", i. e. those beyond privacy, integrity and cryptography. We can consider this result is in line with researchers' concerns related with cybersecurity, IoT security, reputation and security management, intrusion detection and general data protection regulation (Finck, 2019).

Additionally, it is possible to observe that, regarding the density of the connecting lines in Fig. 5, from three major security aspects of BC technologies (i.e., "traceability", "privacy", "other security vulnerabilities") directly linked to consumer trust and transparency, "privacy" and, especially, "traceability", are receiving only marginal attention when compared to "other security vulnerabilities".

The analysis of our results show also BC technology appears frequently associated with IoT. For instance, topic #6 with 36 articles and topic #7 with 26 articles are linked to IoT with a β value of 2.51 and of 2.52, respectively. These results are not presented in Fig. 5 or Table 4, to avoid excess of information that would make them more difficult to read. Moreover, as IoT is a system of interconnected objects, not an application domain neither an aspect of BC technologies, we decide to keep it separately. However, it seems BC can help in overcoming some of the IoT challenges, namely decentralization, traceability and reliability (Fernandez-Carames and Fraga-Lamas, 2019). Dai et al. (2019) call this trend blockchain of things (BCoT). IoT is showing to be useful in supporting a multiplicity of domains of application, such as supply chain, logistics, manufacturing, food industry, health care, Internet of vehicles and smart cities.

Unlike other studies conducting literature analyses by applying the LDA, none of the topics discovered are clearly associated to a single term. This result enables to highlight the multidisciplinary nature of BC research within consumer trust. As an example, we can compare the results achieved in Fig. 5 with the corresponding ones presented on Table 6 from the study by (Moro et al., 2015): while in the latter all the uncovered topics are associated to at least one term with a βbelow 1.0 (the lowest of which is 0.08), in our case the

Table 4
Topics discovered in detail.

# topic	Number of Articles	Aspects of BC Technologies				Domain of Application		Year of publication					
		Taxonomy term	03B2	Taxonomy term	β	Taxonomy term	β	2014	2015	2016	2017	2018	2019
1	55	BC type	2.06	access type/control	2.45	finance	2.07	0	0	2	5	22	26
						supply chain	2.53						
2	22	BC type	2.48	privacy	2.48	finance	2.60	0	0	0	1	9	12
		transaction related	2.50			supply chain	3.28						
3	30	network topology	2.21	BC type	2.35	finance	1.65	0	0	0	1	12	17
						food	3.99						
4	30	network topology	2.12	—		finance	2.09	0	1	1	4	13	11
						supply chain	3.70						
5	21	network topology	1.95	other security vulnerabilities	2.16	finance	1.92	0	0	1	5	6	9
						health	2.76						
6	36	network topology	1.68	privacy	2.33	health	3.09	0	0	0	4	13	19
		transaction related	2.46			finance	3.56						
7	26	network topology	1.86	other security vulnerabilities	2.10	transportation	3.65	0	1	2	0	11	12
		access type/control	2.33	privacy	2.45	energy	3.79						
8	24	network topology	2.30	traceability	2.49	finance	2.48	0	0	1	1	5	17
						food	3.14						
9	18	network topology	1.85	other security vulnerabilities	2.30	finance	2.55	1	0	0	0	8	9
		BC type	2.33			energy	3.56						
10	17	network topology	1.87	other security vulnerabilities	2.25	finance	2.31	0	0	0	0	7	10
						supply chain	3.71						
11	50	other security vulnerabilities	2.03	transaction related	2.49	supply chain	3.15	0	0	0	6	23	21
						finance	3.16						
12	44	other security vulnerabilities	1.49	network topology	1.86	finance	1.92	0	1	0	11	15	17
		traceability	2.47			public administration	3.93						
13	35	other security vulnerabilities	2.21	network topology	2.25	health	2.97	0	0	1	7	9	18
		privacy	2.26	transaction related	2.43	finance	3.16						
		access type/control	2.45										
14	13	other security vulnerabilities	2.04	network topology	2.17	finance	2.77	0	0	0	0	4	9
		BC type	2.39			health	2.88						
15	11	other security vulnerabilities	1.82	network topology	2.08	finance	2.18	0	0	0	2	5	4
		BC type	2.29			supply chain	3.97						

