Internet of Things and Cyber-Physical Systems 4 (2024) 1–18

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems



Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions

Abderahman Rejeb [a,*], Karim Rejeb [b], Andrea Appolloni [a], Sandeep Jagtap [c], Mohammad Iranmanesh [d], Salem Alghamdi [e], Yaser Alhasawi [f], Yasanur Kayikci [g,h]

[a] Department of Management and Law, Faculty of Economics, University of Rome Tor Vergata, Via Columbia, 2, Rome, 00133, Italy
[b] Faculty of Sciences of Bizerte, University of Carthage, Tunis, Tunisia
[c] Sustainable Manufacturing Systems Centre, School of Aerospace, Transport and Manufacturing, Cranfield University, Cranfield, MK43 0AL, UK
[d] School of Business and Law, Edith Cowan University, Joondalup, WA, Australia
[e] Digital Transformation and Information Department Institute of Public Administration (IPA), Saudi Arabia
[f] Management Information System Department King Abdulaziz University (KAU), Saudi Arabia
[g] Sheffield Business School, Sheffield Hallam University, Sheffield, UK
[h] Science Policy Research Unit, University of Sussex Business School, Brighton, UK

ARTICLE INFO

Keywords:
Internet of things
Blockchain technology
Supply chain management
Healthcare
Energy
WSN
Security
Topic modeling

ABSTRACT

As the fusion of the Internet of Things (IoT) and blockchain technology advances, it is increasingly shaping diverse fields. The potential of this convergence to fortify security, enhance privacy, and streamline operations has ignited considerable academic interest, resulting in an impressive body of literature. However, there is a noticeable scarcity of studies employing Latent Dirichlet Allocation (LDA) to dissect and categorize this field. This review paper endeavours to bridge this gap by meticulously analysing a dataset of 4455 journal articles drawn solely from the Scopus database, cantered around IoT and blockchain applications. Utilizing LDA, we have extracted 14 distinct topics from the collection, offering a broad view of the research themes in this interdisciplinary domain. Our exploration underscores an upswing in research pertaining to IoT and blockchain, emphasizing the rising prominence of this technological amalgamation. Among the most recurrent themes are IoT and blockchain integration in supply chain management and blockchain in healthcare data management and security, indicating the significant potential of this convergence to transform supply chains and secure healthcare data. Meanwhile, the less frequently discussed topics include access control and management in blockchain-based IoT systems and energy efficiency in wireless sensor networks using blockchain and IoT. To the best of our knowledge, this paper is the first to apply LDA in the context of IoT and blockchain research, providing unique perspectives on the existing literature. Moreover, our findings pave the way for proposed future research directions, stimulating further investigation into the less explored aspects and sustaining the growth of this dynamic field.

1. Introduction

The significant influence of technology has woven itself into the social fabric of society, ushering in transformative changes. Over the past few decades, technological advancements have instigated profound shifts in our lifestyle, reshaping the way we live, work, and communicate [1–3]. These developments have seeped into every aspect of our existence, creating an era characterized by heightened connectivity and data-centric decision-making [4]. The Internet of Things (IoT) stands as a testament to this technological revolution, representing a paradigm that morphs ordinary objects into smart, interconnected devices [5–8]. IoT encompasses an extensive network of physical objects, from simple household appliances such as thermostats and refrigerators, to complex industrial machinery. These items are equipped with sensors, software, and various technologies designed to collect and share data over the internet [4]. This digital connectivity engenders an ecosystem where the efficiency, convenience, and utility of these objects are remarkably improved. The ascendancy of IoT has been fueled by the digital

* Corresponding author.
E-mail addresses: abderrahmen.rejeb@gmail.com (A. Rejeb), karim.rejeb@fsb.ucar.tn (K. Rejeb), andrea.appolloni@uniroma2.it (A. Appolloni), s.z.jagtap@cranfield.ac.uk (S. Jagtap), m.iranmanesh@ecu.edu.au (M. Iranmanesh), ghamdisa@ipa.edu.sa (S. Alghamdi), yalhasawi@kau.edu.sa (Y. Alhasawi), Y.Kayikci@shu.ac.uk (Y. Kayikci).

https://doi.org/10.1016/j.iotcps.2023.06.003
Received 28 May 2023; Received in revised form 13 June 2023; Accepted 18 June 2023
Available online 19 June 2023
2667-3452/© 2023 The Author(s). Published by Elsevier B.V. on behalf of KeAi Communications Co., Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

revolution [9] and the pervasive reach of internet connectivity [10], leading to its exponential popularity. At its core, IoT embodies the concept of ubiquitous computing, which envisions computing as an integral, almost invisible part of our lives. It is designed to operate seamlessly in the background, assisting humans with a myriad of tasks and decisions [11]. IoT applications are not limited to a single sector but span a multitude of areas and demonstrate the flexibility and adaptability of this concept. For example, in households, IoT is transforming mundane tasks through smart home systems [12].

According to Ref. [13], these systems manage energy consumption, automate home security, and even control home appliances, which can be monitored and controlled remotely. The introduction of IoT into smart homes has brought about a new level of convenience, control, and efficiency, and fundamentally altered the way people live. In the industrial sector, IoT is revolutionizing complex processes such as predictive maintenance in manufacturing. Traditional maintenance strategies relied heavily on scheduled inspections and repairs, which were often inefficient and costly. With IoT, however, sensors embedded in machinery can monitor performance data in real-time and predict potential failures before they occur [14]. This not only reduces downtime but also extends the lifespan of the machinery, leading to significant cost savings and improved efficiency [5]. Furthermore, IoT is making considerable strides in sectors such as healthcare, transportation, and urban planning [11]. state that IoT devices like wearables and remote monitoring tools empower patients with more control over their health, providing real-time information [15]. argue that the technology has paved the way for intelligent transportation systems due its ability to enhance traffic management, reduce fuel consumption, and enable autonomous vehicles. In the context of urban planning [16], highlight that IoT can serve as the foundation for the development of smart cities, where resources and services are optimized through data collected from citizens, devices, and assets.

While IoT brings many benefits, it also introduces a range of challenges that need to be effectively addressed. The rapid development of the technology and the surge in interconnected devices have given rise to considerable privacy, security, and management issues. As such, IoT devices collect, process, and transmit vast volumes of data [5]. Often of a sensitive nature, this data can range from personal information like health records from smart wearables to critical business data from industrial machinery [11]. The sheer volume and variety of data these devices generate make data management significant challenges. It involves not just storing and processing this data but also ensuring its integrity, authenticity, and availability at all times [17]. Moreover, privacy concerns also arise as more and more personal information is collected and transmitted by IoT devices [18]. In a world where data has become a valuable commodity, the protection of personal information is paramount. However, the use of IoT requires data from various aspects of a user's life to be constantly generated and transmitted, thereby potentially exposing users to privacy breaches [19]. Security is also one of the most pressing issues faced by IoT. The interconnected nature of IoT devices inherently makes them vulnerable to cyber-attacks [20]. Hackers can exploit weak security in one device to gain access to the network and compromise other connected devices [21]. Such breaches can have devastating consequences, especially in critical applications such as infrastructure or healthcare. Therefore, there is a need to overcome these challenges by introducing robust and innovative solutions that can safeguard the data, enhance privacy, and ensure the security of the IoT ecosystem [22]. This is where blockchain technology comes to the fore.

Blockchain is originally devised for the digital currency, Bitcoin, but it has evolved beyond its initial application, revolutionizing various sectors of the economy [22]. Blockchain is a type of distributed ledger technology that stores data across multiple systems in a way that is secure, transparent, and immutable [23]. The security feature of blockchain comes from its cryptographic algorithms and the decentralized nature of its network [24]. Each block in a blockchain is linked to then previous one through a cryptographic hash function, making it nearly impossible to alter data once it is recorded. Due to the fact that data is stored across a network of computers rather than a central server, it is difficult for hackers to compromise the system [25]. The transparent and immutable nature of blockchain makes it an ideal solution for data management and privacy concerns in IoT [26]. Transparency ensures that all transactions are open for verification by all participants, which enhances trust and collaboration [23]. Meanwhile, the immutability of blockchain ensures the integrity of data as it prevents any alteration of recorded data [27]. The combination of IoT and blockchain has potential applications in diverse areas, from creating secure, efficient supply chains to improving data privacy in smart homes.

The integration of IoT and blockchain has been attracting growing interest not only from industry practitioners looking to leverage these technologies for practical applications but also from the academic community. The burgeoning interest is underpinned by the recognition that the convergence of these two transformative technologies has the potential to catalyze innovation and technologies progress and shape the digital landscape of the future. Academia has seen an increasing number of studies focusing on the intersection of IoT and blockchain. The surge in academic attention is indicative of the perceived significance and potential impact of these technologies when used in tandem. Numerous review studies have been conducted in this domain, each contributing to the cumulative understanding of the subject matter. For instance, Ref. [28] conduct an extensive examination of current blockchain protocols utilized in IoT networks and propose a classification of threat models addressed by blockchain technology. Ref. [29] review the possibilities of integrating blockchain and IoT to drive innovation in business models. Their findings reveal that incorporating blockchain into the IoT framework enables the establishment of a secure decentralized architecture, thereby enhancing existing businesses and facilitating the development of new business models by eliminating the reliance on third-trust parties.

Moreover, Ref. [30] investigate the current state of blockchain applications in the IoT domain and identify key research areas that enable blockchain to ensure security in large-scale distributed environments. The authors find that the potential of blockchain, specifically smart contracts, can improve the dependability and scalability of IoT applications by establishing trust for data and executed processes. Ref. [31] make a comprehensive review of how blockchain can be adapted to meet the unique demands of IoT, specifically in the development of blockchain-IoT applications, and find that blockchain can offer seamless authentication, data privacy, security, resistance to attacks, ease of deployment, and self-maintenance within the IoT context. Finally, Ref. [27] explore the role of blockchain in addressing data security concerns in IoT and highlight the challenges it faces in the IoT context. Despite this influx of research, a noticeable gap in the literature emerges upon closer inspection. While these review studies have provided valuable insights into the intersection of IoT and blockchain technology, none have utilized a comprehensive sample of journal articles and employed analytical methods, such as Latent Dirichlet Allocation (LDA). Theoretically, LDA is a sophisticated machine learning algorithm used for topic modeling, which allows for the discovery of abstract topics within a large collection of documents [32]. This method could offer a nuanced understanding of the main thematic structures of the body of literature concerning IoT and blockchain integration. Regrettably, the application of LDA in this context remains limited. The current body of review studies, although valuable, might not fully capture the breadth and depth of this rapidly evolving field without the comprehensive and nuanced analysis that methods like LDA can provide [33]. Therefore, there is a compelling need for review studies employing such sophisticated methods to contribute to both theory and practice in this exciting intersection of IoT and blockchain technology.

The subsequent sections of this article are organized as follows: Section 2 presents the research method used in this study. Section 3 offers a summary of the review's findings. Section 4 analyzes the topics identified through the LDA approach. Finally, the article concludes by discussing the summary and limitations of the review.

2. Research method

This article employs a three-tiered hierarchical Bayesian model known as Latent Dirichlet Allocation (LDA) [34]. In theory, LDA comprises a set of algorithms designed to detect and tag the topics present in extensive text collections. It operates under the assumption that each document within the collection is a mixture of various topics, each characterized by a specific word distribution [35]. The objective of LDA is to uncover these latent topics by analyzing word patterns and co-occurrences across the documents. By utilizing LDA, analysts can generate K topics denoted as βK, representing probability distributions over terms in a set of texts using the vocabulary V. A notable strength of the LDA method lies in its ability to quickly and automatically extract relevant themes and patterns from vast volumes of text data. Consequently, we chose to use LDA in this study as it allows for a systematic and unbiased examination of an extensive corpus of literature, as demonstrated in previous research [33,36]. The tasks of statistical computing, graphical design, and natural language processing (NLP) were carried out utilizing the programming languages R and Python.

2.1. Literature selection

This study harnesses the power of text mining by extracting information exclusively from abstracts of chosen publications, specifically those addressing the synergy between IoT and blockchain technology. As in previous research utilizing LDA [37], our analysis primarily hinges on abstract-level scrutiny to yield insights into the intertwined nature of these two groundbreaking technologies. This method ensures that we encapsulate relevant information concerning the overlapping applications of IoT and blockchain technology. By dissecting abstracts, we are able to identify a broad spectrum of topics, trends, and insights that might otherwise be concealed. As a result, our examination offers a more comprehensive exploration of the potential advantages and challenges intertwined with the intersection of IoT and blockchain technology. To gather pertinent publications, we turned to the well-regarded Scopus database, which is renowned for its inclusive coverage of academic studies. On April 1st, 2023, we conducted searches in Scopus using the following search query: ("internet of things" OR iot OR rfid OR wsn OR "wireless sensor network*" OR gps OR actuator* OR sensor*) AND (blockchain* OR "block-chain*" OR "block chain*") [4].

The terms within the first set of parentheses are used to find publications related to IoT. These terms encompass the broad category of IoT, including specific aspects such as Radio-Frequency Identification (RFID), Wireless Sensor Network (WSN), GPS, actuators, and sensors. The AND operator is used to ensure that the search results include both the IoT-related and the blockchain-related terms. The second set of parentheses are used to find publications related to blockchain technology. The Asterisk (*) is a wildcard symbol that allows the search to include variations of the term. For example, "blockchain*" would include "blockchain", "blockchains", "blockchain-based", and so on. By using these two sets of terms together with the AND operator, the search query will return only those publications that contain at least one term from each set, thereby ensuring that the publications are relevant to the interplay between IoT and blockchain technology. In line with previous research [38], we restricted our investigation to articles written in English to ensure the academic integrity of the information procured. We aimed for an exhaustive exploration of the intersection of IoT and blockchain within the academic literature, hence our decision to focus exclusively on journal articles for our ultimate assessment. This selection ensured the acquisition of high-quality and peer-reviewed insights, offering a holistic overview of the research landscape. Emphasizing journal articles also maintained a rigorous standard in our understanding of IoT and blockchain's intersection while capturing a broad picture of the current research status and identifying existing knowledge lacunas.

2.2. Data pre-processing for LDA analysis

Prior to embarking on the unsupervised LDA analysis, it was essential to pre-process the amassed text data relating to the integration of IoT and blockchain technology. Initial steps involved the removal of newline characters, Uniform Resource Locator (URL), punctuations, and other miscellaneous symbols. Subsequently, the open-source Python library, Gensim, was utilized to transform the text by eliminating verbs, adverbs, adjectives, and stop words. To enhance the precision our analysis, a tailored set of stop words was formulated by supplementing the default Gensim list with additional irrelevant terms pertaining to our specific context. Finally, the Gensim library was employed to disassemble phrases into discrete words and assign them distinctive identifiers (IDs). By adhering to this systematic approach, we could not only enumerate the frequency of individual words across the texts but also assess their relative significance within the context of blockchain and IoT interplay.

2.3. Development of the LDA model and identification of optimal K number of topics

The construction of an effective lexicon is a pivotal step in developing the LDA model and deciphering themes from the texts concerning IoT and blockchain. The 'id2word' function from the Gensim package allows for the creation of a vectorized bag of words swiftly and effortlessly. Subsequently, the Mallet toolset, known for its versatility in clustering, topic modeling, and document classification, was employed to build the LDA model [39]. Mallet is a valuable instrument for analyzing data and gleaning insights. The modeling process necessitates various configurations. For this study, Mallet was used to execute multiple simulated LDA models, each comprising different numbers of topics. The optimal number of topics was determined using the topic coherence score, which evaluates the coherence of a topic by scrutinizing the relationships among its constituent words.

