Journal of Open Innovation: Technology, Market, and Complexity

MDPI

Review

Blockchain for Securing AI Applications and Open Innovations

Rucha Shinde [1], Shruti Patil [2,*], Ketan Kotecha [2] and Kirti Ruikar [3]

[1] Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India; rucha.shinde.phd2020@sitpune.edu.in
[2] Symbiosis Centre for Applied Artificial Intelligence (SCAAI), Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India; director@sitpune.edu.in
[3] School of Architecture, Building and Civil Engineering, Loughborough University, Loughborough LE11 3TU, UK; k.d.ruikar@lboro.ac.uk
* Correspondence: shruti.patil@sitpune.edu.in

Abstract: Nowadays, open innovations such as intelligent automation and digitalization are being adopted by every industry with the help of powerful technology such as Artificial Intelligence (AI). This evolution drives systematic running processes, involves less overhead of managerial activities and increased production rate. However, it also gave birth to different kinds of attacks and security issues at the data storage level and process level. The real-life implementation of such AI-enabled intelligent systems is currently plagued by the lack of security and trust levels in system predictions. Blockchain is a prevailing technology that can help to alleviate the security risks of AI applications. These two technologies are complementing each other as Blockchain can mitigate vulnerabilities in AI, and AI can improve the performance of Blockchain. Many studies are currently being conducted on the applicability of Blockchains for securing intelligent applications in various crucial domains such as healthcare, finance, energy, government, and defense. However, this domain lacks a systematic study that can offer an overarching view of research activities currently going on in applying Blockchains for securing AI-based systems and improving their robustness. This paper presents a bibliometric and literature analysis of how Blockchain provides a security blanket to AI-based systems. Two well-known research databases (Scopus and Web of Science) have been examined for this analytical study and review. The research uncovered that idea proposals in conferences and some articles published in journals make a major contribution. However, there is still a lot of research work to be done to implement real and stable Blockchain-based AI systems.

Keywords: blockchain; artificial intelligence; federated learning; consensus algorithm; smart contract; open innovation

Citation: Shinde, R.; Patil, S.; Kotecha, K.; Ruikar, K. Blockchain for Securing AI Applications and Open Innovations. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 189. https://doi.org/10.3390/joitmc7030189

Received: 13 July 2021
Accepted: 12 August 2021
Published: 14 August 2021

1. Introduction

In the present era, the vast use of electronic gadgets, social media, and automation causes a voluminous amount of data to be produced per second. At the same time, there is a rise in cyber-attacks such as identity thefts, data breaches, etc. There are various cybersecurity measures that deal with such kinds of attacks. Blockchain technology is an emerging trend in the world of the internet and digitalization, providing high level security. The available security measures are based on centralized servers/systems. Here, ingle points of failure, susceptibility to security breaches, and the need for trusted third parties are all disadvantages. Instead, Blockchain technology is a decentralized system wherein the trusted third parties are absent, and trust is established within the nodes available in the network. Initially, Blockchain came into the picture in the form of cryptocurrencies such as Bitcoin, Ether, and Ripple. After understanding the potential features of Blockchain, many researchers came with the idea of applying Blockchain technology to various industrial applications such as voting, healthcare, banking, and supply chain management, to meet integrity, availability and confidentiality requirements, without any involvement of a central authority [1–3].

The fourth industrial revolution is characterized as a technical revolution that combines digital technology developed during the third industrial Revolution with physical and biological domains. The fourth industrial revolution's sophisticated technologies, such as autonomous cars, 3-D printing, the Internet of Things (IOT), and genetic engineering, drive disruptive innovation by combining individual information and communications technology (ICT) with scientific procedures. To deal with the quickly changing environment, since using internal corporate information alone has limitations, external knowledge may be leveraged to boost a company's innovation activity performance [4]. Open innovation is a comprehensive approach to innovation management that involves "systematically promoting and discovering a diverse range of internal and external sources for innovation opportunities, actively incorporating that investigation with firm resources and capabilities, and extensively leveraging those opportunities via different channels [5]". Artificial intelligence has a great impact on managing innovation in the industry [6,7]. Open innovation's distributed nature collides with blockchain technology's distributed nature. With improved IP management, more transparency, additional knowledge and collaborative empowerment with smart contracts and open data, and latest liquidity for funding innovation, Blockchain technology will serve with ad-equate technological skills to make open innovation a viable platform and attain widespread acceptance [8–10].

Artificial intelligence has completely changed the way we live. Automation is happening at every level and sector at an increasingly faster pace. AI is advancing dramatically, and it has transformed everything socially, economically, and politically. AI has dramatically advanced the application areas such as healthcare, business, education, autonomous vehicles, the travel industry, social media, and agriculture. Increased adoption of AI for critical tasks makes it more vulnerable to attacks, as certain application areas such as in healthcare, military and civil society are becoming attractive target areas for the attack.