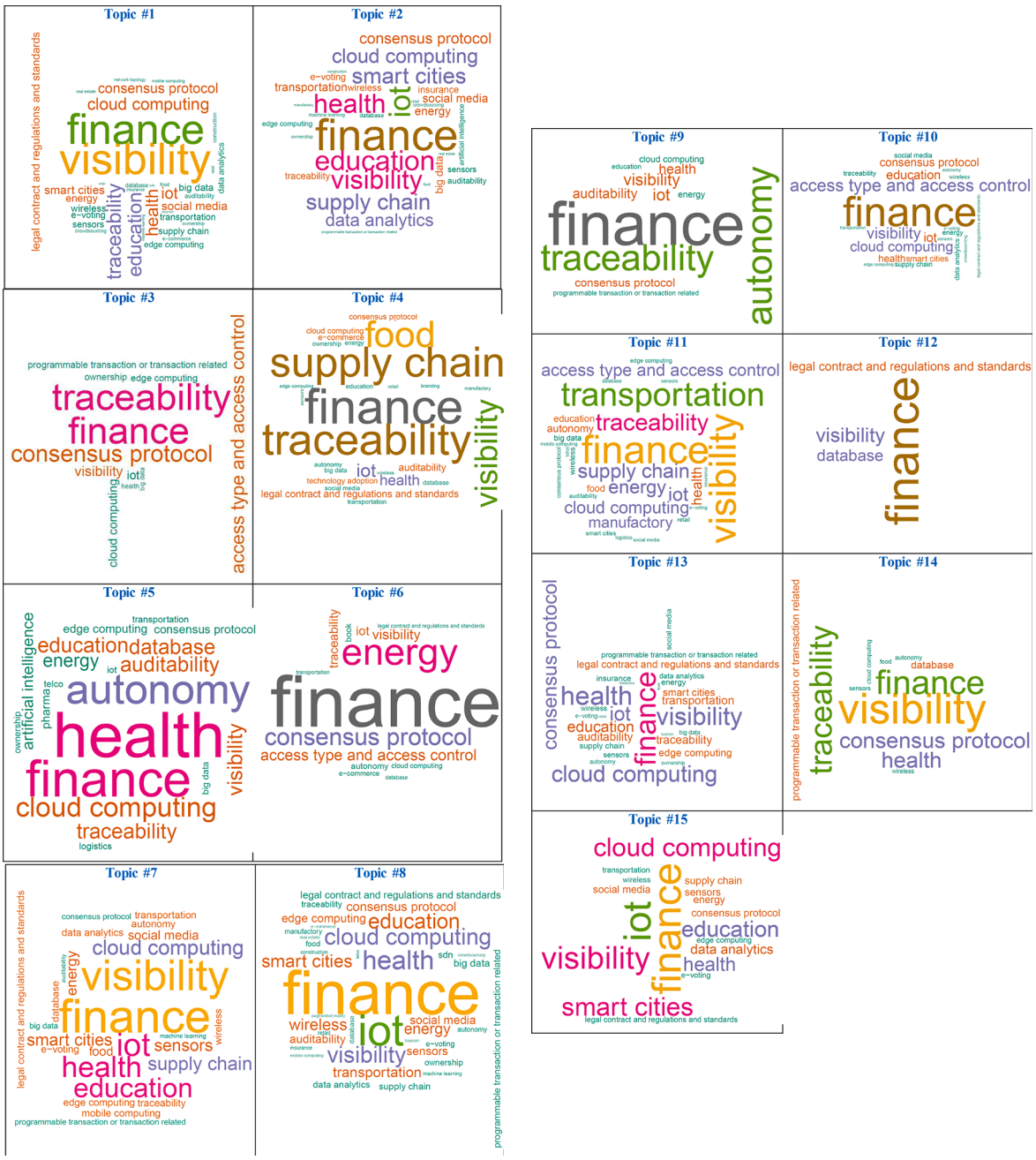

Fig. 6. Word clouds per topic.

collected articles appear more evenly characterised by several terms. As an example, the topic #12 is the one exhibiting the lowest β value of 1.49, regarding the "other security vulnerabilities" aspect of BC technologies. This topic has 44 articles best matching it, and it is also characterised by other aspects of BC technologies with low β values ("network topology": 1.86; "traceability": 2.47) in comparison to the remaining.

Although BC technologies are only being recently studied by the academic community, the timeframe already encompasses six years (2014–2019) of scientific publications. In Fig. 7, we use the values presented in Table 4 to show how the eight topics in which "network topology" is the most significant term (i.e., by showing the lowest β value in comparison to the remaining terms from the same topic) developed over the studied period in terms of the number of publications most closely related to each topic (i.e., topics 3 to 10). Likewise, we also show the evolution of "other security vulnerabilities" BC technology aspect over the same period, since it was the second most relevant one (topics 11 to 15). Fig. 7 shows a significant increase in publications focusing in network topology from 2017 to 2019, whereas the increase is not so steep for "other security vulnerabilities", a key issue regarding consumer trust. Thus, results

Table 5
Examples of articles per topic.

# topic	Examples of articles
1	(Dobler et al., 2019; Wood and Steiner, 2016)
2	(Kubilay et al., 2019; Sadhya et al., 2018)
3	(Buccafurri et al., 2019; Niya et al., 2018)
4	(Kiayias et al., 2017; Li et al., 2018)
5	(Patel, 2019; Zhang and Ma, 2018)
6	(Giordanengo, 2019; Pustišek et al., 2019)
7	(Grüner et al., 2019; Hristov and Hristova, 2019)
8	(Adamik and Kosta, 2018; Linsner et al., 2019)
9	(Almadhoun et al., 2018; Meeuw et al., 2018)
10	(Awwad et al., 2018; Seitz et al., 2018)
11	(Mezquita et al., 2019; Ulybyshev et al., 2018)
12	(Biryukov and Tikhomirov, 2019; Grundmann et al., 2019)
13	(Abdeen et al., n.d.; Benchoufi and Ravaud, 2017)
14	(Duan et al., 2019; Manzoor et al., 2019)
15	(Gruhler et al., 2019; Ku-Mahamud et al., n.d.)

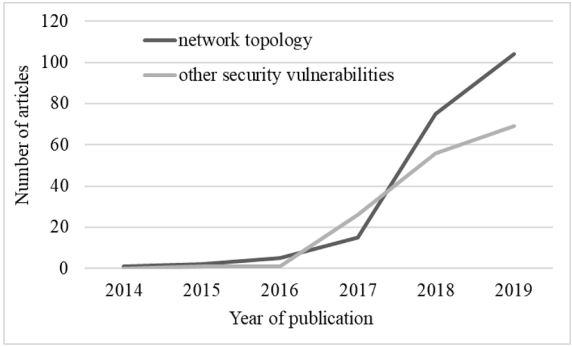

Fig. 7. Publications per year of the two mainstream aspects of BC technologies.

suggest that research regarding network topologies is flourishing, emphasizing the importance of this theme to computer network researchers. Nevertheless, these findings should be interpreted with caution, given the recency of the theme, with the forthcoming years requiring future refreshed literature analyses to confirm the suggested trends.

4.2. RQ2: What are the aspects of BC technologies mostly addressed by the more prominent application domains, beyond the finance area?

In a first overview, we acknowledge that BC literature within consumer trust has become broader, covering a variety of domains of application well beyond its inception domain, i.e., finance. Nevertheless, it is still clear that research in finance emerged earlier, with 14 of the 15 topics being associated to "finance". The exception is topic #7, which is associated with "transportation" and "energy" domains. Beyond finance, the other prominent application domains are supply chain, food, health and to a less extent the public administration domain. This last one has only one connecting line, with topic #12 and a high β value of 3.93. On the other hand, topic #12 is also connected with the following aspects of BC technologies: "network topology" (β value of 1.86), "other security vulnerabilities" (β value of 1.49) and "traceability" (β value of 2.47). This means these aspects of BC technologies were the most relevant to the public administration domain related articles.