In essence, this metric assigns a numerical score to each topic that echoes the extent to which its words correlate and form a cohesive theme. A higher coherence score signifies a stronger interrelation among the words within a topic and indicate their significant contribution to the theme. This is desirable for accurate and precise topic modeling. Fig. 1 illustrates the coherence scores produced by the unsupervised learning system. Guided by the principle of coherence score, the most effective LDA model would be one that possesses the highest and most consistent score because this indicates greater semantic coherence within each topic. The outcomes reveal that after implementing 14 topics, the model reaches a mean value of 0.4393, suggesting that incorporating more than 14 topics would not yield additional valuable insights. Consequently, the

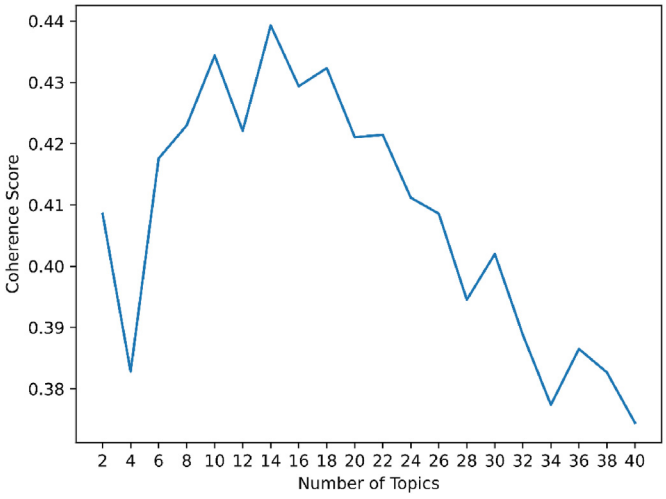


Fig. 1. Coherence scores plot.

model with 14 topics was selected as the ideal choice for analysis based on the coherence scores generated during the LDA modeling process. Table 1 presents the coherence scores for all the assessed topic numbers.

2.4. Identification of topics

The LDA model is a type of probabilistic model utilized to unearth topics from a collection of documents [40], in our case, those related to the integration of IoT and blockchain technology. In the graphical representation shown in Fig. 2, rectangles are depicted as replicates, with 'M' representing documents and 'N' indicating the occurrence of a topic within each document. The distribution of observed words, marked as 'w', is predicated upon the topic distribution, signified as 'z'. In this model, 'β' denotes the distribution of words across topics, 'θ' signifies the distribution of topics across documents, and 'α' illustrates the distribution of words within individual topics. We employed the LDA model to identify the frequency at which the fourteen topics gleaned from the literature were discussed in the chosen journal articles. We adopted the semantic coherence approach to quantify the frequency of topic-associated terms present in the abstract of each article. Through an inductive process based on the semantic coherence score, two researchers independently curated a set of articles for each topic. This allowed the LDA model to highlight latent topics unique to each document, along with their relevance and frequency across the texts, thereby shedding light on the current state of research regarding the intersection of IoT and blockchain technology. The LDA model was derived from all abstracts and analyzed using several Python packages. PyLDAvis was employed to ascertain the average distance between topics and the ten most significant terms within our dataset. Additionally, the Matplotlib library was used to graphically depict the research findings and enhance the clarity and understanding of the results.

2.5. Bibliometric analysis

To gain deeper insights into the significance of the chosen journal articles on IoT and blockchain technology, a bibliometric analysis was carried out. We employed the bibliometric R package to execute the methodology proposed by Ref. [41]. This tool simplifies the process of discovering links between academic papers, thereby enabling researchers to thoroughly understand the underlying networks and themes within the data. Our study primarily aimed to conduct performance analysis and scientific mapping, both of which were achieved through the use of bibliometric methods. As elaborated by Ref. [42], the former allows for intricate scrutiny of scholarly collaborations and research output, while the latter facilitates the comprehension of the genesis and development of a specific research domain—in this case, the intersection of IoT and blockchain technology.

3. Findings

3.1. Descriptive results

The objective of the bibliometric analysis was to delve into the prominent academic journals exploring the interplay between IoT and blockchain technology. Table 2 showcases pertinent data derived from the selected articles that form part of this study. A noteworthy revelation from the results is that, on average, each article garnered 25.85 citations annually. This suggests a substantial level of interest and interaction within the research community, indicating that the amalgamation of IoT and blockchain technology is garnering considerable scholarly attention. The relatively high average citation rate per year might also imply the pertinence and caliber of the ongoing research in this domain, as well as the potential influence of IoT and blockchain integration on various fields of application. In addition, the data in the table uncovers a collaboration index of 2.33. This measure assesses the degree of cooperative endeavors among researchers within a specific domain. In this context, it signifies the average number of authors per article in the literature concerning the intersection of IoT and blockchain technology. This collaboration index can be construed as researchers synergizing in small to medium-sized groups to address the multifaceted aspects of IoT and blockchain integration. It may also suggest that the field is interdisciplinary in nature, with scholars from diverse backgrounds and areas of expertise uniting to tackle complex challenges (see Table 3).

In analyzing the robust and dynamic landscape of research on the convergence of IoT and blockchain technology, it is crucial to consider the remarkable expansion and evolution over time. Spanning the seven-

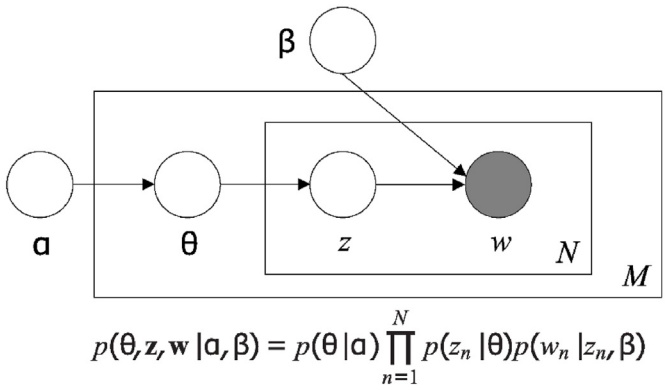


Fig. 2. LDA model representation [40].

Table 1
Value of coherence score per number of topics.

Number of Topics	Coherence score	Number of Topics	Coherence score
2	0.4085	22	0.4214
4	0.3828	24	0.4112
6	0.4176	26	0.4086
8	0.4230	28	0.3945
10	0.4344	30	0.4020
12	0.4221	32	0.3888
14	**0.4393**	34	0.3774
16	0.4294	36	0.3865
18	0.4323	38	0.3827
20	0.4211	40	0.3744

Table 2
Main bibliometric results.

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2016:2023
Sources (Journals)	864
Documents	4455
Average years from publication	1.8
Average citations per documents	25.85
Average citations per year per doc	6.648
References	225885
DOCUMENT TYPES	
article	3936
review	519
DOCUMENT CONTENTS	
Keywords Plus (ID)	13341
Author's Keywords (DE)	7944
AUTHORS	
Authors	10034
Author Appearances	18939
Authors of single-authored documents	217
Authors of multi-authored documents	9817
AUTHORS COLLABORATION	
Single-authored documents	244
Documents per Author	0.444
Authors per Document	2.25
Co-Authors per Documents	4.25
Collaboration Index	2.33

Table 3
LDA model results.

Topic	Keywords	Theme
1	0.027*"scheme" + 0.025*"security" + 0.020*"authentication" + 0.019*"device" + 0.018*"blockchain" + 0.016*"IoT" + 0.013*"attack" + 0.013*"key" + 0.013*"protocol" + 0.012*"data" + 0.012*"communication" + 0.010*"secure" + 0.010*"network" + 0.007*"signature" + 0.006*"user"	Security and authentication in blockchain-based IoT networks
2	0.043*"IoT" + 0.026*"access" + 0.022*"control" + 0.022*"blockchain" + 0.017*"system" + 0.013*"agricultural" + 0.010*"device" + 0.008*"management" + 0.008*"data" + 0.007*"smart" + 0.007*"resource" + 0.006*"technology" + 0.006*"model" + 0.006*"contract" + 0.005*"platform"	Access control and management in blockchain-based IoT systems
3	0.029*"technology" + 0.016*"blockchain" + 0.015*"chain" + 0.013*"supply" + 0.013*"digital" + 0.009*"industry" + 0.008*"AI" + 0.007*"IoT" + 0.006*"management" + 0.006*"industry 4.0" + 0.006*"development" + 0.006*"review" + 0.006*"business" + 0.006*"process" + 0.006*"application"	Blockchain and IoT integration in supply chain management
4	0.054*"learning" + 0.025*"model" + 0.022*"data" + 0.021*"federated" + 0.019*"system" + 0.015*"machine" + 0.014*"privacy" + 0.013*"detection" + 0.012*"deep" + 0.011*"blockchain" + 0.010*"accuracy" + 0.008*"framework" + 0.008*"training" + 0.007*"technique" + 0.006*"smart"	Federated learning and blockchain in smart systems
5	0.041*"data" + 0.022*"smart" + 0.020*"blockchain" + 0.014*"system" + 0.012*"contract" + 0.011*"service" + 0.010*"user" + 0.009*"IoT" + 0.008*"trust" + 0.008*"device" + 0.007*"management" + 0.007*"privacy" + 0.006*"security" + 0.006*"information" + 0.005*"IIoT"	Blockchain in IoT and IIoT for data security and privacy
6	0.049*"consensus" + 0.036*"algorithm" + 0.028*"node" + 0.018*"blockchain" + 0.017*"IIoT" + 0.016*"network" + 0.016*"mechanism" + 0.016*"transaction" + 0.011*"fault" + 0.011*"performance" + 0.010*"problem" + 0.008*"model" + 0.008*"tolerance" + 0.008*"protocol" + 0.008*"efficiency"	Blockchain consensus algorithms and security in IIoT
7	0.034*"edge" + 0.031*"computing" + 0.017*"resource" + 0.017*"model" + 0.016*"blockchain" + 0.016*"IoT" + 0.014*"network" + 0.014*"data" + 0.010*"device" + 0.010*"cloud" + 0.009*"task" + 0.009*"fog" + 0.009*"user" + 0.009*"service" + 0.008*"time"	Blockchain and edge computing in IoT
8	0.062*"data" + 0.027*"blockchain" + 0.016*"system" + 0.016*"IoT" + 0.013*"security" + 0.012*"healthcare" + 0.011*"access" + 0.010*"privacy" + 0.008*"patient" + 0.008*"information" + 0.008*"medical" + 0.008*"sharing" + 0.008*"storage" + 0.008*"control" + 0.007*"health"	Blockchain in healthcare data management and security
9	0.057*"energy" + 0.018*"grid" + 0.015*"blockchain" + 0.015*"trading" + 0.013*"system" + 0.013*"smart" + 0.013*"power" + 0.007*"EV" + 0.007*"market" + 0.006*"transaction" + 0.006*"COVID-19" + 0.006*"network" + 0.006*"demand" + 0.006*"solution" + 0.005*"electricity"	Blockchain in energy systems and trading
10	0.040*"blockchain" + 0.022*"system" + 0.020*"IoT" + 0.018*"network" + 0.014*"security" + 0.010*"device" + 0.008*"solution" + 0.007*"data" + 0.007*"application" + 0.006*"communication" + 0.006*"resource" + 0.006*"framework" + 0.005*"architecture" + 0.005*"time" + 0.005*"smart"	Blockchain in IoT systems and next-generation networks
11	0.024*"vehicle" + 0.022*"system" + 0.021*"chain" + 0.020*"blockchain" + 0.016*"supply" + 0.014*"food" + 0.013*"data" + 0.009*"IoV" + 0.009*"transport" + 0.008*"information" + 0.007*"traceability" + 0.007*"quality" + 0.006*"management" + 0.006*"safety" + 0.006*"IoT"	Blockchain in supply chain and transportation systems
12	0.061*"blockchain" + 0.039*"IoT" + 0.021*"smart" + 0.020*"security" + 0.019*"application" + 0.011*"device" + 0.011*"system" + 0.010*"technology" + 0.008*"network" + 0.008*"city" + 0.008*"challenge" + 0.008*"transaction" + 0.007*"issue" + 0.007*"privacy" + 0.006*"solution"	Blockchain and IoT applications in smart cities
13	0.072*"IoT" + 0.023*"blockchain" + 0.023*"security" + 0.016*"network" + 0.014*"device" + 0.013*"smart" + 0.012*"application" + 0.012*"challenge" + 0.011*"technology" + 0.010*"data" + 0.010*"architecture" + 0.009*"system" + 0.007*"issue" + 0.007*"privacy" + 0.007*"computing"	Security and networking in IoT and blockchain applications
14	0.050*"node" + 0.019*"WSN" + 0.018*"energy" + 0.018*"routing" + 0.015*"network" + 0.013*"cluster" + 0.011*"sensor" + 0.010*"blockchain" + 0.009*"data" + 0.008*"trust" + 0.008*"malicious" + 0.008*"IoT" + 0.008*"packet" + 0.006*"security" + 0.006*"protocol"	Blockchain, IoT, and energy efficiency in wireless sensor networks (WSN)

year period from 2016 to early 2023 (see Fig. 3), the scholarly output in this interdisciplinary domain has undergone transformative growth, manifested in an astounding annual growth rate of 99.96%. The initial phase, spanning from 2016 to 2018, was characterized by an emergent interest in the intersection of these two revolutionary technologies. The academic output, though relatively modest in the beginning, grew at a rapid pace. From a mere five publications in 2016, the output increased to 21 in 2017 and then took a quantum leap to 124 in 2018. This phase marked the advent of a novel academic discourse surrounding IoT and blockchain technology and the need to explore and understand the potential synergies between them. The middle phase, encompassing the years 2019 and 2020, was one of consolidation and rapid expansion. The burgeoning academic interest during this period led to a substantial surge in the research output, reaching 402 and 671 publications, respectively. This phase marked a period of intellectual maturation as the scholarly community began to delve deeper into the intricacies and challenges of integrating IoT with blockchain technology. The recent phase, spanning from 2021 to early 2023, is characterized by an even more vibrant and intense scholarly engagement. Despite a temporary dip in 2021, likely due to global uncertainties (e.g., COVID-19), the number of publications rebounded strongly in 2022, reaching an unprecedented high of 1574. As of April 2023, the number of publications stands at 639, indicating a continued momentum in research activity. This phase represents an era of innovation and exploration because scholars continue to unlock the transformative potential of IoT and blockchain convergence. The scholarly output thus far indicates a thriving and dynamic research landscape that is poised for further growth and discoveries.

Fig. 4 shows that the field of IoT and blockchain research appears to be largely dominated by technical and interdisciplinary journals. As a

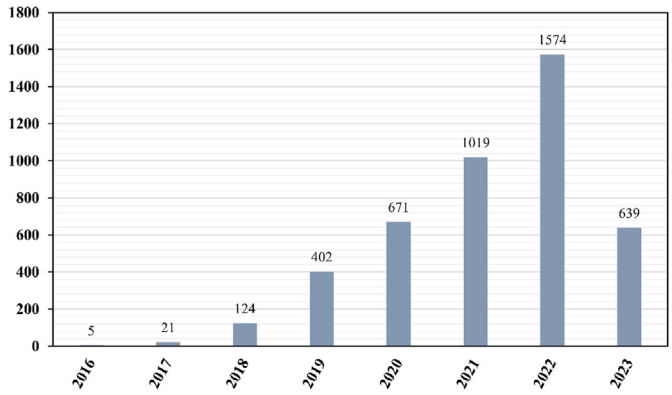


Fig. 3. Year-wise distribution of selected publications.

renowned professional association for the advancement of technology, IEEE significantly leads the discourse with three of its journals - *IEEE Internet of Things Journal*, *IEEE Access*, and *IEEE Transactions on Industrial Informatics* - ranking among the top five most productive platforms. This suggests that the intersection of IoT and blockchain is primarily seen as a technological issue, with a strong focus on the development, application, and implications of these technologies in various sectors. Moreover, *Sensors* and *Electronics Switzerland* are among the top five, further substantiating this observation. The former's focus on sensor technology aligns with the fundamental aspects of IoT, where sensors play a critical role in data acquisition. The latter's broad scope in electronics and electrical engineering highlights the technical orientation of this field of study. Interestingly, the high productivity of these journals suggests a vibrant and dynamic research landscape. It reflects the global academic community's recognition of the transformative potential of integrating IoT with blockchain technology, which is likely driving the high volume of scholarly output. This trend indicates a promising future for research in this interdisciplinary domain as researchers continue to explore and understand the complexities and possibilities at the confluence of IoT and blockchain technology.