Figure 1 depicts the different categories of attacks on AI systems [11]. Input attacks are those in which input to the AI System is manipulated to alter the output, as in the case of a perturbed image. It does not need to have a corrupted AI system. Input attacks fall under four categories: perceivable, imperceivable, digital and physical attacks. Perceivable attacks are those on physical entities and are visible to the human eye. Attacks on physical or digital entities that are invisible to human senses are known as imperceptible attacks. Digital attacks are conducted on digital data such as images, videos, documents, and files and are mostly imperceivable. In the case of physical attacks, the target is physical objects. In most of the scenarios, physical attacks are easy and perceivable. In a poisoning attack, the attacker aims to harm the AI model so that when it is used, it has natural weaknesses that enable them to manipulate it easily. The learning algorithms in dataset poisoning learn a model by identifying patterns in the poisoned data, resulting in a disrupted learning process. Manipulating the algorithm by identifying the weakness in it is known as algorithm poisoning. Federated learning has the threat of such attacks as the user controls data and algorithms [12–14]. In this case, even though a model has been thoroughly trained with a completely qualified database and has been determined to be non-toxic, it can still be updated with a toxic model at different points along the development process. Figure 2 represents the target locations for the attack in the AI implementation process. Due to these vulnerabilities, certain critical applications are not being applied in real life. For this to happen measures would need to be in place that reduce an organization's susceptibility to an attack and protect it with multi-tiered levels of protection. These measures would be those that detect and rectify potential sources of data, algorithm, model, and input poisoning that result in 'corrupt' outputs.

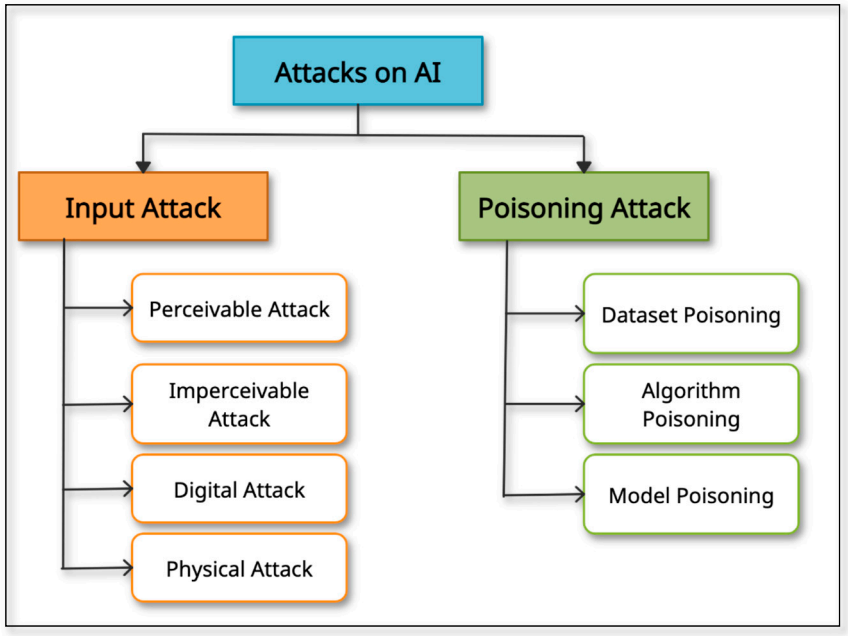

Figure 1. Categories of Attacks on AI.