The application domain "supply chain" appears connected with topics #1, #2, #4, #10, #11 and #15, with 55, 22, 30, 17, 50 and 11 articles, respectively. This represents a total of 185 articles concerning "supply chain" which were mainly published in 2018 and 2019. Regarding their connection with the aspects of BC technologies, topic #1 highlights "BC type" with a β value of 2.06 and "access type/access control" with a β value of 2.45, whereas topic #2 adds "transaction related" (β value = 2.50) and "privacy" (β value = 2.48). The other "supply chain" concerned topics show more prevalence of a connection with the aspects of BC technologies emphasised in RQ1 already: "network topology", with a β value of 1.87 for topic #10, of 2.08 for topic #15 and of 2.12 for topic #4, as well as "other security vulnerabilities" with a β value of 1.82 for topic #15, of 2.03 for topic #11 and of 2.25 for topic #10. Aside from these two noticeable aspects of BC technologies, these results establish other aspects of BC technologies relevant to the "supply chain" domain, which are "BC type", "access type/access control", "transaction related" and "privacy".

When analysing the health domain, the third most prominent application domain after finance and supply chain, we find it is connected with topic #5 with 21 articles, topic #6 (36 articles), topic #13 (35 articles) and topic #14 (13 articles), which totals 105 papers. On their turn, as the most outstanding aspects of BC technologies for these topics and with a β value below 2 we find again "network topology" with a β value of 1.68 for topic #6 and of 1.95 for topic #5 and "other security vulnerabilities" for topic #15 with a

β value of 1.82. However, the privacy BC aspect is not too far behind for topics #13 (β value of 2.26) and #6 (β value of 2.33). It is also noteworthy to mention the importance of the "transaction related" BC aspect, such as smart contracts and off-chain transactions, for the health application domain, with a β value of 2.43 for topic #13 and of 2.46 for topic #6. Thus, "privacy" and the "transaction related" aspects (Table 1) are becoming prevalent for the health applications, beyond the usual suspects "network topology" and "other security vulnerabilities".

The topics associated with the "transaction related" aspect of BC technologies are #2, #6, #11, and #13 (Fig. 5). All of them are related to "finance". Yet, two of these topics are also related to "supply chain" (#2 with β value of 3.28, #11 with β value of 3.15), while the two remaining are closer to "health" (#6 with β value of 3.09, #13 with β value of 2.97) when compared to "finance" (#6 with β value of 3.56, #13 with β value of 3.16). This is an evidence that transaction related aspects are a major concern for scholars investigating BC applications in both BC emerging application domains, supply chain and health. Also, this result reveals a research gap for the remaining application domains, such as transportation and energy, to which scholars should also pay more attention concerning the specificities of the BC transaction related aspects, such as smart contracts, applied to those domains.

4.3. RQ3: What are the relations between BC application domains and the aspects of BC technologies and how can these associations be useful to the BC research community?

Our results show the topic modelling tool is useful to provide and depict the relations between subjects of a body of knowledge. In the previous RQ we analysed the aspects of BC technologies addressed by the two most prominent application domains after finance. With RQ3 we intend to analyse the relations between the remaining application domains and the aspects of BC technologies addressed by the corresponding topics of articles and how these can be useful to the BC research community. As we were expecting the finance application domain dominates the majority of the topics, accounting for 406 papers. Only topic #7 is not associated with finance. This topic has 26 articles and is related with transportation (with a β value of 3.65) and energy (β value of 3.79) application domains. This exceptional topic is associated with the following aspects of BC technologies: "network topology" (β value of 1.86), "other security vulnerabilities" (β value of 2.10), "access type/access control" (β value of 2.33) and privacy (βalue of 2.45).

The public administration application domain is also an outstanding case, as it is connected only to topic #12 (β value of 3.93), which has 44 articles with 11 of them published in 2017, more than any other topic in this year. Beyond the usual suspects "other security vulnerabilities" (β value of 1.49) and "network topology" (β value of 1.86), public administration articles also address the "traceability" aspect of BC technologies, with a β value of 2.47. This is a very interesting finding, as traceability and provenance are, in our viewpoint, the two most interesting and innovative characteristics brought by BC technologies. Particularly in the public administration domain, being able to provide trustworthy trace back of public procedures and to immutably assure provenance of public sector information can bring about transparency and conduce to increased citizen trust in public institutions (Allessie et al., 2019; de Moura et al., 2020). The only other topic also linked with traceability, with a β value of 2.49, is topic #8 (with 24 articles). This topic links with the food application domain, which includes agriculture and farming, with a β value of 3.14. Indeed, traceability is a driver for BC applications in food domain, namely to guarantee food provenance and conditioning state in cold chains (Tian, 2016). The study of the application of BC to the food domain is nevertheless skimpy. In our analysis, this domain only regards one more topic, i.e. topic #3 with 30 articles, making a total of 54 articles (topics #8 and #3).

These different associations we found between the application domains and the various aspects of the BC technologies lead us to recommend the research community to devote more attention to traceability functionalities brought by BC technologies and to how these can be valued by, in particular, the less addressed domains such as public administration, food, energy and transportation domains (Caro et al., 2018; Chaudhary et al., 2019; Kamilaris et al., 2019; Lei et al., 2017; Li et al., 2019; Wang and Zhang, 2018).