The core objective of this research is to construct and analyze an LDA model focusing on the integration of IoT and blockchain technology. The research team employed ten keywords and their associated weights to examine the 14 topics suggested by the model. An inductive analysis was carried out to identify the themes linked to these keywords. From this analysis, 14 key topics surfaced, representing a comprehensive overview of the current trends and focus areas in the field of IoT and blockchain research. The most discussed themes within the literature were Topic 8, which revolves around the use of blockchain in healthcare data management and security, and Topic 3, which centers on the integration of blockchain and IoT in supply chain management. The prominence of Topic 8 underscores the growing appreciation of the potential benefits that blockchain technology can bring to healthcare data management and security. Several researchers have highlighted that blockchain can play a pivotal role in ensuring the secure and efficient handling of sensitive healthcare data, particularly in situations where traditional data management techniques prove to be inadequate or unsafe [43–46]. The considerable attention dedicated to this topic underscores the significance of developing innovative solutions that leverage blockchain technology to enhance the privacy, reliability, and security of healthcare data management [43]. Conversely, the central role of Topic 3 in the literature reflects the increasing interest in developing more effective and seamless supply chain management solutions using IoT and blockchain technology. As global trade continues to grow and the demand for efficient logistics increases, supply chain management becomes a critical challenge. Consequently, the integration of IoT and blockchain in this area offers the potential to optimize supply chain processes by improving traceability, reducing operational costs, and enhancing overall supply chain security [22]. The growing interest in this topic emphasizes the importance of exploring innovative IoT and blockchain solutions to elevate the efficiency, reliability, and transparency of supply chain management [5,47].

Utilizing PyLDAvis, a Python package developed by Ref. [48], the significance of the weights of the chosen topics within the LDA model pertaining to IoT and blockchain can be readily understood. Each defined topic is represented as a corresponding colored circle on a 2D map (Fig. 5) produced using PyLDAvis. Among these, Topic 8 (Blockchain in healthcare data management and security) has the largest circle size, indicating its dominant influence in the current research landscape. Additionally, the intertopical distance map reveals overlaps between Topic 5 (Blockchain in IoT and IIoT for data security and privacy) and Topic 8, Topic 8 and Topic 10 (Blockchain in IoT systems and next-generation networks), Topic 10 and Topic 12 (Blockchain and IoT applications in smart cities), and between Topic 12 and Topic 13 (Security and networking in IoT and blockchain applications). These overlaps suggest that there are strong interconnections between these themes

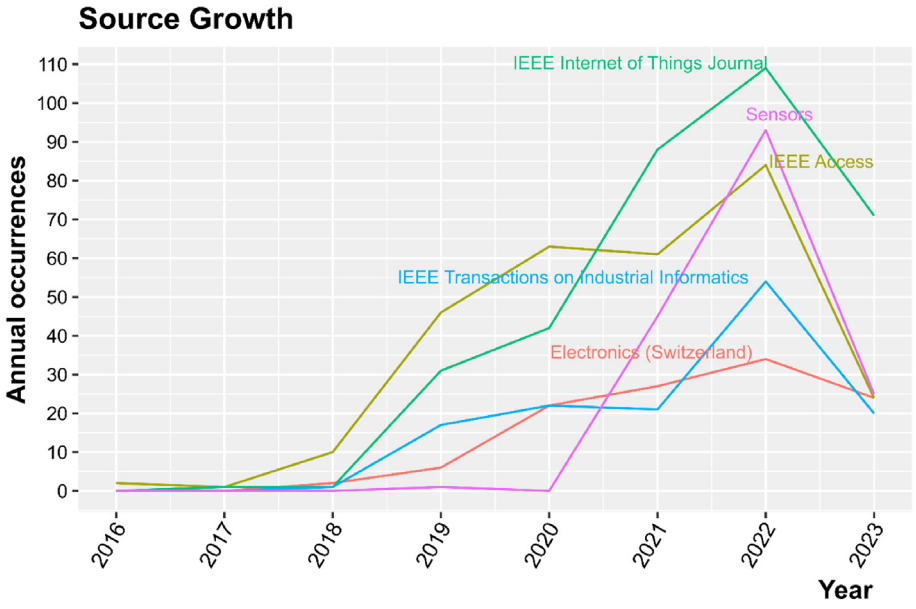


Fig. 4. Most productive journals in the field of IoT and blockchain technology.

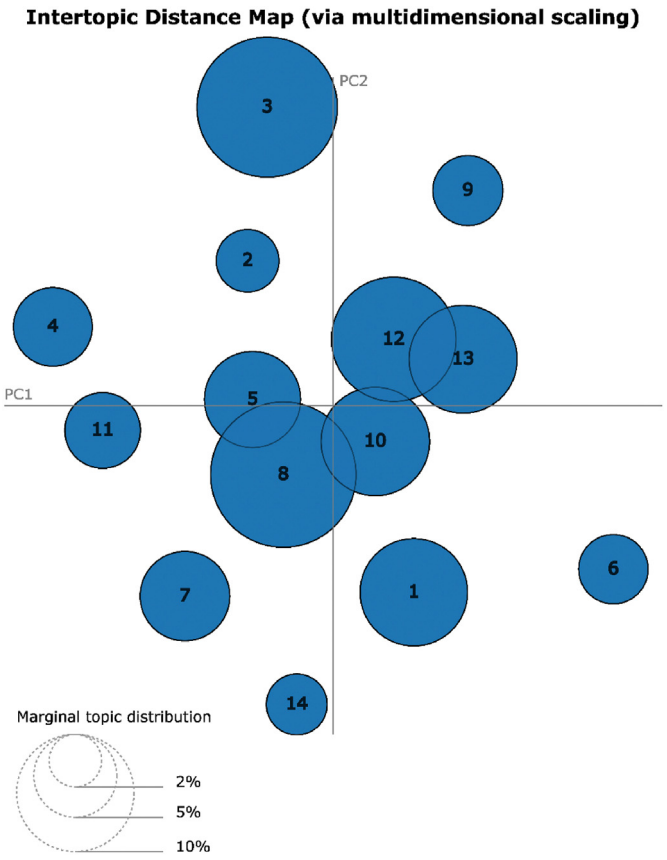


Fig. 5. Intertopical distance map.

within the literature, mainly because they all deal with aspects of data security, privacy, networking, and application of IoT and blockchain in diverse fields. The overlapping nature of these topics also indicates that researchers are exploring various dimensions of data security and networking, dealing with both broader issues, such as integrating IoT and blockchain in healthcare and smart cities (Topics 8 and 12), and more focused aspects, such as data security in IIoT and next-generation networks (Topics 5 and 10). Despite the overlaps, Fig. 5 shows distinctness in the diameters of the different circles and substantial variation in the topics related to IoT and blockchain applications. This suggests that the field comprises numerous subfields, each being examined independently. This diversity and the overlaps observed can present untapped opportunities for interdisciplinary research. Consequently, scholars could explore the intersections between these topics to discover new insights and contribute to a more comprehensive understanding of IoT and blockchain applications in various sectors.

According to Fig. 6, it is clear that a minimum of 500 papers examine each of the identified topics within the scope of IoT and blockchain. The topics that are most frequently discussed include Topic 8 (Blockchain in healthcare data management and security), appearing in 1700 papers; Topic 3 (Blockchain and IoT integration in supply chain management), addressed in 1687 papers; and Topic 12 (Blockchain and IoT applications in smart cities), featured in 1391 papers. These themes underscore the critical role of blockchain and IoT in enhancing security, privacy, and efficiency in pivotal sectors such as healthcare, supply chains, and urban infrastructure. However, some topics receive less attention. These include Topic 2 (Access control and management in blockchain-based IoT systems), mentioned in 511 papers; Topic 14 (Blockchain, IoT, and energy efficiency in wireless sensor networks), appearing in 523 papers; and Topic 9 (Blockchain in energy systems and trading), discussed in 649 papers. These topics, while currently less explored, are intrinsically interconnected and collectively represent an emerging frontier in blockchain and IoT research. They all explore blockchain's potential in addressing critical challenges in various IoT domains - be it access control and management in IoT systems, enhancing energy efficiency in wireless sensor networks, or revolutionizing energy systems and trading. Access control and management in IoT (Topic 2) is a crucial issue given the ever-expanding landscape of IoT devices. The advent of blockchain technology could offer a solution, providing a secure and decentralized mechanism to manage access and permissions across multiple devices [23]. This decentralization aspect of blockchain also plays a crucial role in Topic 14, where the use of IoT devices in wireless sensor networks could benefit from blockchain technology for improving energy efficiency [49]. By enabling peer-to-peer energy transactions, blockchain could potentially minimize losses associated with centralized energy distribution, thereby enhancing overall energy efficiency [50]. Similarly, the use of blockchain in energy systems and trading (Topic 9) represents another promising area where the decentralized and transparent nature of blockchain could revolutionize the way energy is traded, and transactions are recorded. While these areas are currently less dominant in the literature, the relative scarcity of research also suggests they may be ripe for innovative investigations. These areas could yield substantial advancements in the integration of blockchain and IoT, offering new solutions to pressing challenges in IoT security, energy efficiency, and energy trading. Consequently, they represent valuable directions for future research

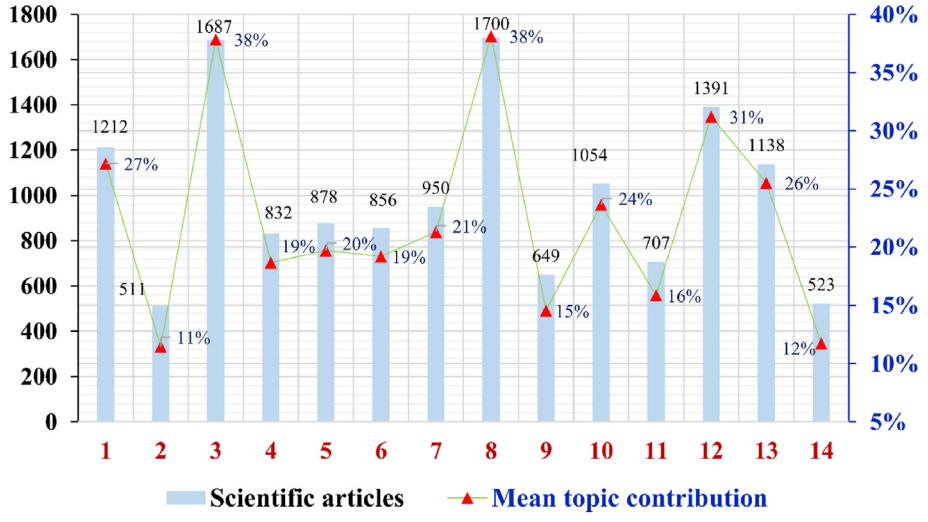


Fig. 6. Topics distribution amongst documents.

within the broader context of IoT and blockchain technology.

This disparity in attention might be attributed to the novelty and development stage of these subjects within the broader application of IoT and blockchain technologies. The paucity of extensive empirical evidence in these nascent areas might be limiting more comprehensive academic exploration. In summary, the distribution of topics across the selected articles is uneven, with a median value of 914 and an average value of 1006.286. This pattern suggests that certain areas within the intersection of IoT and blockchain are receiving more scholarly focus while others are relatively understudied. The skewed distribution could be due to a variety of factors, such as the perceived importance of certain topics, the availability of resources for research in specific areas, and the alignment of researchers' interests with these topics. These factors might give rise to certain "hotspot" areas in the research landscape that get more scholarly focus while other areas remain more unexplored.

4. Discussion of topics

4.1. Security and authentication in blockchain-based IoT networks

Topic 1 is primarily centered around the concepts of blockchain technology and its applications within the realm of IoT security. The key terms associated with this topic, such as scheme, security, authentication, device, blockchain, IoT, attack, key, protocol, and data, indicate a strong focus on the development and analysis of security protocols and authentication schemes utilizing blockchain in IoT environments (Table 3). The studies under this topic predominately explore how blockchain can enhance security and trust within IoT networks. They do this by focusing on key areas such as secure access control, efficient authentication, key agreement, and secure communication. For example, Ref. [24] introduce a blockchain-based access control scheme in the Internet of Drones (IoD) context. This scheme facilitates secure communication between drones and the ground station server, employing the ripple protocol consensus algorithm to incorporate transactions into the blockchain. As a result, the data collected by the drones is protected and resistant to tampering. Similarly, Ref.[51] present a blockchain-based authentication scheme that employs Hyperelliptic Curve Cryptography (HECC) to mitigate security vulnerabilities in IoD systems. The proposed scheme showcases resilience against different attacks and surpasses existing approaches in terms of security features, communication costs, and computational efficiency. Furthermore, studies on Topic 1 delve into the development of efficient key agreement protocols that do not rely on traditional certificates. For instance, Ref. [52] propose a secure and efficient certificateless public-key signature (CL-PKS) scheme, along with utilization of the ECDHE key exchange mechanism, to enhance the security of cross-domain authentication and key agreement in the Industrial Internet of Things (IIoT). This proposal incorporates a consortium blockchain and demonstrates computational efficiency and enhanced communication when compared to alternative schemes. In another study, Ref. [53] suggest a decentralized pairing-based certificateless authenticated key agreement (AKA) protocol that addresses the vulnerabilities such as the single point of failure and the key escrew problem. The proposed protocol establishes a session key for communication purposes and employs ring signatures for node authentication, resulting in benefits such as flexibility in group size and decreased computation costs. Furthermore, Ref.[54] develop a lightweight provable data possession scheme based on blockchain technology to tackle the issues of high computation overhead in tag generation and vulnerability to collusion attacks in low-performance devices and IoT settings. The proposed scheme incorporates a secure method for outsourced tag generation and leverages the chainecodes of blockchain to guarantee data correctness and thwart collusion attacks. Finally, Ref. [55] propose an effective and innovative security scheme for IoT application by combining the advantages of blockchain, random number generation, and dynamic key generation. In summary, Topic 1 sheds light on the use of blockchain technology as a key enabler for security in IoT. The topic emphasizes the need for robust, efficient, and scalable security mechanisms in various IoT domains, from IoD and IIoT to Wireless Body Area Networks (WBANs), and presents blockchain as a potential solution to these changes. As such, this topic appears to be an important area of focus for researchers aiming to enhance the security and trustworthiness of IoT networks. Based on the discussion of Topic 1, emerging future research directions might include:

1. Exploring more efficient blockchain consensus algorithms specifically designed for IoT environments to improve system performance and security.
2. Examining the impact of quantum computing threats on blockchain-based IoT security protocols and authentication schemes.
3. Investigating the scalability of blockchain-based security solutions as the number of IoT devices continues to grow exponentially.
4. Developing dynamic and adaptive blockchain-based security protocols that can respond to the evolving threat landscape in IoT.
5. Studying the integration of blockchain with advanced machine learning techniques to detect and mitigate sophisticated attacks on IoT systems.
6. Investigating how blockchain-based identity and access management solutions can improve the security of IoT devices.
7. Examining the balance between the security provided by blockchain technology and the privacy of users in IoT environments.
8. Researching the applicability of blockchain-based solutions in securing newer IoT technologies like 5G and beyond.