5. Application and limitations of the proposed approach

Our results highlight the multidisciplinary nature of BC research within consumer trust. By means of answering to our research questions we conclude the following. From three major aspects of BC technologies (i.e., "traceability", "privacy", "other security vulnerabilities") directly linked to consumer trust and transparency, "privacy" and, especially, "traceability", are receiving only marginal attention from scholars when compared to the aspect "other security vulnerabilities". Besides the already known finance domain, the other prominent application domains are supply chain, food, health, transportation, energy and to a less extent the public administration domain. The application of BC in the public sector can be useful in a variety of administrative processes, such as notarization, diploma certification and other provenance certification, and as so beneficial for interactions with citizens and businesses (Allessie et al., 2019). Traceability and reliability of BC record-keeping can bring about increased trust in public institutions.

The BC "transaction related" aspect, which in our taxonomy (Table 1) regards smart contracts and off-chain transactions, are a major concern for scholars investigating supply chain and health emerging application domains. We suggest scholars to address the specificities of the BC transaction related aspects applied to less investigated BC application domains, such as transportation and energy.

In our approach, we considered only the Scopus database. This is a limitation of our study because (1) Scopus only indexes finished works, missing important on-going research on this vibrant topic, and (2) other important databases may index works that are missing in Scopus. Yet, it should be noted the wide scope of Scopus which is being used for literature analyses in multiple domains (e.g., Cattelan and Elaine, 2017; Parlina et al., 2020). In the future, we intend to extend our approach to cover other specific databases such as ACM, IEEE, AIS eLibrary repository, EBSCO, which may index works that are not included in Scopus. Additionally, an automated approach such as the one adopted has important limitations. By considering the frequency of specific words within documents, there is

the possibility that, in some cases, those words may have different meanings because of the textual context (e.g., in "this study addresses physical security", the word "security" is likely not relevant within BC). We tried to overcome this limitation by using specific terms that are only mentioned within the contexts encompassed by our analysis, such as "smart contracts" and "off-chain transactions". In future research, context-based analysis can be conducted using techniques such as context-semantic graph for visualization themes (Salloum et al., 2018). Our literature analysis approach is semi-automated because the textual contents of the articles are manually collected, and currently it requires expert intervention to define the taxonomy. A fully automated literature analysis procedure directly from the databases to the model (end-to-end) would require to (1) extract automatically the textual contents of the articles, to (2) automatically identify the relevant lexicon of keywords for a given body of knowledge, and only then to (3) apply topic modelling. We propose in the future that task (1) can be done using web scraping, while task (2) can be accomplished by using the keywords already defined in (Cortez et al., 2018).

6. Future research trends

With regard to recommendations for future research resulting from our analysis, most of the published research so far has been adopting more the technological innovation approach, relegating to a second plan the managerial and social perspectives of trust related issues of BC. Therefore, the marketing, social and economic sciences' researchers should devote efforts to the application of BC and its impact to consumer trust. From a managerial standpoint, our results highlight the lag between technological practice concerns and BC adoption to address such concerns. The results of our analysis also show "privacy" and, especially, "traceability", which are directly linked to consumer trust and transparency, are receiving not enough attention from scholars. Specifically, within consumer trust, traceability is an important issue, namely to supply chain management and transportation (Behnke and Janssen, 2020; Sarpong, 2014). However, the uncovered topics show that it is still not a mainstream line of research. As consumers continue to pressure organizations from many industries for transparency increase (Kang and Hustvedt, 2014), researchers should devote more efforts in understanding the social and psychological effect of providing more meaningful information as a trigger to consumer trust. Specifically, this study calls for further research on the adoption and advertising of adopting BC technologies as these become known to a wider audience as a symbol of trust. BC can incorporate trust by design and this paradigm shift from external third-party rules' verification to built-in trust among participants of a BC network and its impact on consumer trust should be further analysed.

BC advances can, in suitable contexts, elevate information systems to a strategic importance in the modern competitive enterprise and society. Ehrenberg and King (2020) claim BC is a sociotechnical system and learning-by-doing as a necessary condition of long-term BC evolution. The success of BC information systems, i.e. sociotechnical systems involving BC, depends on it addressing the needs of individuals, organizations, institutions and society. A sustainable ecosystem including BC depends on trust.

We envision the following three major areas where blockchain trustability will have further research developments. Alongside with the technological developments, their socioeconomic implications are also to be studied.

6.1. *Self-sovereignty identity mechanisms combined with data analytics and blockchain*

In these times of increasing personal data tracks left by people online while interacting with services, and digital connections generating everyday more data available to analyse, the concept of self-sovereign identities (SSIs) is gaining pace. A digital identity is a means to prove that someone or something is who they claim to be and to differentiate identities, whereas SSI is stated to be based on decentralized identifiers (DIDs) which should be fully under the control of the DID subject, independent from any centralized provider or certificate authority (Mühle et al., 2018; Reed et al., 2020). Alongside with distributed technologies, SSI bodes more user control over her/his data and a more user-centric experience. Future research challenges involve empowering users with self-sovereignty identity, enabling user confidence regarding data markets and data usage control. For instance, how can the user be in control of the data which is produced by the connected objects she/he uses, incorporated in everyday objects such as vehicles and refrigerators, knowing some kind of its fingerprint data can be register in a BC. What SSI mechanisms can provide the user the ownership of the data she/he produces and even to create data aggregation mechanisms she/he can user-friendly control and even be rewarded by providing access to her/his data to third parties, if desired. We expect the future developments in this realm will help to cement user confidence in distributed ledger technologies (DLT). It is therefore expected to see an increase in research related with trust regarding data analytics combined with blockchain (Salah et al., 2019).

6.2. *Blockchain-based web reputation systems*

Blockchain-based web reputation systems are on the rise, providing for instance the tokenization of the reputation (Almasoud et al., 2020; Bellini et al., 2020). These systems enable to replicate reputation values associated with transactions and smart contracts, namely as marketing tools. Several challenges are yet to be addressed in this domain, such as the aggregation of overall reputation or rating values in different smart contracts involving one person or entity; the transfer of the reputation rating between different blockchain types, which needs interoperability protocols; the detection and resolution of reputation fraud and mistrustful actions in a BC-based reputation system. This calls for effective reliable distributed mechanisms of reputation computations based on DLT and interoperability standards.