4.2. Access control and management in blockchain-based IoT systems

Topic 2, labeled "Access control and management in blockchain-based IoT systems", revolves around the intersection of blockchain technology, IoT systems, and the concept of access control. The key terms associated with this topic, such as IoT, access, control, blockchain, system, and agricultural, indicate a focus on the application of blockchain for managing and controlling access in IoT systems, including specific sectors like agriculture. The research papers falling under this topic broadly explore various aspects of implementing blockchain for access control in IoT systems. They cover a range of sub-topics, including resolving unauthorized access vulnerabilities, adopting smart control-based access control, and designing blockchain-based access control models. For example, Ref. [56] introduce a blockchain-based and encrypted Currency-Based Access Control model (CcBAC) that leverages Trused Execution Environment (TEE) technology to tackle privacy concerns in IoT. Their findings show that the CcBAC model effectively enables fine-grained access control, robust auditability, and access procedure for IoT devices, granting resource owners complete authority over access while ensuring security and privacy. Likewise, Ref. [57] propose a framework based on smart contracts to address access control challenges in IoT by incorporating multiple Access Control Contracts (ACCs), a Judge Contract (JC), and a Register Contract (RC). The results show the efficiency of the framework in achieving dynamic and static access right validation, misbehavior judging, and comprehensive management access control methods within an IoT system. Ref. [58] propose a model that leverages zero-knowledge proof and smart contract technology within the blockchain to strengthen access control security in IoT. The results indicate that deploying access control attribute information in blockchain, employing encrypted access control tokens, and utilizing smart contracts significantly enhance attribute privacy protection, access efficiency, and mitigate risks associated with conventional centralized access control models in the IoT ecosystem. Therefore, scholars delve into the conjunction of blockchain with other technologies, such as smart contracts and trusted execution environments, to design secure and efficient access control models for IoT systems. Another interesting aspect is the application of these technologies in specific use cases. For instance, Ref. [59] propose a blockchain-based smart waste management system to mitigate environmental impacts and optimize solid waste management in

cities. Ref. [60] also propose an IoT-driven solid waste management system for developing countries and urban areas, leveraging blockchain-enabled Vehicular Ad-hoc Networks (VANETs) for decentralized solutions. The results of the authors demonstrate successful implementation of waste bin identification, real-time tracking, trash weighing, and waste collection from dump locations through geofencing. Consequently, this highlights the practical, real-world implications of these technologies and their potential to revolutionize fields like waste management. The presence of the terms like agricultural and e-commerce further suggest that this topic also covers applications of blockchain and IoT in sectors like agriculture and e-commerce [61,62]. This could involve things like using blockchain to ensure secure and efficient access control in IoT-enabled agricultural systems and e-commerce platforms [63,64]. In summary, Topic 2 is primarily concerned with the potential of blockchain technology to enhance access control and management in IoT systems. It emphasizes the need for robust and efficient access control mechanisms in various IoT environments and sectors and highlights the potential of blockchain as a solution to these challenges. This topic appears to be a crucial area of interest for scholars working on blockchain and IoT and their intersection with access control. Future research directions related to Topic 2 might include:

1. Investigating the integration of blockchain and advanced AI techniques for smarter, self-learning access control systems in IoT.
2. Developing blockchain-based access control systems that can adapt to evolving user behavior and changing threat landscapes.
3. Evaluating the trade-off between the robustness of blockchain-based access control mechanisms and the system's performance and scalability.
4. Exploring the application of Zero Knowledge Proofs in blockchain-based access control systems for further improving user privacy.
5. Studying the role of user interfaces and user experience design in ensuring the effective adoption of blockchain-based access control systems.
6. Exploring how blockchain can enhance IoT access control within multi-cloud and edge computing environments.
7. Conducting comparative studies of different blockchain architectures for IoT access control to determine the most efficient models.

4.3. Blockchain and IoT integration in supply chain management

The third topic is labeled "Blockchain and IoT integration in supply chain management", and it focuses on the fusion of blockchain technology, IoT, and supply chain management. Technology, blockchain, chain, supply, digital, industry, AI, IoT, are a few of the most significant terms related to this topic. More specifically, these terms denote a distinct concentration on the implementation of blockchain and IoT technologies in the supply chain management sphere, likely in the context of Industry 4.0. In this cluster, scholars explore the usage and implications of blockchain and IoT technologies in improving, modernizing, and transforming supply chain management. The papers cover diverse sub-topics, including barriers to circular economy adoption, the impact of emerging IoT investments on firm performance, the applications of RFID in supply chain management, and the drivers of digital transformation in SMEs [4,5]. For example, Ref. [65] aim to prioritize barriers to establishing a circular economy and propose blockchain-IoT strategies to overcome these barriers, with the goal of creating sustainable ecosystems and mitigating the challenges to circular economy implementation. Ref. [66] explore the mediating effect of digital options on the relationship between emerging information technology investments and firm performance. The findings indicate that IoT has a profound impact on the market value of a firm's assets, while blockchain technology strongly influences return on net assets (ROE). Other studies, such as [67], examine the relationship between sustainable supply chain management and digital transformation through the deployment of blockchain, IoT, and big data analytics and find that the mix of these technologies can improve sustainable performance, enhance companies' market position, and foster the development of sustainable policies in the context of supply chains. In the same vein, Ref. [68] explore the impact of blockchain on global supply chain operational and managerial processes and find that the technology exhibits informational, automational, and transformational impacts. Overall, Topic 3 underlines the importance and potential of blockchain and IoT technologies in supply chain management, specifically within the paradigm of digital transformation or Industry 4.0. The topic emphasizes the ongoing shift towards more digital advanced, efficient, and sustainable supply chains, and highlights how these emerging technologies can play a pivotal role in this transformation. To advance the understanding of Topic 3, future research directions might include:

1. Investigating the potential of combining other advanced technologies, such as AI and machine learning, with blockchain and IoT for more advanced, autonomous, and efficient supply chain management.
2. Assessing the potential of blockchain technology in other facets of supply chain management like inventory management, logistics, and procurement.
3. Evaluating the effectiveness of blockchain and IoT technologies in mitigating common supply chain issues such as counterfeit goods, slow response times, and lack of transparency.
4. Developing strategies to address the technological and cultural challenges that companies might face when implementing blockchain and IoT in their supply chains.
5. Conducting in-depth case studies of different industries to understand the industry-specific applications and implications of blockchain and IoT in supply chain management.
6. Exploring the ethical implications of increased transparency in supply chains due to the implementation of blockchain and IoT technologies.
7. Investigating how the integration of blockchain and IoT in supply chain management can contribute to achieving sustainability goals.
8. Conducting empirical studies to measure the actual performance improvement achieved through the implementation of blockchain and IoT in supply chains.

4.4. Federated learning and blockchain in smart systems

Topic 4 is titled "Federated learning and blockchain in smart systems", and it predominately focuses on the integration of federated learning, blockchain technology, and intelligent systems. Conceptually, federated learning represents a machine learning approach that allows for decentralized learning, where the model learns from data located on different devices or servers without the need to centrally collect this data. The integration of blockchain technology in such systems could provide additional security and privacy benefits, making this combination especially relevant for applications dealing with sensitive or private data. For example, Ref. [69] propose a differentially privacy blockchain-based explainable federated learning (DP-BFL) framework within the context of social media 3.0, and the findings demonstrate that the framework achieves high utility, enhanced privacy, and elevated efficiency in machine learning models while reducing the impact of malicious entities and protecting privacy. Ref. [70] develop an adaptive self-reconfiguration (ASR) framework for active vision systems operating in a distributed blockchain network and demonstrate that the proposed framework enables resource and data sharing, reduces learning and configuration durations, and outperforms state-of-the-art systems in terms of accuracy and latency, making it suitable for real-time applications. Ref [71] develop a blockchain-based asynchronous federated learning (BAFL) framework that provides efficiency, security, and resilience against poisoning attacks in federated attacks. The findings show that the BAFL framework can lead to higher performance and efficiency compared to other distributed machine learning methods. Moreover, Ref. [72] examine the unintended property leakage in

blockchain-assisted federated learning for intelligent edge computing and confirm the efficiency and effectiveness of novel property inference attacks in inferring various properties of training data while ensuring the quality of main functions in federated learning. Finally, Ref. [73] recommend the integration of blockchain technology with federated learning in IoT systems to protect against attacks and improve the security of big data analytics. In summary, Topic 4 delves into the merging of decentralized learning, blockchain, and intelligent systems, which represents a powerful amalgamation capable of providing enhanced security and privacy. Studies show promising results of this integration, including its applications in social media 3.0, adaptive self-reconfiguration in active vision systems, and its protection against cyber-attacks. The exploration and affirmation of the effectiveness of this synergy, particularly in inferring various properties of training data and strengthening the security of big data analytics in IoT systems, set a compelling direction for future research and technological advancements. To advance the knowledge of Topic 4, future research directions might include:

1. Exploring the applications of federated learning and blockchain in other sectors, such as healthcare or finance, where the protection of sensitive data is paramount.
2. Assessing the implications of integrating advanced encryption techniques into federated learning and blockchain-based systems for improved data privacy and security.
3. Investigating the potential of integrating other emerging technologies, such as edge computing or quantum computing, into federated learning and blockchain systems for improved computational efficiency.
4. Evaluating the potential impact of legislation and regulation on the development and application of federated learning and blockchain in smart systems.
5. Examining the socio-economic impacts of the integration of federated learning and blockchain technology in smart systems, such as impacts on jobs or data ownership.
6. Designing strategies to promote the adoption of federated learning and blockchain technologies in industries that are traditionally slow to adopt new technologies.

4.5. Blockchain in IoT and IIoT for data security and privacy

Topic 5 is labeled "Blockchain in IoT and IIoT for data security and privacy," and it concentrates on the utilization of blockchain technology within the IoT and the Industrial Internet of Things (IIoT). This includes a focus on ensuring data security, privacy, and managing trust relationships. Key terms such as data, smart, system, contract, service, user, trust, device, management, privacy, security, IIoT, sharing, application, network, mechanism, platform, solution, technology, decentralized, and framework all align with the topic. From the papers reviewed, it is clear that there is a significant interest in using blockchain technology to improve trust management in IoT networks [74], to bolster security systems in smart homes [75], and to create a real-time interactive platform based on publish-subscribe mechanism [76]. Another focus of research on this topic is data trading and sharing. For instance, blockchain has been used to facilitate decentralized data trading [77], to manage the cost of IoT sensor data storage [78], and to incentivize vehicular crowdsensing activities [79]. The use of smart contracts is another recurring theme. This includes using smart contracts for data commodity transactions in the IIoT [80], fuzzing smart contracts for TOD vulnerability detection [81], and proposing a blockchain-based privacy-preserving reputation framework for participatory sensing systems [82]. Several studies also concentrate on data privacy, with some proposing a decentralized personal data store based on Ethereum to achieve GDPR compliance [83] and a blockchain-enabled antileakage sharing protection scheme for undisclosed IIoT vulnerabilities [84]. Others focus on operational data security in industrial control systems [85] and a fair, secure, and trusted decentralized IIoT data marketplace enabled by blockchain [86]. Finally, scholars explore the intersection of semantic knowledge management, blockchain, and privacy in IoT applications [87]. In short, Topic 5 sheds light on the potential of blockchain technology in enhancing security, privacy, and trust management in IoT and IIoT systems. As such, future research directions might include:

1. Developing predictive models that can anticipate and mitigate security vulnerabilities in blockchain-IoT systems.
2. Investigating the role of quantum computing in enhancing blockchain security and data privacy in IoT and IIoT.
3. Evaluating the potential of federated blockchain models for improved data sharing and privacy in IoT and IIoT environments.
4. Applying AI and machine learning for the automation of smart contracts to increase efficiency and security in IoT and IIoT data exchanges.
5. Exploring how blockchain can facilitate edge computing in IoT and IIoT for better data security, privacy, and decentralized processing.
6. Analyzing the socio-technical aspects of privacy and security in blockchain-IoT systems – user behavior, policy implications, ethical considerations.
7. Developing adaptive blockchain algorithms that can dynamically adjust to the evolving security requirements of IoT and IIoT applications.
8. Assessing the application of blockchain in ensuring data integrity and traceability in critical IoT and IIoT systems like healthcare or industrial control systems.
9. Designing decentralized identity solutions using blockchain in IoT and IIoT to enhance user privacy and control over personal data.

4.6. Blockchain consensus algorithms and security in IIoT

Topic 6 is primarily concerned with the role and optimization of consensus algorithms in blockchain networks, with particular focus on their application in IIoT sector. The representative terms, such as consensus, algorithm, node, blockchain, IIoT, network, and mechanism, suggest a deep focus on the various mechanisms and models for achieving consensus in a blockchain network, and their direct implications on the security, trustworthiness, and performance of IIoT systems. Studies on this topic mainly delve into exploring and improving the existing consensus algorithms for blockchain, with an eye towards their implementation in IIoT systems. For instance, Ref. [88] propose a scalable Byzantine fault tolerance algorithm based on a tree topology network (STBFT) to overcome the scalability issue of the practical Byzantine fault tolerance algorithm in large-scale wide area network environments. The results show that the tree topology network structure is more scalable, fault-tolerant, and resource-efficient thanks to the STBFT algorithm's layering and grouping of consensus nodes. Ref. [89] introduce a credit identity ring optimization blockchain algorithm (CRBFT) based on practical Byzantine fault tolerance (PBFT) to solve security issues in the IoT network. The results show that compared to PBFT, CRBFT achieves competitive performance in terms of throughput, communication overhead, and consistency delay, and it boosts system security. Efforts have also been made to develop consensus mechanisms specific to certain IIoT applications. For example, Ref. [90] propose a unique blockchain and IoT-based consensus mechanism called COME to solve the problem of electric car coordination and scheduling at charging stations. The results show that the proposed COME consensus mechanism is more superior than the practical Byzantine Fault Tolerance consensus protocol in terms of conflict resolution, scalability, charging time, wait time, and bandwidth analysis. In addition, Ref. [91] introduce a trust-based hierarchical consensus mechanism (THCM) to solve the problems associated with smart grid data security and efficiency and find that the proposed solution is more efficient and scalable for smart grid data management than current consensus algorithms, increasing efficiency, throughput, and reducing storage. Security in IIoT systems is a

recurring theme in this topic, with several papers discussing novel consensus algorithms that can mitigate security vulnerabilities. For instance, Ref. [92] propose a blockchain-based secure routing model for IoT networks, and the results show the model's efficacy in reducing transaction costs and energy consumption, detecting malicious nodes, and optimizing routing paths and security, all of which point to its potential for improving the efficiency and security of data routing in IoT networks. Similarly, Ref. [93] examine how the Merkle-Hellman Knapsack Cryptosystem (MHKC) can be applied to blockchain applications and demonstrate the performance and effectiveness of different metaheuristic algorithms in attacking MHKC with various knapsack length. In a nutshell, Topic 6 encapsulates the ongoing research efforts in optimizing blockchain consensus algorithms for better performance, security, and efficiency in IIoT systems. It highlights the significance of robust consensus mechanisms in enhancing the scalability, reliability, and security of blockchain networks in the context of IIoT. Potential future research directions related to Topic 6 might include:

1. Investigating new models and architectures for achieving consensus in blockchain networks with a focus on scalability and efficiency for large-scale IIoT applications.
2. Evaluating the performance of existing blockchain consensus algorithms in specific IIoT use cases (e.g., manufacturing, logistics, smart grids) and identifying potential bottlenecks or vulnerabilities.
3. Examining the interplay of blockchain consensus mechanisms with other emerging technologies, such as AI, edge computing, and 5G/6G networks, in the context of IIoT.
4. Developing advanced cryptographic techniques and consensus algorithms to enhance the security and privacy of IIoT data in blockchain networks.
5. Proposing and testing novel incentive mechanisms to encourage honest participation in blockchain networks, thereby increasing their reliability and trustworthiness in IIoT applications.
6. Investigating how consensus mechanisms in blockchain can support the unique requirements of IIoT systems, such as real-time processing, high scalability, and robustness against various network and security threats.
7. Assessing the implications of consensus mechanisms on the energy efficiency of blockchain networks, which is a critical consideration for IIoT applications.