6.3. Socio-technological governance mechanisms

Blockchain-based systems group components assembled together for a particular purpose and involve a varied set of actors such as distributed ledger designers, programmers, transaction proponents, transaction validators, token holders, end-users, etc. To have confidence in such systems implies to trust in a distributed complex socio-technical hybrid system. Indeed, BC represents composite power dynamics supported by a complex technological infrastructure. Even if of varied type and number, different types of actors involved in the operations, maintenance, usage and regulation of a blockchain-based network can influence its operation, the design of new features and evolution, as pointed out by (De Filippi et al., 2020). This might bring out complex governance problems, for instance when comes to decide who designs, writes, tests and verifies the smart contracts, how to solve disputes, how to select off-chain activities and trusted oracles, and which regulation compliance to respect. As so, BC suitable good governance practices have to be developed and adopted hence, to prevent suspicious actions which could sap the confidence in BC-based systems. To design governance practices respectful of the user confidence and simultaneously uncompromising the decentralized nature of the BC systems, the community has to bear in mind mechanism to avoid plutocracy – domination by a few large operators who control most of the resources – and to avoid technocracy – domination by a few influential stakeholders who steer technological design and development which can have extensive socio-technical implications. Traditional centralized governance practices are insufficient in the BC and DLT realms, which are inherently distributed with polycentric (Thiel and Moser, 2019) decision-making procedures, defined by uneven influence dynamics among multiplex power's clusters. This calls for further and innovative research.

7. Conclusions and perspectives

Following our research questions, we devised a set of keywords and used these to query the Scopus database and obtained a total of 432 articles. We followed a mixed approach (based on top-down and bottom-up procedures) to structure our analysis. The top-down procedure is based on the existing literature on BC taxonomies, whereas the bottom-up procedure drawn from each article's list of keywords extracted from the 432 gathered articles published until November 2019. We established manual links between the BC concepts from the existing taxonomies and the article's list of keywords. Then these articles are automatically analysed by using text mining and topic modelling processes, for which we adopted the popular latent Dirichlet allocation (LDA) algorithm, to uncover relevant topics enabling to analyse the existing body of knowledge. Through such an approach, we seek to contribute to a better understanding of the relations between aspects characterising BC technologies and the dominant BC application domains, from the important consumer trust perspective. We also address the application and some limitations of our approach. We plan to extend our approach to cover other databases such as ACM, IEEE, AIS eLibrary repository, EBSCO, which may index works that are not included in the Scopus database. Resulting from our analysis, some future research trends regarding blockchain trustability are brought out.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by the Fundação para a Ciência e Tecnologia (FCT) within the following Projects: UIDB/04466/2020 and UIDP/04466/2020.

References

Abdeen, M. A. R., Ali, T., Khan, Y., & Yagoub, M. C. E. (n.d.). Fusing Identity Management, HL7 and Blockchain into a Global Healthcare Record Sharing Architecture.
Abrizah, A., Zainab, A.N., Kiran, K., Raj, R.G., 2013. LIS journals scientific impact and subject categorization: a comparison between Web of Science and Scopus. Scientometrics 94 (2), 721–740.
Adamik, F., Kosta, S., 2018. SmartExchange: decentralised trustless cryptocurrency exchange. In: International Conference on Business Information Systems, pp. 356–367.
Aggarwal, C.C., Zhai, C. (Eds.), 2012. Mining Text Data. Springer US, Boston, MA.
Allessie, D., Sobolewski, M., Vaccari, L., Pignatelli, F., 2019. Blockchain for Digital Government 29677. https://doi.org/10.2760/93808.
Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K., 2018. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), pp. 1–8.
Almasoud, A.S., Hussain, F.K., Hussain, O.K., 2020. Smart contracts for blockchain-based reputation systems: A systematic literature review. J. Network Comp. Appl. 170, 102814. https://doi.org/10.1016/j.jnca.2020.102814.
Awwad, M., Kalluru, S.R., Airpulli, V.K., Zambre, M.S., Marathe, A., Jain, P., 2018. Blockchain technology for efficient management of supply chain. In: Proceedings of the International Conference on Industrial Engineering and Operations Management, pp. 440–449.
Ayaburi, E.W., Treku, D.N., 2020. Effect of penitence on social media trust and privacy concerns: the case of Facebook. Int. J. Inf. Manage. 50, 171–181.
Baiyere, A., Salmela, H., Tapanainen, T., Mendling, J., Pentland, B.T., Recker, J., 2020. Digital transformation and the new logics of business process management. Eur. J. Inf. Syst. https://doi.org/10.1080/0960085X.2020.1718007.
Bastani, K., Namavari, H., Shaffer, J., 2019. Latent Dirichlet allocation (LDA) for topic modeling of the CFPB consumer complaints. Expert Syst. Appl. 127, 256–271.
Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS. Research Papers.
Behnke, K., Janssen, M.F.W.H.A., 2020. Boundary conditions for traceability in food supply chains using blockchain technology. Int. J. Inf. Manage. 52, 101969. https://doi.org/10.1016/j.ijinfomgt.2019.05.025.
Bellini, E., Iraqi, Y., Damiani, E., 2020. Blockchain-based distributed trust and reputation management systems: a survey. IEEE Access 8, 21127–21151.
Benchoufi, M., Ravaud, P., 2017. Blockchain technology for improving clinical research quality. Trials 18 (1). https://doi.org/10.1186/s13063-017-2035-z.