4.7. Blockchain and edge computing in IoT

Topic 7 discusses the integration of blockchain technology with edge computing in the context of IoT systems. Keywords such as edge, computing, resource, model, blockchain, IoT, network, and data indicate the topic's focus on optimizing resource allocation and computational tasks in decentralized IoT networks using blockchain technology. Under this topic, several studies focus on resource allocation in edge computing environments within the IoT paradigm. For instance, the paper of [94] focuses on cloud/edge computing resource allocation and pricing for offloading computationally heavy blockchain tasks in IoT and finds that the suggested iterative greedy-search-based method enhances overall performance by optimizing the revenue of the service provider and IoT terminals. Similarly, Ref. [95] aim to optimize hardware resource allocation for edge nodes in a multitier mobile edge computing (MEC) hierarchy. The results show that the proposed method, which is implemented through a parametric Bayesian optimizer, outperforms pseudorandom resource allocation by completing a greater fraction of computational tasks within a given budget. Computation offloading, which involves transferring computational tasks from devices with limited resources to more powerful servers, is another prominent theme in this topic. For example, Refs. [96,97] explore how blockchain can facilitate secure and efficient offloading in mobile edge computing (MEC) systems. Some studies also investigate the potential of blockchain in enhancing the security and reliability of edge computing in IoT. The study of [98] presents a framework combining fog, multi-access edge computing (MEC), software-defined networking (SDN), network virtualization, and blockchain for IoT applications, achieving higher efficiency in terms of latency and resource utilization while addressing challenges such as security, traffic management, availability, reliability, and energy constraints. Ref [99] introduce EntrapNet, a blockchain-based computing verification protocol for distributed shared computing networks, overcoming the problem of incorrect computing results from untrusted service providers and bringing the cost of secure computing down to a level where it can be used in practice. Finally, Ref. [100] propose a decentralized and trusted edge computing platform (DeTEC) that successfully integrates blockchain technology to incentivize contributions, resolves user requests to adequate edge servers, and guarantees the trustworthiness of computational results. Overall, Topic 7 represents a blend of research on the integration of blockchain and edge computing in IoT. The studies show various innovative ways to use blockchain technology to improve the security, efficiency, and reliability of edge computing systems. They also highlight the importance of optimizing resource allocation and computation offloading in such environments. Potential future research directions related to Topic 7 might include:

1. Investigating the use of blockchain technology to enhance the security and privacy of data in edge computing environments.
2. Developing blockchain-based models for efficient resource allocation and computation offloading in mobile edge computing systems.
3. Evaluating the performance of blockchain-based edge computing systems in real-world IoT applications.
4. Proposing novel architectures and protocols for decentralized edge computing platforms that leverage blockchain technology.
5. Exploring the interplay of blockchain with other emerging technologies, such as 5G/6G networks and artificial intelligence, in the context of edge computing for IoT.
6. Investigating energy-efficient algorithms and mechanisms for blockchain-based edge computing systems in IoT.

4.8. Blockchain in healthcare data management and security

Topic 8 deals with the application of blockchain technology in the healthcare industry for secure data management. Keywords such as data, blockchain, system, IoT, security, healthcare, access, and privacy indicate that the core theme of the topic centers on ensuring the security, privacy, and controlled access of healthcare data within IoT systems by leveraging blockchain technology. One of the key areas under this topic is the control and management of personal health data. For example, Ref. [101] introduce an IoT-based configurable blockchain for mHealth data, offering privacy protection, user control, and HIPAA compliance, thereby enabling personalized healthcare systems with secure data storage and analysis [102]. introduce a scheme that utilizes blockchain technology to protect the privacy of medical data during sharing. By employing K-anonymity, searchable encryption, and Hyperledger Fabric, the scheme ensures secure access control and confidentiality while also demonstrating practical scalability and performance. Several studies also discuss the secure storage and sharing of healthcare data. For example, Ref. [103] present a novel framework that leverages WBAN and blockchain technology to guarantee the confidentiality, security, and authenticity of health data. By integrating sensor devices, cloud storage, and blockchain, the proposed framework enables secure data transmission and storage, effectively addressing privacy and security concerns in healthcare. The system aims to benefit patients, healthcare providers, and health insurance providers by enabling informed self-care, remote patient monitoring, and preventing fraudulent claims. Similarly, Ref. [102] propose a model for a secure and decentralized medical information system using blockchain technology, enabling safe storage and sharing of medical data, real-time data collection during surgery, anonymous data sharing, and implementation with Hyperledger Fabric.

Moreover, the studies also explore the integration of blockchain with other technologies for enhancing healthcare data security. For example, Ref. [104] introduce a blockchain-based access control system using smart contracts, providing a secure and trustworthy method for sharing electronic health records, addressing the challenges of third-party dependence and ensuring privacy in healthcare data sharing. Therefore, Topic 8 represents research focusing on the use of blockchain for secure data management in the healthcare industry. It shows how blockchain can enhance privacy, control, and security in the storage, sharing, and access of healthcare data. Possible avenues for future research in Topic 8 might involve:

1. Studying the impact of blockchain on patient privacy and data security in telemedicine and mHealth applications.
2. Developing novel blockchain-based architectures for securing electronic medical records (EMRs).
3. Investigating the role of blockchain in securing wearable and IoT medical device data.
4. Examining the ethical implications of using blockchain for healthcare data management.
5. Evaluating the performance and security of blockchain-based healthcare systems in real-world scenarios.
6. Exploring the interplay of blockchain with emerging technologies such as artificial intelligence and machine learning in the context of healthcare data management and security.

4.9. Blockchain in energy systems and trading

Topic 9, labeled as "Blockchain in energy systems and trading," primarily encompasses the application of blockchain technology in the energy sector, including energy systems, power grids, energy trading, and smart energy solutions. The key terms such as energy, grid, blockchain, trading, system, smart, power, and EV (electric vehicle) reflect the focus on integrating blockchain within the energy industry. One substantial area under this topic is the use of blockchain for managing and improving energy systems. In this context, Ref. [105] create a decentralized demand side management system within a community microgrid, incorporating IoT smart meters and renewable energy sources while leveraging blockchain for secure communication and transaction processing. The results demonstrate the effectiveness of this approach in reducing overall energy consumption costs and individual users' energy expenses. Energy trading via blockchain is another crucial theme in this topic. For instance, Ref. [106] examine the use of blockchain in decentralized energy markets, proposing and implementing a model that enables validated clean energy trading, achieves high transaction throughput, and provides empirical results on network scalability and deployment costs. Ref. [107] present an enhanced blockchain-based method that monitors carbon emission reduction, overcomes the limitations of prior solutions, and promotes fair trade for environmental prioritization. The results demonstrate the effectiveness of a hierarchical blockchain framework utilizing smart contracts, ensuring transparency, integrity, and automated control approaches in carbon emission trading. Importantly, some studies delve into the intersection of blockchain with other emerging technologies in the realm of energy management. As a case in point, Ref [108] introduce an energy trading platform for renewable energy microgrids, leveraging permissioned blockchain, smart contracts, automated trading processes, IoT, and a homomorphic encryption scheme to enhance privacy protection, user participation, and overall practicality. Moreover, Ref. [109] investigate the application of decentralized blockchain mechanisms in delivering secure, transparent, and reliable energy flexibility, showcasing its ability to efficiently align energy demand and production in the smart grid while minimizing the necessary energy flexibility for convergence. Finally, the research of [110] develops a permissioned Corda framework for P2P energy trading that enhances security, minimizes transaction propagation time and ensures fair distribution. The results demonstrate the efficacy of the framework in mitigating delay trading attacks and achieving improved latency and throughput performance. In conclusion, Topic 9 represents a collection of research focusing on the utilization of blockchain technology in energy systems, energy trading, and related areas, demonstrating how blockchain can boost efficiency, ensure privacy, and promote sustainable practices in the energy sector. Potential future research directions for Topic 9 might include:

1. Examining the influence of blockchain on renewable energy trading and distribution.
2. Constructing innovative blockchain-based architectures for the management and optimization of smart grids.
3. Investigating blockchain's role in facilitating green energy practices like carbon emission trading.
4. Evaluating the performance and scalability of blockchain-based energy systems under real-world conditions.
5. Investigating the synergy of blockchain with other emerging technologies such as AI and IoT within the context of energy systems and trading.
6. Studying how blockchain can assist in managing the energy consumption of IoT devices and networks.

4.10. Blockchain in IoT systems and next-generation networks

Topic 10, labeled as "Blockchain in IoT systems and next-generation networks," primarily delves into the incorporation and implications of blockchain technology within the domains of IoT, network security, and the emerging architectures of next-generation networks. The salient terms such as blockchain, system, IoT, network, security, and device, among others, reinforce the focus on applying blockchain technology for the enhancement of IoT systems, bolstering network security, and facilitating the transition towards next-generation networks like 5G and beyond. A noteworthy trend within this topic is the implementation of blockchain in IoT systems. For instance, Ref. [111], propose a coordinated satellite-terrestrial network and network scheduling strategy to overcome the efficiency issues of blockchain and IoT applications. The findings indicate that the proposed system enables higher efficiency in supporting blockchains. Another central theme is the integration of blockchain with 5G and forthcoming 6G network systems. Research such as [112,113] point towards the potential for leveraging blockchain technology in managing and optimizing resources within the frameworks of these advanced networks. The studies argue that blockchain can play a key role in enabling efficient service orchestration in 5G multicloud environments and enhancing resource management in 6G communications. The potential of blockchain for ensuring network security also forms a pivotal point within this topic. Terms like security, attack, and secure highlight the importance of this theme. The idea is further backed by studies that delve into related aspects such as employing blockchain for facilitating secure transactions, data security, and mitigating cybersecurity threats within IoT and network systems. In summary, Topic 10 encapsulates research that investigates the integration of blockchain within IoT systems, the enhancement of network security, and the preparedness for next-generation network systems. The body of research indicates the versatility and capability of blockchain to drive efficiency, ensure security, and facilitate smooth transitions to advanced networks in these domains.

Potential future research avenues for Topic 10 might include:

1. Further exploring blockchain's potential in enhancing the security framework of IoT systems.
2. Studying the implications and benefits of blockchain within the frameworks of 6G and future network systems.
3. Evaluating the real-world efficiency and potential challenges of implementing blockchain-based solutions in IoT and network systems.

4. Investigating the integration of blockchain with other cutting-edge technologies for enhancing IoT systems and network operations.
5. Designing novel blockchain-based architectures to manage and optimize next-generation networks.
6. Identifying and addressing potential cybersecurity threats for advanced network systems using blockchain technology.

4.11. Blockchain in supply chain and transportation systems

Topic 11 concentrates on the deployment and potential advantages of blockchain technology within the realms of supply chains, food systems, and transportation logistics. The terms such as vehicle, system, chain, blockchain, supply, food, data, and IoT affirm the exploration and evaluation of blockchain applications in these particular domains. An important aspect within this topic is the application of blockchain technology in supply chain management. Studies like [114–116] offer insights into how blockchain can promote transparency, balance, and agility in supply chains, contributing to their overall efficiency and robustness. Another significant theme emerging from this cluster is the application of blockchain in food systems, a notion underlined by representative terms such as food, traceability, quality, and safety. This theme is represented in studies like [117,118], which propose blockchain-based models for enhancing food traceability and security in the food supply chain. The domain of transportation and vehicle systems also sees a keen interest in the application of blockchain. For instance, Ref. [119] suggest a method for optimizing the location of an intelligent transportation logistics warehouse by utilizing IoT devices and blockchain technology, resulting in cost reduction and enhanced tracking of the supply chain. The results highlight the benefits of this approach, such as decreased consumptions, precise positioning, and reduced overall expenses, ultimately leading to optimal warehouse placement and improved management of enterprise resources. In another research paper, Ref. [120] investigate how modern warehousing practices are associated with the adoption of IoT-blockchain technology and their impact on organizational business performance. The results indicate that financial and infrastructure practices play a crucial role in promoting IoT blockchain adoption, and integrating organizational, operational, flexibility, and security practices can enhance deployment success and enhance performance in the warehousing industry. In short, Topic 11 represents research that investigates the application and benefits of blockchain in enhancing supply chain management, food system security, and transportation logistics. This body of research illustrates how blockchain can improve transparency, security, and efficiency in these sectors.

Future research directions for Topic 11 could involve:

1. Exploring the integration of blockchain with other emerging technologies like AI and IoT in the context of supply chain management.
2. Evaluating the real-world efficiency and potential challenges of implementing blockchain-based solutions in supply chains and transportation logistics.
3. Investigating the application of blockchain in enhancing food traceability and security in different geographical and cultural contexts.
4. Studying the impact of blockchain technology on sustainable and green practices in supply chains and transportation systems.
5. Designing novel blockchain-based architectures to manage complex supply chains and transportation networks.
6. Developing blockchain-based solutions for mitigating cybersecurity threats in supply chain and transportation systems.

4.12. Blockchain and IoT applications in smart cities

Topic 12 covers the integration and potential advantages of blockchain and IoT technologies within the realm of smart city solutions. The recurring terms, including blockchain, IoT, smart, security, application, device, system, technology, network, city, challenge, transaction, privacy, and solution, reveal the focus of the research on enhancing security, privacy, and overall operational efficiency of IoT-based smart city applications using blockchain technology. Key areas of research within this topic include the examination of security and privacy concerns related to IoT systems in the context of smart cities. Ref. [121] examine the security concerns in smart cities and the implications of quantum computers on blockchain-based applications, presenting a blockchain framework tailored for smart cities and exploring potential solutions to enhance security in the face of quantum threats. In addition, Ref. [122] propose a novel approach using a blockchain-defined network and a grey wolf-optimized modular neural network to enhance security in smart environments, effectively addressing security, privacy, and confidentiality issues. The results show that the proposed system achieves exceptional security (99.12%), improved efficiency, and low latency compared to other neural networks, such as multi-layer perceptron and deep learning networks.

Studies like [123,124] discuss how IoT and blockchain can support secure, efficient data communication within smart cities. Moreover, some papers, such as [125], present the Blockchain-of-Blockchains (BoBs), a hierarchical blockchain-based platform designed to address data management challenges, ensure data integrity, and enable interoperability in smart cities. By integrating IoT and overcoming the limitations of centralized cloud-based systems, the proposed platform enhances transparency, traceability, and integrity in data operations. Implementation using Hyperledger Fabric and Ethermint demonstrates the feasibility and performance of the BoBs concept for smart city organizations. To summarize, Topic 12 highlights the ongoing research efforts to leverage blockchain and IoT for enhancing smart city solutions, with a particular focus on improving security, privacy, and operational efficiency.

Future research directions in this area might include:

1. Exploring the real-world challenges and practical limitations of integrating blockchain with IoT in the context of smart cities.
2. Assessing the impact of blockchain technology on the scalability and performance of IoT systems within smart city environments.
3. Developing novel blockchain-based architectures for secure and efficient IoT data communication in smart cities.
4. Studying the interplay of blockchain and IoT with other emerging technologies (e.g., AI, edge computing) in the context of smart city applications.
5. Evaluating the potential of blockchain and IoT in enhancing various smart city services, such as energy management, traffic control, and waste management.