Biryukov, A., Tikhomirov, S., 2019. Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. Pervasive Mob. Comput. 59, 101030. https://doi.org/10.1016/j.pmcj.2019.101030.
Bozic, B., 2017. Consumer trust repair: a critical literature review. Eur. Manage. J. 35 (4), 538–547.
Buccafurri, F., Lax, G., Musarella, L., Russo, A., 2019. Ethereum Transactions and Smart Contracts among Secure Identities. DLT@ ITASEC, 5–16.
Canito, J., Ramos, P., Moro, S., Rita, P., 2018. Unfolding the relations between companies and technologies under the Big Data umbrella. Comput. Ind. 99, 1–8.
Caro, M.P., Ali, M.S., Vecchio, M., Giaffreda, R., 2018. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany, IOT Tuscany 2018, 1–4. https://doi.org/10.1109/IOT-TUSCANY.2018.8373021.
Casino, F., Dasaklis, T.K., Patsakis, C., 2019. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inform. 36, 55–81.
Cattelan, G., Elaine, N., 2017. Scientific literature analysis on big data and internet of things applications on circular economy: a bibliometric study. Scientometrics 111 (1), 463–492. https://doi.org/10.1007/s11192-017-2281-6.
Chaudhary, R., Jindal, A., Aujla, G.S., Aggarwal, S., Kumar, N., Choo, K.-K., 2019. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. Comput. Security 85, 288–299.
Chaum, D., 1983. In: Advances in Cryptology. Springer US, Boston, MA, pp. 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18.
Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., Shi, W. (2017). On security analysis of proof-of-elapsed-time (PoET). Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10616 LNCS, 282–297. https://doi.org/10.1007/978-3-319-69084-1_19.
Cheng, C.H., Hung, W.L., 2018. Tea in benefits of health: A literature analysis using text mining and latent dirichlet allocation. In: ACM International Conference Proceeding Series, Proceedings of the 2nd International Conference on Medical and Health Informatics, pp. 148–155. https://doi.org/10.1145/3239438.3239459.
Cortez, P., 2014. Modern Optimization with R. Springer.
Cortez, P., Moro, S., Rita, P., King, D., Hall, J., 2018. Insights from a text mining survey on Expert Systems research from 2000 to 2016. Expert Systems 35 (3), e12280.
Currie, W.L., Gozman, D.P., Seddon, J.J.M., 2018. Dialectic tensions in the financial markets: a longitudinal study of pre- and post-crisis regulatory technology. J. Inf. Technol. 33, 304–325. https://doi.org/10.1057/s41265- 017-0047-5.
Dai, H.-N., Zheng, Z., Zhang, Y., 2019. Blockchain for internet of things: a survey. IEEE Internet Things J. 6 (5), 8076–8094.
De Filippi, P., Hassan, S., 2018. Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday, University of Illinois at Chicago Library, 2016, 21(12).
De Filippi, P., Mannan, M., Reijers, W., 2020. Blockchain as a confidence machine: the problem of trust & challenges of governance. Technol. Soc. 62, 101284 https://doi.org/10.1016/j.techsoc.2020.101284.
Delgado-Ballester, E., Luis, J.Â., Ân, M.-A., 2001. Brand trust in the context of consumer loyalty. Eur. J. Mark. 35 (12), 309–566. https://doi.org/10.1108/EUM0000000006475.
Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J., 2018. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 30 (7), 1366–1385.
Dobler, M., Ballandies, M., Holzwarth, V., 2019. On the Extension of Digital Ecosystems for SCM and Customs with Distributed Ledger Technologies: Requirements Anlysis, Innovation Assessment, and Prototype Design for the Lake Constance Region. In: 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 1–8.
Duan, H., Zheng, Y., Du, Y., Zhou, A., Wang, C., Au, M.H., 2019. Aggregating crowd wisdom via blockchain: A private, correct, and robust realization. In: 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom, pp. 1–10.
Ehrenberg, A.J., King, J.L., 2020. Blockchain in Context. Inf Syst Front 22 (1), 29–35.
Evangelopoulos, N., Zhang, X., Prybutok, V.R., 2012. Latent Semantic Analysis: five methodological recommendations. Eur. J. Inf. Syst. 21 (1), 70–86.
Feng, L., Chiam, Y. K., Lo, S.K., 2018. Text-Mining Techniques and Tools for Systematic Literature Reviews: A Systematic Literature Review. Proceedings – Asia-Pacific Software Engineering Conference, APSEC, 2017-December, 41–50. https://doi.org/10.1109/APSEC.2017.10.
Feng, L., Chiam, Y.K., Lo, S.K., Skute, I., 2019a. Opening the black box of academic entrepreneurship: a bibliometric analysis. Scientometrics 120 (1), 237–265. https://doi.org/10.1007/s11192-019-03116-w.
Feng, Q.i., He, D., Zeadally, S., Khan, M.K., Kumar, N., 2019b. A survey on privacy protection in blockchain system. J. Network Comp. Appl. 126, 45–58.
Fernandez-Carames, T.M., Fraga-Lamas, P., 2019. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. IEEE Access 7, 45201–45218.
Finck, M., 2019. Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? https://doi.org/10.2861/535.
Gillespie, N., Dietz, G., Lockey, S., 2014. Organizational reintegration and trust repair after an integrity violation: a case study. Bus. Ethics Q. 24 (3), 371–410.
Giordanengo, A. (2019). Possible usages of smart contracts (blockchain) in healthcare and why no one is using them.
Grover, P., Kar, A.K., Janssen, M., Ilavarasan, P.V., 2019. Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions – insights from user-generated content on Twitter. Enterprise Inf. Syst. 13 (6), 771–800.
Gruhler, A., Rodrigues, B., Stiller, B., 2019. A reputation scheme for a blockchain-based network cooperative defense. In: IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 71–79.
Grundmann, M., Leinweber, M., Hartenstein, H., 2019. Banklaves: concept for a trustworthy decentralized payment service for Bitcoin. In: IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 268–276.
Grüner, A., Mühle, A., Gayvoronskaya, T., Meinel, C., 2019. A comparative analysis of trust requirements in decentralized identity management. In: International Conference on Advanced Information Networking and Applications, pp. 200–213.
Guo, Y., Liang, C., 2016. Blockchain application and outlook in the banking industry. Financial Innov. 2 (24), 12. https://doi.org/10.1186/s40854-016-0034-9.
Harzing, A.-W., Alakangas, S., 2016. Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison. Scientometrics 106 (2), 787–804.
Hawlitschek, F., Notheisen, B., Teubner, T., 2018. 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.
Hristov, P., Hristova, T., 2019. Explaining The DLT Applications in The Context of a Customers, Facility Managements and Utility Companies Relationship. 2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA), 1–5.
Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V., Akella, V., 2019. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. Int. J. Inf. Manage. 49, 114–129.
Iansiti, M., Lakhani, K. R. (2107). The Truth About Blockchain.
Imeri, A., Agoulmine, N., Feltus, C., Khadraoui, D., 2019. Blockchain: analysis of the new technological components as opportunity to solve the trust issues in supply chain management. Adv. Intelligent Syst. Comp. 998, 474–493. https://doi.org/10.1007/978-3-030-22868-2_36.
Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., Irani, Z., 2020. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. Int. J. Inf. Manage. 50, 302–309.
Kamilaris, A., Fonts, A., Prenafeta-Boldú, F.X., 2019. The rise of blockchain technology in agriculture and food supply chains Vol. 91, 640–652. https://doi.org/10.1016/j.tifs.2019.07.034.
Kang, J., Hustvedt, G., 2014. Building trust between consumers and corporations: the role of consumer perceptions of transparency and social responsibility. J. Bus. Ethics 125 (2), 253–265.
Kiayias, A., Russell, A., David, B., Oliynykov, R., 2017. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Annual International Cryptology Conference, pp. 357–388.