4.13. Security and networking in IoT and blockchain applications

Topic 13, labeled as "Security and networking in IoT and blockchain applications," centers on the integration of blockchain technologies with IoT to improve security in various network settings. The recurrent terms such as IoT, blockchain, security, network, device, smart, application, challenge, technology, and data highlight a focus on solving complex security issues inherent to IoT networks using blockchain technologies. An essential aspect of this topic involves the discussion of security issues related to IoT and blockchain. For instance, Refs. [126,127], review the current state of IoT security, detailing the main threats and possible solutions, and highlight the importance of blockchain in enhancing IoT security. The role of blockchain in securing IoT applications is another prominent theme. For instance, the study of [128] proposes a blockchain-based networking solution for IoT devices that minimizes bandwidth overhead, computational cost, and delays related to conventional blockchain implementations while maintaining an important level of security and privacy advantages. Moreover, some research emphasizes the role of Software Defined Networking (SDN) and Network Function Virtualization (NFV) in the IoT context, as exemplified by Refs. [129, 130]. These studies reflect the growing interest in the interplay of these technologies in enhancing the security and efficiency of IoT systems.

Overall, Topic 13 highlights the ongoing research efforts to enhance security and networking in IoT and blockchain applications. It underlines the potential of blockchain technology in addressing the security issues associated with IoT networks. Future research directions for this topic could include:

1. Exploring novel blockchain-based solutions to enhance IoT security in various settings, including smart homes, smart cities, and healthcare systems.
2. Investigating the interoperability issues and challenges in the integration of blockchain, IoT, SDN, and NFV.
3. Developing efficient networking architectures leveraging blockchain for handling large-scale IoT systems.
4. Studying the implications of blockchain adoption in terms of IoT network performance and scalability.
5. Evaluating the role of blockchain in securing different IoT applications, considering various threats and attacks.

4.14. Blockchain, IoT, and energy efficiency in wireless sensor networks (WSNs)

Topic 14, labeled as "Blockchain, IoT, and energy efficiency in wireless sensor networks (WSNs)," encompasses studies exploring the implementation and potential advantages of blockchain and IoT within wireless sensor networks (WSNs), particularly with respect to improving energy efficiency and enhancing security. Key terms such as node, WSNs, energy, routing, network, cluster, sensor, blockchain, data, and trust highlight the primary areas of interest within this topic. The papers on this topic indicate a focus on technical aspects such as energy-aware routing protocols, clustering, security, and trust mechanisms, which are essential components for efficient and secure wireless sensor networks. One prevalent theme within this topic is the application of blockchain in improving the security of WSNs. For example, Ref. [131] introduce a novel algorithm that employs blockchain technology to enhance the security and accuracy of localization in hostile WSNs by evaluating and sharing trust values of beacon through blockchain. Simulation results confirm the effectiveness of the proposed algorithm in comparison to existing approaches [132]. address the vulnerabilities in the RPL routing protocol in IoT-LLNs (Low Power and Lossy Networks) and propose an IoT routing security model that utilizes blockchain technology. With the support of blockchain and smart contracts, real-time alerts can be generated to detect sensor nodes that tamper with LLN configuration information, thereby enhancing routing security. The findings emphasize the potential of blockchain in enhancing the security and integrity of IoT routing in LLNs. Furthermore, energy efficiency in wireless sensor networks is another significant area of research on this topic. Relatedly, the studies of [133,134] suggest a focus on developing energy-efficient routing protocols in WSNs, potentially using blockchain technology. Moreover, some studies explore the intersection of blockchain, IoT, and other technologies or methodologies. For instance, the paper [135] explores the integration of machine learning and blockchain for improved node detection and data storage in WSNs. To recap, Topic 14 underlines the incorporation of blockchain and IoT in WSN, emphasizing energy efficiency and security enhancements. Future research directions might include:

1. Examining the impact of blockchain on the energy consumption of WSNs.
2. Investigating novel blockchain-based routing protocols for improved energy efficiency in WSNs.
3. Studying the role of blockchain in enhancing the security of IoT-enabled WSNs.
4. Exploring the integration of blockchain and IoT with other emerging technologies, such as machine learning and AI, for better WSN performance.
5. Evaluating real-world applications and challenges of implementing blockchain in WSNs.

5. Conclusions

Digitalization has become an integral part of modern human life, impacting every aspect of our daily activities. As we navigate through the 21st century, we are increasingly reliant on digital technologies for communication, work, healthcare, education, and even entertainment. This digital era has cultivated an environment where technology is not just a tool, but a fundamental component of our society, facilitating unprecedented levels of convenience, efficiency, and global connectivity. Among these technologies, IoT has emerged as a game-changer. IoT signifies the interconnection of physical devices through the internet, enabling these devices to gather, analyze, and exchange data in real-time. IoT plays an indispensable role in various sectors, including transportation, healthcare, agriculture, and smart cities, to name a few. It brings about enhanced efficiency, improved decision-making, and a heightened level of automation and control, thus substantially transforming our living and working environments. Despite the vast and intricate landscape of IoT, the broader application and expansion of the technology are not devoid of challenges. Paramount among these challenges are issues related to security, privacy, and data integrity. As IoT devices multiply, the amount of data generated also increases exponentially. However, these devices are often low-powered with limited computational resources, making them vulnerable to various forms of cyber attacks. Furthermore, the proliferation of IoT also brings forth concerns regarding privacy. With vast amounts of personal data being collected, processed, and stored by IoT devices, there is growing apprehension about data misuse and unauthorized access.

However, the entrance of blockchain technology presents a promising antidote to these challenges. With its innate features of decentralization, immutability, and transparency, blockchain emerges as a critical component in reinforcing the IoT infrastructure. Blockchain operates on a decentralized network, which means that there is no single point of failure susceptible to attacks. This, in turn, enhances the robustness of the system and reduces the potential for single points of data manipulation. The immutability of blockchain, where data, once entered, cannot be altered or deleted, bolsters data integrity. This ensures that IoT data remains trustworthy and verifiable over time. The transparency of blockchain also allows every transaction to be traceable, visible, and hence, accountable. Such transparency facilitates auditability and enhances trust among system users. The integration of blockchain with IoT forms a powerful alliance that guarantees the secure storage and transmission of data. This symbiotic relationship fosters trust and confidence in IoT systems, which is essential for their wider adoption and acceptance. It is a shift from a model of centralized trust, often dependent on a single entity, to a decentralized model where trust is distributed and shared among network participants. Beyond securing data and improving trust, the fusion of blockchain and IoT is transformative. It is poised to revolutionize various domains by creating a secure and decentralized environment for device-to-device communication, thereby enhancing the autonomy of IoT devices. The employment of smart contracts - self-executing contracts with terms directly written into code - can facilitate seamless interactions between devices without the need for third-party intervention. This increased automation can significantly streamline IoT operations and open up new avenues for innovation.

Although the intersection of blockchain and IoT is burgeoning with potential, there seems to be a dearth of data-driven reviews exploring this synergy, specifically using sophisticated methods like Latent Dirichlet Allocation (LDA). As a powerful form of topic modeling, LDA can provide valuable insights by identifying latent patterns and topics within vast amounts of text data. As a data-driven tool, it has the potential to explore the nuances and themes in the emerging blockchain and IoT literature, offering a comprehensive overview that could inform researchers, technologists, and decision-makers.

Drawing on a sample of 4455 publications, this review reveals that the interdisciplinary field of IoT and blockchain technology has experienced an extraordinary journey, starting from just five publications in 2016 to an unprecedented high of 1574 in 2022. This dramatic growth showcases the burgeoning academic interest in this fusion, transitioning from an emergent exploration to a mature, innovative discourse, indicating a vibrant research landscape ready for future breakthroughs. Moreover, the research field of IoT and blockchain is predominantly populated by technical and interdisciplinary publications, with the renowned technology association IEEE leading the discourse through its highly productive journals. This trend, highlighting the strong emphasis on technical development and application, not only reveals the perceived technological importance of the IoT-blockchain intersection but also promises a vibrant future for this interdisciplinary domain as researchers continue to navigate its complexities and potential. The application of the LDA technique uncovered 14 topics within the corpus of IoT and blockchain research: 1) Security and authentication in blockchain-based IoT networks, 2) Access control and management in blockchain-based IoT systems, 3) Blockchain and IoT integration in supply chain management, 4) Federated learning and blockchain in smart systems, 5) Blockchain in IoT and IIoT for data security and privacy, 6) Blockchain consensus algorithms and security in IIoT, 7) Blockchain and edge computing in IoT, 8) Blockchain in healthcare data management and security, 9) Blockchain in energy systems and trading, 10) Blockchain in IoT systems and next-generation networks, 11) Blockchain in supply chain and transportation systems, 12) Blockchain and IoT applications in smart cities, 13) Security and networking in IoT and blockchain applications, and 14) Blockchain, IoT, and energy efficiency in wireless sensor networks (WSN). According to the LDA model, the IoT-blockchain literature was predominately focused on Topics 8 and 3. This pronounced focus reflects the direct applicability and transformative potential of blockchain and IoT convergence in these two critical domains. For Topic 3, "Blockchain and IoT integration in supply chain management", the research concentration indicates an acknowledgment of the challenges in current supply chain systems, such as transparency, traceability, and efficiency. Due to its immutable and decentralized nature, blockchain technology brings a high degree of trust and visibility to the supply chain, thus enabling better traceability of goods and transactions. Meanwhile, IoT can enhance real-time monitoring capabilities, ensuring the seamless and timely flow of goods. Together, these technologies could lead to more efficient, secure, and resilient supply chain systems, driving improvements in areas like product authenticity verification, demand forecasting, and inventory management. The intense focus on this topic signifies the importance of technology-driven solutions in optimizing supply chain operations, reflecting an evolving research trend toward integrated and intelligent supply chain management. Turning to Topic 8, "Blockchain in healthcare data management and security," the high volume of research underscores the urgent need for secure and privacy-preserving solutions in healthcare data management, a requirement made more pressing by the digital transformation in healthcare, characterized by Electronic Health Records (EHRs), telemedicine, and health IoT devices. The vast amount of sensitive health data generated can be securely managed and shared using blockchain, ensuring data integrity and patient privacy. The integration of blockchain with IoT also opens up opportunities for real-time patient monitoring and personalized care. Furthermore, it can foster a more patient-centric healthcare model by giving patients control over their data. The concentrated research on this topic reflects the growing realization of the potential of blockchain and IoT to resolve longstanding issues in healthcare data management and to drive patient-centered, data-driven healthcare models. Thus, the heavy concentration of literature on these two topics underlines the academic and practical recognition of the transformative impact of blockchain and IoT integration in supply chain management and healthcare, two sectors that are critical to societal wellbeing and economic functioning. This analysis also suggests the likely future trajectory of research in this area, hinting at potential research gaps and unexplored possibilities in other domains.

The lesser representation of Topics 2, 14, and 9 in the corpus might initially seem surprising, but it also signals potential opportunities for deeper exploration and greater innovation in these areas. Topic 2, which revolves around "Access control and management in blockchain-based IoT systems," has received relatively less attention. A possible explanation for this could be the inherently complex nature of devising efficient and secure access control mechanisms in decentralized IoT networks. It might also point to a greater focus on more immediate, overarching security issues associated with IoT and blockchain. However, the underemphasis on this topic could overlook the nuanced and crucial role of access control in the broader security architecture, which can have profound implications for user privacy and data integrity. In addition, Topic 14, "Blockchain, IoT, and energy efficiency in wireless sensor networks (WSN)," might not have received as much focus due to the highly specialized nature of the topic. Integrating energy efficiency with blockchain and WSN in IoT might require interdisciplinary expertise that bridges not only information technology and blockchain, but also energy systems and networking. Moreover, the topic's practical applications might be seen as confined to specific industries or sectors, leading to a lower general interest. Therefore, the unique combination of these technologies could offer unprecedented opportunities to improve the sustainability and efficiency of IoT systems, an aspect of growing importance in the age of environmental consciousness. Finally, the lower emphasis on Topic 9, "Blockchain in energy systems and trading," could suggest that the integration of blockchain into the energy sector is still in its nascent stage. This might be due to regulatory hurdles, technical challenges, and the historical inertia of traditional energy systems. With global climate commitments and the increasing feasibility of decentralized energy systems, there may be substantial opportunities in the near future for blockchain to revolutionize this sector, thereby warranting more scholarly attention.

Although this study is comprehensive, it is not without its limitations. Firstly, the reliance on the LDA method as a powerful tool for topic modeling may not perfectly distinguish between topics, especially when they are closely related or overlapping. Therefore, this may lead to a lack of precision in topic identification. Secondly, our review was confined to English language research articles indexed by the Scopus database. Consequently, the review may exclude relevant research published in other languages or in non-indexed journals, potentially introducing a language and indexing bias. Moreover, the time frame of the study extends only up until early 2023, meaning that the latest developments and trends may not be captured. Finally, given the fast-paced evolution of blockchain and IoT technologies, certain emerging topics and novel applications might not have been fully incorporated in the current review. As a result, there is a need for continuous updating and reviewing. Despite these limitations, we believe our study provides valuable insights and a comprehensive overview of the research landscape at the convergence of blockchain and IoT.

Declaration of competing interest

We declare that we have no conflicts of interest related to the research presented in this article.

References

[1] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, B. Adebisi, Towards green computing for Internet of things: energy oriented path and message scheduling approach, Sustain. Cities Soc. 38 (2018) 195–204, https://doi.org/10.1016/j.scs.2017.12.018.

[2] Y.L. Cheng, M.H. Lim, K.H. Hui, Impact of internet of things paradigm towards energy consumption prediction: a systematic literature review, Sustain. Cities Soc. 78 (2022), 103624, https://doi.org/10.1016/j.scs.2021.103624.

[3] S.A. Khowaja, A.G. Prabono, F. Setiawan, B.N. Yahya, S.-L. Lee, Contextual activity based Healthcare Internet of Things, Services, and People (HIoTSP): an architectural framework for healthcare monitoring using wearable sensors, Comput. Network. 145 (2018) 190–206, https://doi.org/10.1016/j.comnet.2018.09.003.

[4] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, S. Zailani, Internet of Things research in supply chain management and logistics: a bibliometric analysis, Internet of Things 12 (2020), 100318, https://doi.org/10.1016/j.iot.2020.100318.

[5] M. Ben-Daya, E. Hassini, Z. Bahroun, Internet of things and supply chain management: a literature review, Int. J. Prod. Res. 57 (2019) 4719–4742, https://doi.org/10.1080/00207543.2017.1402140.

[6] F. Xhafa, B. Kilic, P. Krause, Evaluation of IoT stream processing at edge computing layer for semantic data enrichment, Future Generat. Comput. Syst. 105 (2020) 730–736, https://doi.org/10.1016/j.future.2019.12.031.

[7] A. Poniszewska-Maranda, D. Kaczmarek, N. Kryvinska, F. Xhafa, Studying usability of AI in the IoT systems/paradigm through embedding NN techniques into mobile smart service system, Computing 101 (2019) 1661–1685, https://doi.org/10.1007/s00607-018-0680-z.

[8] A. Sula, E. Spaho, K. Matsuo, L. Barolli, F. Xhafa, R. Miho, A new system for supporting children with autism spectrum disorder based on IoT and P2P technology, Int. J. Space-Based Situated Comput. 4 (2014) 55–64, https://doi.org/10.1504/IJSSC.2014.060688.

[9] A. French, J. Shim, The digital revolution: internet of things, 5G, and beyond, Commun. Assoc. Inf. Syst. 38 (2016), https://doi.org/10.17705/1CAIS.03840.

[10] O. Mazhelis, E. Luoma, H. Warma, Defining an internet-of-things ecosystem, in: S. Andreev, S. Balandin, Y. Koucheryavy (Eds.), Internet of Things, Smart Spaces, and Next Generation Networking, Springer, Berlin, Heidelberg, 2012, pp. 1–14, https://doi.org/10.1007/978-3-642-32686-8_1.