Kramer, R.M., Pittinsky, T.L., 2012. Restoring Trust in Organizations and Leaders: Enduring Challenges and Emerging Answers. In: Restoring Trust in Organizations and Leaders: Enduring Challenges and Emerging Answers. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199756087.0010001.
Ku-Mahamud, K. R., Omar, M., Bakar, N. A. A., & Muraina, I. D. (n.d.). Awareness, Trust, and Adoption of Blockchain Technology and Cryptocurrency among Blockchain Communities in Malaysia.
Kubilay, M.Y., Kiraz, M.S., Mantar, H.A., 2019. CertLedger: A new PKI model with Certificate Transparency based on blockchain. Computers & Security 85, 333–352.
Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C.P.A., Sun, Z., 2017. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J. 4 (6), 1832–1843.
Li, X., Whinston, A.B., 2020. Analyzing Cryptocurrencies. Inf. Syst. Front. 22 (1), 17–22.
Li, Z., Xiao, Z., Xu, Q., Sotthiwat, E., Mong Goh, R.S., Liang, X., 2019. Blockchain and IoT Data Analytics for Fine-Grained Transportation Insurance. In: Proceedings of the International Conference on Parallel and Distributed Systems. https://doi.org/10.1109/PADSW.2018.8644599.
Li, Z., Barenji, A.V., Huang, G.Q., 2018. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. Rob. Comput. Integr. Manuf. 54, 133–144.
Linsner, S., Kuntke, F., Schmidbauer-Wolf, G.M., Reuter, C., 2019. Blockchain in agriculture 4.0-an empirical study on farmers expectations towards distributed services based on distributed ledger technology. In: Proceedings of Mensch und Computer 2019, pp. 103–113.
Ma, Y., Sun, Y., Lei, Y., Qin, N., Lu, J., 2019. A survey of blockchain technology on security, privacy, and trust in crowdsourcing services. World Wide Web 23 (1), 393–419.
Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S.S., Ylianttila, M., 2019. Blockchain based proxy re-encryption scheme for secure IoT data sharing. In: IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 99–103.
Harrison McKnight, D., Choudhury, V., Kacmar, C., 2002. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. J. Strateg. Inf. Syst. 11 (3-4), 297–323.
Meeuw, A., Schopfer, S., Ryder, B., Wortmann, F., 2018. LokalPower: Enabling local energy markets with user-driven engagement. In: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1–6.
Mezquita, Y., González-Briones, A., Casado-Vara, R., Chamoso, P., Prieto, J., Corchado, J.M., 2019. Blockchain-Based Architecture: A MAS Proposal for Efficient Agri-Food Supply Chains. In: International Symposium on Ambient Intelligence, pp. 89–96.
Morey, T., Forbath, T., Schoop, A., 2015. May). Designing for Transparency and Trust. Harvard Business Review, Customer Data, p. 11.
Moro, S., Cortez, P., Rita, P., 2015. Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation. Expert Syst. Appl. 42 (3), 1314–1324.
Moro, S., Pires, G., Rita, P., Cortez, P., 2019. A text mining and topic modelling perspective of ethnic marketing research. J. Business Res. 103, 275–285.
de Moura, L.M.F., Brauner, D.F., Janissek-Muniz, R., 2020. Blockchain and a Technological Perspective for Public Administration: A Systematic Review. Rev. Administr. Contemporânea 24 (3), 259–274. https://doi.org/10.1590/1982-7849rac2020190171.
Moura, T., Gomes, A., 2017. Blockchain voting & its effects on election transparency & voter confidence. ACM International Conference Proceeding Series, Part F1282, 574–575. https://doi.org/10.1145/3085228.3085263.
Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C., 2018. A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. 30, 80–86.
Müller, O., Junglas, I., Brocke, J.V., Debortoli, S., 2016. Utilizing big data analytics for information systems research: challenges, promises and guidelines. Eur. J. Inf. Syst. 25 (4), 289–302.
Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
Nilashi, M., Jannach, D., Ibrahim, O.B., Esfahani, M.D., Ahmadi, H., 2016. Recommendation quality, transparency, and website quality for trust-building in recommendation agents. Electron. Commer. Res. Appl. 19, 70–84.
Niya, S. R., Shüpfer, F., Bocek, T., & Stiller, B. (2018). Setting up flexible and light weight trading with enhanced user privacy using smart contracts. NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, 1–2.
Nofer, M., Gomber, P., Hinz, O., Schiereck, D., 2017. Blockchain. Bus. Inf. Syst. Eng. 59 (3), 183–187.
Pappas, N., 2016. Marketing strategies, perceived risks, and consumer trust in online buying behaviour. J. Retail. Consumer Serv. 29, 92–103.
Parlina, A., Ramli, K., Murfi, H., 2020. Theme Mapping and Bibliometrics Analysis of One Decade of Big Data Research in the Scopus Database. Idc, 1–26. https://doi.org/10.3390/info11020069.
Patel, V., 2019. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics J 25 (4), 1398–1411.
Pilkington, M., 2016. In: Research Handbook on Digital Transformations. Edward Elgar Publishing, pp. 225–253. https://doi.org/10.4337/9781784717766.00019.
Pustišek, M., Umek, A., Kos, A. (2019). Approaching the Communication Constraints of Ethereum-Based Decentralized Applications. Sensors, 19(11), 2647.
Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadell, M. (2020). Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations.
Sadhya, V., Sadhya, H., Hirschheim, R., & Watson, E. (2018). Exploring technology trust in bitcoin: the blockchain exemplar.
Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A., 2019. Blockchain for AI: review and open research challenges. IEEE Access 7, 10127–10149.
Salloum, S.A., Al-Emran, M., Monem, A.A., Shaalan, K., 2018. Using text mining techniques for extracting information from research articles. In: Intelligent natural language processing: trends and applications. Springer, pp. 373–397.
Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, August). Survey of consensus protocols on blockchain applications. 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017. https://doi.org/10.1109/ICACCS.2017.8014672.
Santos, M.R.C., Laureano, R.M.S., Moro, S., 2020. Unveiling research trends for organizational reputation in the nonprofit sector. Voluntas 31 (1), 56–70.
Sarkintudu, S.M., Ibrahim, H.H., Abdwahab, A.B., 2018. Taxonomy development of Blockchain platforms: Information systems perspectives. AIP Conf. Proc. 2016 https://doi.org/10.1063/1.5055532.
Sarpong, S. (2014). Traceability and supply chain complexity: confronting the issues and concerns. European Business Review, 26(3), 271–284. https://doi.org/10.1108/EBR-09-2013-0113.
Seebacher, S., Schüritz, R., 2017. Blockchain technology as an enabler of service systems: A structured literature review. Lecture Notes in Business Inf. Process. 279, 12–23. https://doi.org/10.1007/978-3-319-56925-3_2.
Seitz, A., Henze, D., Miehle, D., Bruegge, B., Nickles, J., Sauer, M., 2018. Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study. In: 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, pp. 182–188.
Shepherd, S.J., 2007. Concepts and architectures for next-generation information search engines. Int. J. Inf. Manage. 27 (1), 3–8.
Singh, V., Verma, S., Chaurasia, S.S., 2020. Mapping the themes and intellectual structure of corporate university: co-citation and cluster analyses. Scientometrics 122 (3), 1275–1302.
Sirdeshmukh, D., Singh, J., Sabol, B., 2002. Consumer trust, value, and loyalty in relational exchanges. J. Market. 66 (1), 15–37.
Tasca, P., Tessone, C.J., 2019. A taxonomy of blockchain technologies: principles of identification and classification. Ledger 4. https://doi.org/10.5195/ledger.2019.140.
Thakore, R., Vaghashiya, R., Patel, C., Doshi, N., 2019. Blockchain - based IoT: a survey. Procedia Comput. Sci. 155, 704–709.
Thiel, A., Moser, C., 2019. Foundational Aspects of Polycentric Governance. In: Governing Complexity. Cambridge University Press, pp. 65–90. https://doi.org/10.1017/9781108325721.004.
Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. 2016 13th International Conference on Service Systems and Service Management, ICSSSM 2016. https://doi.org/10.1109/ICSSSM.2016.7538424.
Ulybyshev, D., Villarreal-Vasquez, M., Bhargava, B., Mani, G., Seaberg, S., Conoval, P., Pike, R., Kobes, J., 2018. (WIP) blockhub: Blockchain-based software development system for untrusted environments. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 582–585.
Van Rijswijk, W., & Frewer, L. J. (2012). Consumer needs and requirements for food and ingredient traceability information. Int. J. Consumer Stud., 36(3), 282–290. https://doi.org/10.1111/j.1470-6431.2011.01001.x.

Voorhees, E.M., 1986. Implementing agglomerative hierarchic clustering algorithms for use in document retrieval. Inf. Process. Manage. 22 (6), 465–476.
Wang, F.Y., Zhang, J.J., 2018. Transportation 5.0 in CPSS: Towards ACP-based society-centered intelligent transportation. In: IEEE Conference on Intelligent Transportation Systems. https://doi.org/10.1109/ITSC.2017.8317905.
Wieninger, S., Schuh, G., & Fischer, V. (2019, June). Development of a Blockchain Taxonomy. Proceedings – 2019 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2019. https://doi.org/10.1109/ICE.2019.8792659.
Wood, G., Steiner, J., 2016. Trustless computing—the what not the how. In: Banking Beyond Banks and Money. Springer, pp. 133–144.
Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., Rong, C. (2019). A Comprehensive Survey of Blockchain: From Theory to IoT Applications and beyond. IEEE Intern. Things J., 6(5), 8114–8154. https://doi.org/10.1109/JIOT.2019.2922538.
Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. Proceedings – 2017 IEEE International Conference on Software Architecture, ICSA 2017. https://doi.org/10.1109/ICSA.2017.33.
Yaga, D., Mell, P., Roby, N., Scarfone, K., 2018. Draft Blockchain Technology Overview (NISTIR-8202). National Institute of Standard and Technology.
Zhang, A., Ma, X., 2018. Decentralized digital certificate revocation system based on blockchain. J. Phys. Conf. Ser. 1069, 012125.
Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., Boshkoska, B.M., 2019. Blockchain technology in agri-food value chain management: a synthesis of applications, challenges and future research directions. Comput. Ind. 109, 83–99.
Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017. https://doi.org/10.1109/BigDataCongress.2017.85.