[11] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, M. Iranmanesh, The Internet of Things (IoT) in healthcare: taking stock and moving forward, Internet of Things 22 (2023), 100721, https://doi.org/10.1016/j.iot.2023.100721.

[12] B.L. Risteska Stojkoska, K.V. Trivodaliev, A review of Internet of Things for smart home: challenges and solutions, J. Clean. Prod. 140 (2017) 1454–1464, https://doi.org/10.1016/j.jclepro.2016.10.006.

[13] M. Alaa, A.A. Zaidan, B.B. Zaidan, M. Talal, M.L.M. Kiah, A review of smart home applications based on Internet of Things, J. Netw. Comput. Appl. 97 (2017) 48–65, https://doi.org/10.1016/j.jnca.2017.08.017.

[14] A. Rejeb, Z. Suhaiza, K. Rejeb, S. Seuring, H. Treiblmaier, The Internet of Things and the circular economy: a systematic literature review and research agenda, J. Clean. Prod. 350 (2022), 131439, https://doi.org/10.1016/j.jclepro.2022.131439.

[15] B. Jan, H. Farman, M. Khan, M. Talha, I.U. Din, Designing a smart transportation system: an internet of things and big data approach, IEEE Wireless Commun. 26 (2019) 73–79, https://doi.org/10.1109/MWC.2019.1800512.

[16] A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, S. Zailani, The Big Picture on the Internet of Things and the Smart City: a Review of what We Know and what We Need to Know, vol. 19, Internet of Things, Netherlands, 2022, https://doi.org/10.1016/j.iot.2022.100565.

[17] A. Rejeb, K. Rejeb, S. Zailani, H. Treiblmaier, K.J. Hand, Integrating the Internet of Things in the Halal Food Supply Chain: A Systematic Literature Review and Research Agenda, vol. 13, Internet of Things (Netherlands), 2021, https://doi.org/10.1016/j.iot.2021.100361.

[18] R.H. Weber, Internet of Things – new security and privacy challenges, Comput. Law Secur. Rep. 26 (2010) 23–30, https://doi.org/10.1016/j.clsr.2009.11.008.

[19] J.H. Ziegeldorf, O.G. Morchon, K. Wehrle, Privacy in the internet of things: threats and challenges, Secur. Commun. Network. 7 (2014) 2728–2742, https://doi.org/10.1002/sec.795.

[20] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wireless Network 20 (2014) 2481–2501, https://doi.org/10.1007/s11276-014-0761-7.

[21] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28, https://doi.org/10.1016/j.jnca.2017.04.002.

[22] A. Rejeb, J.G. Keogh, H. Treiblmaier, Leveraging the internet of things and blockchain technology in supply chain management, Future Internet 11 (2019) 161, https://doi.org/10.3390/fi11070161.

[23] A. Rejeb, J.G. Keogh, S.J. Simske, T. Stafford, H. Treiblmaier, Potentials of blockchain technologies for supply chain collaboration: a conceptual framework, Int. J. Logist. Manag. 32 (2021) 973–994, https://doi.org/10.1108/IJLM-02-2020-0098.

[24] B. Bera, D. Chattaraj, A.K. Das, Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment, Comput. Commun. 153 (2020) 229–249, https://doi.org/10.1016/j.comcom.2020.02.011.

[25] E.F. Jesus, V.R.L. Chicarino, C.V.N. de Albuquerque, A.A. de A. Rocha, A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack, Security and Communication Networks, 2018, e9675050, https://doi.org/10.1155/2018/9675050, 2018.

[26] M. El-Masri, E.M.A. Hussain, Blockchain as a mean to secure Internet of Things ecosystems – a systematic literature review, J. Enterprise Inf. Manag. 34 (2021) 1371–1405, https://doi.org/10.1108/JEIM-12-2020-0533.

[27] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun. 136 (2019) 10–29, https://doi.org/10.1016/j.comcom.2019.01.006.

[28] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: research issues and challenges, IEEE Internet Things J. 6 (2019) 2188–2204, https://doi.org/10.1109/JIOT.2018.2882794.

[29] W. Viriyasitavat, T. Anuphaptrirong, D. Hoonsopon, When blockchain meets Internet of Things: characteristics, challenges, and business opportunities, Journal of Industrial Information Integration 15 (2019) 21–28, https://doi.org/10.1016/j.jii.2019.05.002.

[30] W. Viriyasitavat, L.D. Xu, Z. Bi, D. Hoonsopon, Blockchain technology for applications in internet of things—mapping from system design perspective, IEEE Internet Things J. 6 (2019) 8155–8168, https://doi.org/10.1109/JIOT.2019.2925825.

[31] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001, https://doi.org/10.1109/ACCESS.2018.2842685.

[32] A. Rejeb, K. Rejeb, A. Appolloni, Y. Kayikci, M. Iranmanesh, The landscape of public procurement research: a bibliometric analysis and topic modelling based on Scopus, J. Public Procure. (2023), https://doi.org/10.1108/JOPP-06-2022-0031 ahead-of-print.

[33] Y. Guo, S.J. Barnes, Q. Jia, Mining meaning from online ratings and reviews: tourist satisfaction analysis using latent dirichlet allocation, Tourism Manag. 59 (2017) 467–483, https://doi.org/10.1016/j.tourman.2016.09.009.

[34] D.M. Blei, Probabilistic topic models, Commun. ACM 55 (2012) 77–84, https://doi.org/10.1145/2133806.2133826.

[35] R.-T. Li, K.A. Khor, L.-G. Yu, Identifying indicators of progress in thermal spray research using bibliometrics analysis, J. Therm. Spray Technol. 25 (2016) 1526–1533, https://doi.org/10.1007/s11666-016-0445-1.

[36] S. Moro, P. Cortez, P. Rita, Business intelligence in banking: a literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation, Expert Syst. Appl. 42 (2015) 1314–1324, https://doi.org/10.1016/j.eswa.2014.09.024.

[37] L. Ligorio, A. Venturelli, F. Caputo, Tracing the boundaries between sustainable cities and cities for sustainable development, An LDA analysis of management studies, Technological Forecasting and Social Change 176 (2022), 121447, https://doi.org/10.1016/j.techfore.2021.121447.

[38] B. Fahimnia, J. Sarkis, H. Davarzani, Green supply chain management: a review and bibliometric analysis, Int. J. Prod. Econ. 162 (2015) 101–114, https://doi.org/10.1016/j.ijpe.2015.01.003.

[39] A.K. McCallum, Mallet: A Machine Learning for Languagetoolkit, 2002. Mallet. Cs. Umass. Edu.

[40] D.M. Blei, A.Y. Ng, M.I. Jordan, Latent dirichlet allocation, J. Mach. Learn. Res. 3 (2003) 993–1022.

[41] M. Aria, C. Cuccurullo, bibliometrix: an R-tool for comprehensive science mapping analysis, Journal of Informetrics 11 (2017) 959–975, https://doi.org/10.1016/j.joi.2017.08.007.

[42] A. Caputo, S. Pizzi, M.M. Pellegrini, M. Dabić, Digitalization and business models: where are we going? A science map of the field, J. Bus. Res. 123 (2021) 489–501, https://doi.org/10.1016/j.jbusres.2020.09.053.

[43] A. Rejeb, H. Treiblmaier, K. Rejeb, S. Zailani, Blockchain research in healthcare: a bibliometric review and current research trends, J. of Data, Inf. and Manag. 3 (2021) 109–124, https://doi.org/10.1007/s42488-021-00046-2.

[44] C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, Blockchain technology in healthcare: a systematic review, Healthcare 7 (2019) 56, https://doi.org/10.3390/healthcare7020056.

[45] A. Sharma, S. Kaur, M. Singh, A comprehensive review on blockchain and Internet of Things in healthcare, Transactions on Emerging Telecommunications Technologies 32 (2021) e4333, https://doi.org/10.1002/ett.4333.

[46] K.P. Satamraju, M. B, Proof of concept of scalable integration of internet of things and blockchain in healthcare, Sensors 20 (2020) 1389, https://doi.org/10.3390/s20051389.

[47] M. Kouhizadeh, S. Saberi, J. Sarkis, Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers, Int. J. Prod. Econ. 231 (2021), 107831, https://doi.org/10.1016/j.ijpe.2020.107831.

[48] C. Sievert, K. Shirley, LDAvis: a method for visualizing and interpreting topics, in: Proceedings of the Workshop on Interactive Language Learning, Visualization, and Interfaces, 2014, pp. 63–70.

[49] A. Khatoon, P. Verma, J. Southernwood, B. Massey, P. Corcoran, Blockchain in energy efficiency: potential applications and benefits, Energies 12 (2019) 3317, https://doi.org/10.3390/en12173317.

[50] M. Schletz, A. Cardoso, G. Prata Dias, S. Salomo, How can blockchain technology accelerate energy efficiency interventions? A use case comparison, Energies 13 (2020) 5869, https://doi.org/10.3390/en13225869.

[51] S. Javed, M.A. Khan, A.M. Abdullah, A. Alsirhani, A. Alomari, F. Noor, I. Ullah, An efficient authentication scheme using blockchain as a certificate authority for the internet of drones, Drones 6 (2022) 264, https://doi.org/10.3390/drones6100264.

[52] X. Wang, C. Gu, F. Wei, S. Lu, Z. Li, A Certificateless-Based Authentication and Key Agreement Scheme for IIoT Cross-Domain, Security and Communication Networks, 2022, e3693748, https://doi.org/10.1155/2022/3693748, 2022.

[53] G. Mwitende, Y. Ye, I. Ali, F. Li, Certificateless authenticated key agreement for blockchain-based WBANs, J. Syst. Architect. 110 (2020), 101777, https://doi.org/10.1016/j.sysarc.2020.101777.

[54] Y. Qi, Z. Yang, Y. Luo, Y. Huang, X. Li, Blockchain-based light-weighted provable data possession for low performance devices, CMC-COMPUTERS MATERIALS & CONTINUA 73 (2022) 2205–2221.

[55] K. Fasila, S. Mathew, Fast and efficient security scheme for blockchain-based IoT networks, Comput. Mater. Continua (CMC) 73 (2022) 2097–2114.

[56] W. Jiang, E. Li, W. Zhou, Y. Yang, T. Luo, IoT access control model based on blockchain and trusted execution environment, Processes 11 (2023) 723, https://doi.org/10.3390/pr11030723.

[57] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan, Smart contract-based access control for the internet of things, IEEE Internet Things J. 6 (2019) 1594–1605, https://doi.org/10.1109/JIOT.2018.2847705.

[58] L. Song, X. Ju, Z. Zhu, M. Li, An access control model for the Internet of Things based on zero-knowledge token and blockchain, EURASIP J. Wirel. Commun. Netw. 2021 (2021) 105, https://doi.org/10.1186/s13638-021-01986-4.

[59] Y. Sen Gupta, S. Mukherjee, R. Dutta, S. Bhattacharya, A blockchain-based approach using smart contracts to develop a smart waste management system, Int. J. Environ. Sci. Technol. 19 (2022) 7833–7856, https://doi.org/10.1007/s13762-021-03507-8.

[60] M. Saad, M.K. Khan, M.B. Ahmad, Blockchain-enabled vehicular Ad hoc networks: a systematic literature review, Sustainability 14 (2022) 3919, https://doi.org/10.3390/su14073919.

[61] M. Torky, A.E. Hassanein, Integrating blockchain and the internet of things in precision agriculture: analysis, opportunities, and challenges, Comput. Electron. Agric. 178 (2020), 105476, https://doi.org/10.1016/j.compag.2020.105476.

[62] X. Li, D. Huang, Research on Value Integration Mode of Agricultural E-Commerce Industry Chain Based on Internet of Things and Blockchain Technology, Wireless Communications and Mobile Computing, 2020, e8889148, https://doi.org/10.1155/2020/8889148, 2020.

[63] W. Ren, X. Wan, P. Gan, A double-blockchain solution for agricultural sampled data security in Internet of Things network, Future Generat. Comput. Syst. 117 (2021) 453–461, https://doi.org/10.1016/j.future.2020.12.007.

[64] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, X. Cheng, NormaChain: a blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce, IEEE Internet Things J. 6 (2019) 4680–4693, https://doi.org/10.1109/JIOT.2018.2877634.

[65] R.S. Chaudhari, S.K. Mahajan, S.B. Rane, R. Agrawal, Modeling barriers in circular economy using TOPSIS: perspective of environmental sustainability & blockchain-IoT technology, International Journal of Mathematical, Engineering and Management Sciences 7 (2022) 820–843, https://doi.org/10.33889/IJMEMS.2022.7.6.052.

[66] J. Sun, H. Jiao, Emerging IT investments and firm performance: a perspective of the digital options, Chinese Management Studies. ahead-of-print. https://doi.org/10.1108/CMS-09-2022-0335, 2023.

[67] A. Stroumpoulis, E. Kopanaki, Theoretical perspectives on sustainable supply chain management and digital transformation: a literature review and a conceptual framework, Sustainability 14 (2022) 4862, https://doi.org/10.3390/su14084862.

[68] P.M. Reyes, M.J. Gravier, P. Jaska, J.K. Visich, Blockchain impacts on global supply chain operational and managerial business value processes, IEEE Eng. Manag. Rev. 50 (2022) 123–140, https://doi.org/10.1109/EMR.2022.3187729.

[69] S. Salim, B. Turnbull, N. Moustafa, A blockchain-enabled explainable federated learning for securing internet-of-things-based social media 3.0 networks, IEEE Transactions on Computational Social Systems (2021) 1–17, https://doi.org/10.1109/TCSS.2021.3134463.

[70] I. Sreedevi Shashank, Distributed network of adaptive and self-reconfigurable active vision systems, Symmetry 14 (2022) 2281, https://doi.org/10.3390/sym14112281.

[71] L. Feng, Y. Zhao, S. Guo, X. Qiu, W. Li, P. Yu, BAFL: a blockchain-based asynchronous federated learning framework, IEEE Trans. Comput. 71 (2022) 1092–1103, https://doi.org/10.1109/TC.2021.3072033.

[72] M. Shen, H. Wang, B. Zhang, L. Zhu, K. Xu, Q. Li, X. Du, Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing, IEEE Internet Things J. 8 (2021) 2265–2275, https://doi.org/10.1109/JIOT.2020.3028110.

[73] D. Unal, M. Hammoudeh, M.A. Khan, A. Abuarqoub, G. Epiphaniou, R. Hamila, Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things, Comput. Secur. 109 (2021), 102393, https://doi.org/10.1016/j.cose.2021.102393.

[74] S. Alam, S. Zardari, J.A. Shamsi, Blockchain-based trust and reputation management in SIoT, Electronics 11 (2022) 3871, https://doi.org/10.3390/electronics11233871.

[75] A. Raza, L. Hardy, E. Roehrer, S. Yeom, B.H. Kang, GPSPiChain-blockchain and AI based self-contained anomaly detection family security system in smart home, J. Syst. Sci. Syst. Eng. 30 (2021) 433–449, https://doi.org/10.1007/s11518-021-5496-2.

[76] P. Zheng, Y. Rao, NetDDS, A real-time interactive platform based on the publish-subscribe mechanism, recent advances in electrical & electronic engineering (formerly recent patents on, Electr. Electron. Eng. 15 (2022) 116–126.

[77] Y. Li, L. Li, Y. Zhao, N. Guizani, Y. Yu, X. Du, Toward decentralized fair data trading based on blockchain, IEEE Network 35 (2021) 304–310, https://doi.org/10.1109/MNET.011.2000349.

[78] Y. Kurt Peker, X. Rodriguez, J. Ericsson, S.J. Lee, A.J. Perez, A cost analysis of internet of things sensor data storage on blockchain via smart contracts, Electronics 9 (2020) 244, https://doi.org/10.3390/electronics9020244.

[79] X. Cai, L. Zhou, F. Li, Y. Fu, P. Zhao, C. Li, F.R. Yu, An incentive mechanism for vehicular crowdsensing with security protection and data quality assurance, IEEE Trans. Veh. Technol. (2023), https://doi.org/10.1109/TVT.2023.3262800, 1–15.

[80] Y. Jiang, Y. Zhong, X. Ge, Smart contract-based data commodity transactions for industrial internet of things, IEEE Access 7 (2019) 180856–180866, https://doi.org/10.1109/ACCESS.2019.2959771.

[81] X. Wang, J. Sun, C. Hu, P. Yu, B. Zhang, D. Hou, EtherFuzz: mutation fuzzing smart contracts for TOD vulnerability detection, Wireless Commun. Mobile Comput. (2022), e1565007, https://doi.org/10.1155/2022/1565007, 2022.

[82] H.J. Jo, W. Choi, BPRF: blockchain-based privacy-preserving reputation framework for participatory sensing systems, PLoS One 14 (2019), e0225688, https://doi.org/10.1371/journal.pone.0225688.

[83] M. Alessi, A. Camillò, E. Giangreco, M. Matera, S. Pino, D. Storelli, A decentralized personal data store based on Ethereum: towards GDPR compliance, Journal of Communications Software and Systems 15 (2019) 79–88, https://doi.org/10.24138/jcomss.v15i2.696.

[84] W. Zhang, J. Zhang, Y. Shi, J. Feng, UIV-TSP, A blockchain-enabled antileakage sharing protection scheme for undisclosed IIoT vulnerabilities, Secur. Commun. Network. (2022), e2500213, https://doi.org/10.1155/2022/2500213, 2022.

[85] A. Maw, S. Adepu, A. Mathur, Ics-BlockOpS, Blockchain for operational data security in industrial control system, Pervasive Mob. Comput. 59 (2019), 101048, https://doi.org/10.1016/j.pmcj.2019.101048.

[86] A. Dixit, A. Singh, Y. Rahulamathavan, M. Rajarajan, Fast data: a fair, secure, and trusted decentralized IIoT data marketplace enabled by blockchain, IEEE Internet Things J. 10 (2023) 2934–2944, https://doi.org/10.1109/JIOT.2021.3120640.

[87] J. Yoon, H.W. Park, Pattern and trend of scientific knowledge production in North Korea by a semantic network analysis of papers in journal titled technological innovation, Scientometrics 124 (2020) 1421–1438, https://doi.org/10.1007/s11192-020-03497-3.

[88] W. Jiang, X. Wu, M. Song, J. Qin, Z. Jia, A scalable Byzantine Fault Tolerance algorithm based on a tree topology network, IEEE Access 11 (2023) 33509–33519, https://doi.org/10.1109/ACCESS.2023.3264011.

[89] M. Feng, J. Zheng, S. He, J. Xie, Y. Chen, CRBFT: an optimized blockchain algorithm for edge-based IoT system, IEEE Sensor. J. 22 (2022) 23200–23208, https://doi.org/10.1109/JSEN.2022.3215152.

[90] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, A. Altameem, T. Altameem, R. Sharma, F.-E. Turcanu, M.S. Raboaca, Blockchain and IoT-driven optimized consensus mechanism for electric vehicle scheduling at charging stations, Sustainability 14 (2022), 12800, https://doi.org/10.3390/su141912800.

[91] X. Jiang, A. Sun, Y. Sun, H. Luo, M. Guizani, A trust-based hierarchical consensus mechanism for consortium blockchain in smart grid, Tsinghua Sci. Technol. 28 (2023) 69–81, https://doi.org/10.26599/TST.2021.9010074.

[92] M.B.E. Sajid, S. Ullah, N. Javaid, I. Ullah, A.M. Qamar, F. Zaman, Exploiting machine learning to detect malicious nodes in intelligent sensor-based systems using blockchain, Wireless Commun. Mobile Comput. (2022), e7386049, https://doi.org/10.1155/2022/7386049, 2022.

[93] M. Abdel-Basset, R. Mohamed, O.M. Elkomy, Knapsack Cipher-based metaheuristic optimization algorithms for cryptanalysis in blockchain-enabled internet of things systems, Ad Hoc Netw. 128 (2022), 102798, https://doi.org/10.1016/j.adhoc.2022.102798.

[94] Y. Fan, L. Wang, W. Wu, D. Du, Cloud/edge computing resource allocation and pricing for mobile blockchain: an iterative greedy and search approach, IEEE Transactions on Computational Social Systems 8 (2021) 451–463, https://doi.org/10.1109/TCSS.2021.3049152.

[95] E. Ślapak, J. Gazda, W. Guo, T. Maksymyuk, M. Dohler, Cost-effective resource allocation for multitier mobile edge computing in 5G mobile networks, IEEE Access 9 (2021) 28658–28672, https://doi.org/10.1109/ACCESS.2021.3059029.

[96] Y. Zuo, S. Jin, S. Zhang, Computation offloading in untrusted MEC-aided mobile blockchain IoT systems, IEEE Trans. Wireless Commun. 20 (2021) 8333–8347, https://doi.org/10.1109/TWC.2021.3091861.

[97] Y. Zuo, S. Jin, S. Zhang, Y. Zhang, Blockchain storage and computation offloading for cooperative mobile-edge computing, IEEE Internet Things J. 8 (2021) 9084–9098, https://doi.org/10.1109/JIOT.2021.3056656.

[98] A. Muthanna, A.A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, A. Koucheryavy, Secure and reliable IoT networks using fog computing with software-defined networking and blockchain, J. Sens. Actuator Netw. 8 (2019) 15, https://doi.org/10.3390/jsan8010015.

[99] C. Li, L. Zhang, S. Fang, EntrapNet: a blockchain-based verification protocol for trustless computing, IEEE Internet Things J. 9 (2022) 8024–8035, https://doi.org/10.1109/JIOT.2021.3124007.

[100] L. Cui, S. Yang, Z. Chen, Y. Pan, Z. Ming, M. Xu, A decentralized and trusted edge computing platform for internet of things, IEEE Internet Things J. 7 (2020) 3910–3922, https://doi.org/10.1109/JIOT.2019.2951619.

[101] A. Sengupta, H. Subramanian, User control of personal mHealth data using a mobile blockchain app: design science perspective, JMIR MHealth and UHealth 10 (2022), e32104, https://doi.org/10.2196/32104.

[102] Z. Chen, W. Xu, B. Wang, H. Yu, A blockchain-based preserving and sharing system for medical data privacy, Future Generat. Comput. Syst. 124 (2021) 338–350, https://doi.org/10.1016/j.future.2021.05.023.

[103] H. Kaur, R. Jameel, M.A. Alam, B. Alankar, V. Chang, Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography, J. Enterprise Inf. Manag. (2023), https://doi.org/10.1108/JEIM-02-2021-0084 ahead-of-print.

[104] P. Chinnasamy, A. Albakri, M. Khan, A.A. Raja, A. Kiran, J.C. Babu, Smart contract-enabled secure sharing of health data for a mobile cloud-based E-health system, Appl. Sci. 13 (2023) 3970, https://doi.org/10.3390/app13063970.

[105] M. Afzal, Q. Huang, W. Amin, K. Umer, A. Raza, M. Naeem, Blockchain enabled distributed demand side management in community energy system with smart homes, IEEE Access 8 (2020) 37428–37439, https://doi.org/10.1109/ACCESS.2020.2975233.

[106] J. Westphall, J.E. Martina, Blockchain privacy and scalability in a decentralized validated energy trading context with hyperledger fabric, Sensors 22 (2022) 4585, https://doi.org/10.3390/s22124585.

[107] A.A. Sadawi, B. Madani, S. Saboor, M. Ndiaye, G. Abu-Lebdeh, A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract, Technol. Forecast. Soc. Change 173 (2021), 121124, https://doi.org/10.1016/j.techfore.2021.121124.

[108] Y.-T. Lei, C.-Q. Ma, N. Mirza, Y.-S. Ren, S.W. Narayan, X.-Q. Chen, A renewable energy microgrids trading management platform based on permissioned blockchain, Energy Econ. 115 (2022), 106375, https://doi.org/10.1016/j.eneco.2022.106375.
[109] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain based decentralized management of demand response programs in smart energy grids, Sensors 18 (2018) 162, https://doi.org/10.3390/s18010162.
[110] N.R. Pradhan, A.P. Singh, S.V. Sudha, K.H.K. Reddy, D.S. Roy, Performance evaluation and cyberattack mitigation in a blockchain-enabled peer-to-peer energy trading framework, Sensors 23 (2023) 670, https://doi.org/10.3390/s23020670.
[111] H. Wei, W. Feng, C. Zhang, Y. Chen, Y. Fang, N. Ge, Creating efficient blockchains for the internet of things by coordinated satellite-terrestrial networks, IEEE Wireless Commun. 27 (2020) 104–110, https://doi.org/10.1109/MNET.001.1900326.
[112] E. Zeydan, J. Baranda, J. Mangues-Bafalluy, Y. Turk, S.B. Ozturk, Blockchain-based service orchestration for 5G vertical industries in multicloud environment, IEEE Transactions on Network and Service Management 19 (2022) 4888–4904, https://doi.org/10.1109/TNSM.2022.3194078.
[113] H. Xu, P.V. Klaine, O. Onireti, B. Cao, M. Imran, L. Zhang, Blockchain-enabled resource management and sharing for 6G communications, Digital Communications and Networks 6 (2020) 261–269, https://doi.org/10.1016/j.dcan.2020.06.002.
[114] J. Gao, B. Adjei-Arthur, E.B. Sifah, H. Xia, Q. Xia, Supply chain equilibrium on a game theory-incentivized blockchain network, Journal of Industrial Information Integration 26 (2022), 100288, https://doi.org/10.1016/j.jii.2021.100288.
[115] L. Guo, J. Chen, S. Li, Y. Li, J. Lu, A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance, Digital Communications and Networks 8 (2022) 576–587, https://doi.org/10.1016/j.dcan.2022.03.020.
[116] X.N. Zhu, G. Peko, D. Sundaram, S. Piramuthu, Blockchain-based agile supply chain framework with IoT, Inf. Syst. Front 24 (2022) 563–578, https://doi.org/10.1007/s10796-021-10114-y.
[117] V. Tsoukas, A. Gkogkidis, A. Kampa, G. Spathoulas, A. Kakarountas, Enhancing food supply chain security through the use of blockchain and TinyML, Information 13 (2022) 213, https://doi.org/10.3390/info13050213.
[118] M. Majdalawieh, N. Nizamuddin, M. Alaraj, S. Khan, A. Bani-Hani, Blockchain-based solution for secure and transparent food supply chain network, peer-to-peer netw, Apple 14 (2021) 3831–3850, https://doi.org/10.1007/s12083-021-01196-1.
[119] J. Chen, S. Xu, K. Liu, S. Yao, X. Luo, H. Wu, Intelligent transportation logistics optimal warehouse location method based on internet of things and blockchain technology, Sensors 22 (2022) 1544, https://doi.org/10.3390/s22041544.
[120] S. Kumar, R.D. Raut, P. Priyadarshinee, B.E. Narkhede, Exploring warehouse management practices for adoption of IoT-blockchain, Supply Chain Forum Int. J. 24 (2023) 43–58, https://doi.org/10.1080/16258312.2022.2082852.
[121] A.E. Azzaoui, J.H. Park, Post-quantum blockchain for a scalable smart city, J. Internet Technol. 21 (2020) 1171–1178.
[122] S. Peneti, M. Sunil Kumar, S. Kallam, R. Patan, V. Bhaskar, M. Ramachandran, Bdn-Gwmnn, Internet of things (IoT) enabled secure smart city applications, Wireless Pers. Commun. 119 (2021) 2469–2485, https://doi.org/10.1007/s11277-021-08339-w.
[123] A. Tiwari, U. Batra, IPFS enabled blockchain for smart cities, Int. j. Inf. Tecnol. 13 (2021) 201–211, https://doi.org/10.1007/s41870-020-00568-9.
[124] T. Alam, IBchain: internet of things and blockchain integration approach for secure communication in smart cities, Informatica 45 (2021), https://doi.org/10.31449/inf.v45i3.3573.
[125] M.S. Rahman, M.A.P. Chamikara, I. Khalil, A. Bouras, Blockchain-of-blockchains: an interoperable blockchain platform for ensuring IoT data integrity in smart city, Journal of Industrial Information Integration 30 (2022), 100408, https://doi.org/10.1016/j.jii.2022.100408.
[126] M. Babiker Mohamed, O. Matthew Alofe, M. Ajmal Azad, H. Singh Lallie, K. Fatema, T. Sharif, A comprehensive survey on secure software-defined network for the Internet of Things, Transactions on Emerging Telecommunications Technologies 33 (2022), e4391, https://doi.org/10.1002/ett.4391.
[127] P.M. Chanal, M.S. Kakkasageri, Security and privacy in IoT: a survey, Wireless Pers. Commun. 115 (2020) 1667–1693, https://doi.org/10.1007/s11277-020-07649-9.
[128] A. Bathula, S.K. Basha, Blockchain technology with internet of things in the real time network stream, Int. J. Recent Technol. Eng. 8 (2019) 682–689.
[129] A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S.S. Band, M. Sookhak, P. Tiwari, N. Kumar, Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions, Int. J. Commun. Syst.. n/a (n.d.) e5429. https://doi.org/10.1002/dac.5429.
[130] N.Y.-R. Douha, M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, Y. Kadobayashi, A survey on blockchain, SDN and NFV for the smart-home security, Internet of Things 20 (2022), 100588, https://doi.org/10.1016/j.iot.2022.100588.
[131] R. Goyat, G. Kumar, M.K. Rai, R. Saha, R. Thomas, T.H. Kim, Blockchain powered secure range-free localization in wireless sensor networks, Arabian J. Sci. Eng. 45 (2020) 6139–6155, https://doi.org/10.1007/s13369-020-04493-8.
[132] R. Sahay, G. Geethakumari, B. Mitra, A novel blockchain based framework to secure IoT-LLNs against routing attacks, Computing 102 (2020) 2445–2470, https://doi.org/10.1007/s00607-020-00823-8.
[133] A. Mehbodniya, J.L. Webber, R. Rani, S.S. Ahmad, I. Wattar, L. Ali, S.J. Nuagah, Energy-aware routing protocol with fuzzy logic in industrial internet of things with blockchain technology, Wireless Commun. Mobile Comput. (2022), e7665931, https://doi.org/10.1155/2022/7665931, 2022.
[134] M.P. Swapna, G. Satyavathy, Energy-aware optimal clustering and secure routing protocol for heterogeneous wireless sensor network, International Journal of Computer Networks and Applications 9 (2022) 12–21.
[135] M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran, N. Javaid, Malicious node detection using machine learning and distributed data storage using blockchain in WSNs, IEEE Access 11 (2023) 6106–6121, https://doi.org/10.1109/ACCESS.2023.3236983.



https://dspace.org/

Unleashing the power of Internet of Things and blockchain: a comprehensive analysis and future directions

Rejeb, Abderahman; Rejeb, Karim; Appolloni, Andrea; Jagtap, Sandeep; Iranmanesh, Mohammad ...

2023-07-08
Elsevier
https://doi.org/10.1016/j.iotcps.2023.06.003
Rejeb A, Rejeb K, Appolloni A, et al., (2024) Unleashing the power of Internet of Things and blockchain: a comprehensive analysis and future directions. Internet of Things and Cyber-Physical Systems, Volume 4, 2024, pp. 1-18

Downloaded from a DSpace repository. https://dspace.org/