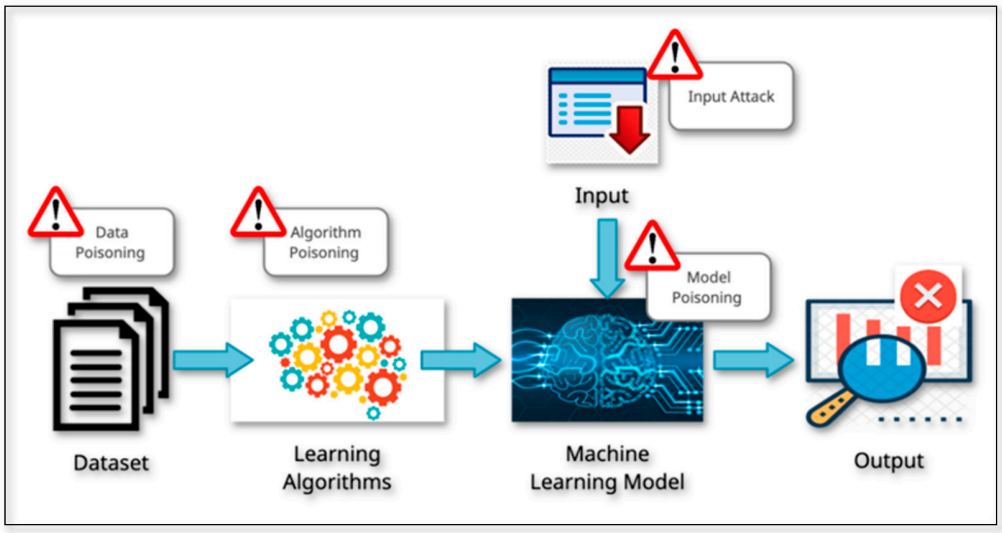

Figure 2. Target areas for attack in AI implementation.

Present Study

Considering the increase in popularity and need for artificial intelligence applications, it is being interrogated by critical applications wherein blind trust in an intelligent application can put human lives at risk. This study focuses on the AI application areas such as the recommender system, IoV based smart city deployment, energy market, AI-based healthcare applications and mobile edge network, in which Blockchain technology is adding trust and transparency. Since 2015, the research in combining Blockchain with AI has begun. Concerning growth pattern, competitiveness, and the social, intellectual, and theoretical context of the field, this study aimed to provide insights into the advancement and emerging trends in integrating two influential technologies, Blockchain and AI. First, the analysis examines trends in publications and citation data from 2015 to April 2021 to outline the progress in the listed sector (i.e., research trends). The study then identifies the key journals and areas of research that are most relevant to the field's growth and the leading authors and regions that contribute to research on integrating Blockchain and AI (i.e., research virtu). At last, the study comments on the potential research relationship and

scholarly and scientific literature for the research of Blockchain and AI integration since 2015. The insights of this study are as follows:

1. To conduct a Bibliometric study for the integration of Blockchain and artificial intelligence considering various application areas.
2. To identify various key features of Blockchain that will secure artificial intelligence models.
3. To survey various applications of Blockchain for artificial intelligence.
4. To understand how Blockchain will provide reliable and private decentralized data storage for training datasets and integrity of AI models and their predictions/results.

The remaining part of the paper is mapped as follows: the study techniques for data collection and extraction and the specifics of data analysis are covered in the second section; the third section provides a discussion on the results of bibliometric analysis with graphical visualization; the fourth section of qualitative analysis outlines the research trends; the article concludes with significant observations, challenges, and future work approaches.

2. Research Strategy-Sources and Methods

To map the literature on Blockchain and artificial intelligence, a bibliometric approach is used for this study since bibliometric analysis is a research technique for evaluating existing research patterns in every new field and determining possible directions for future research [15]. Bibliometric analysis is a process wherein reviewing of published research is assessed using basic metrics. It aids in the identification of the most prominent and cited researchers and organizations, the most significant articles, and the most frequently used keywords within a given research area. The required metadata for analysis is extracted from both "Scopus" and he "Web of Science core collection." Scopus is a renowned abstract and citation database of Elsevier, launched in 2004. Scopus covers the most important abstract and citation information of peer-reviewed literature. Web of Science is delineated as a unifying analysis tool that promptly permits the user to amass, analyze, and distribute information. Web of Science provides varied search and analysis capabilities. Figure 3 depicts the methodological framework used in this study.

2.1. Search Strategy

Table 1 represents the primary and secondary keywords used for search on Scopus and the Web of Science core collection database. Keywords are critical for finding relevant literature for the study. Based on the study's goal, few precise phrases were selected to get a clear picture for the implementation of blockchain in AI domain. We have used "Blockchain" as a fundamental keyword ANDing with "Artificial Intelligence" as a primary keyword. Retrieved results are all from 2015 to 2021. It shows that there was not any research conducted in the mentioned domain before 2015. No filter is applied for country and language. Further Scopus databases were filtered based on the subject area and restricted to computer science, engineering, business, energy, medical, environment, economics, agriculture, and biochemical to retrieve precise literature. Results from Scopus and Web of Science are refined based on the document type. The detailed query for both Scopus and WoS is mentioned below. Only conference papers, articles and review papers are considered for this bibliometric analysis. From the Scopus database 957 documents were chosen, and from the Web of Science database 442 documents resulted from the same query. After removing three duplicate documents, 1396 documents were retained in the rich collection of documents on Blockchain and AI. This analysis is conducted for results retrieved on 12 April 2021. For each of the retrieved documents, metadata such as paper title, publication year, the source, the count of citations, and the author's name, the author's keywords, cited references, organization, and country are extracted.

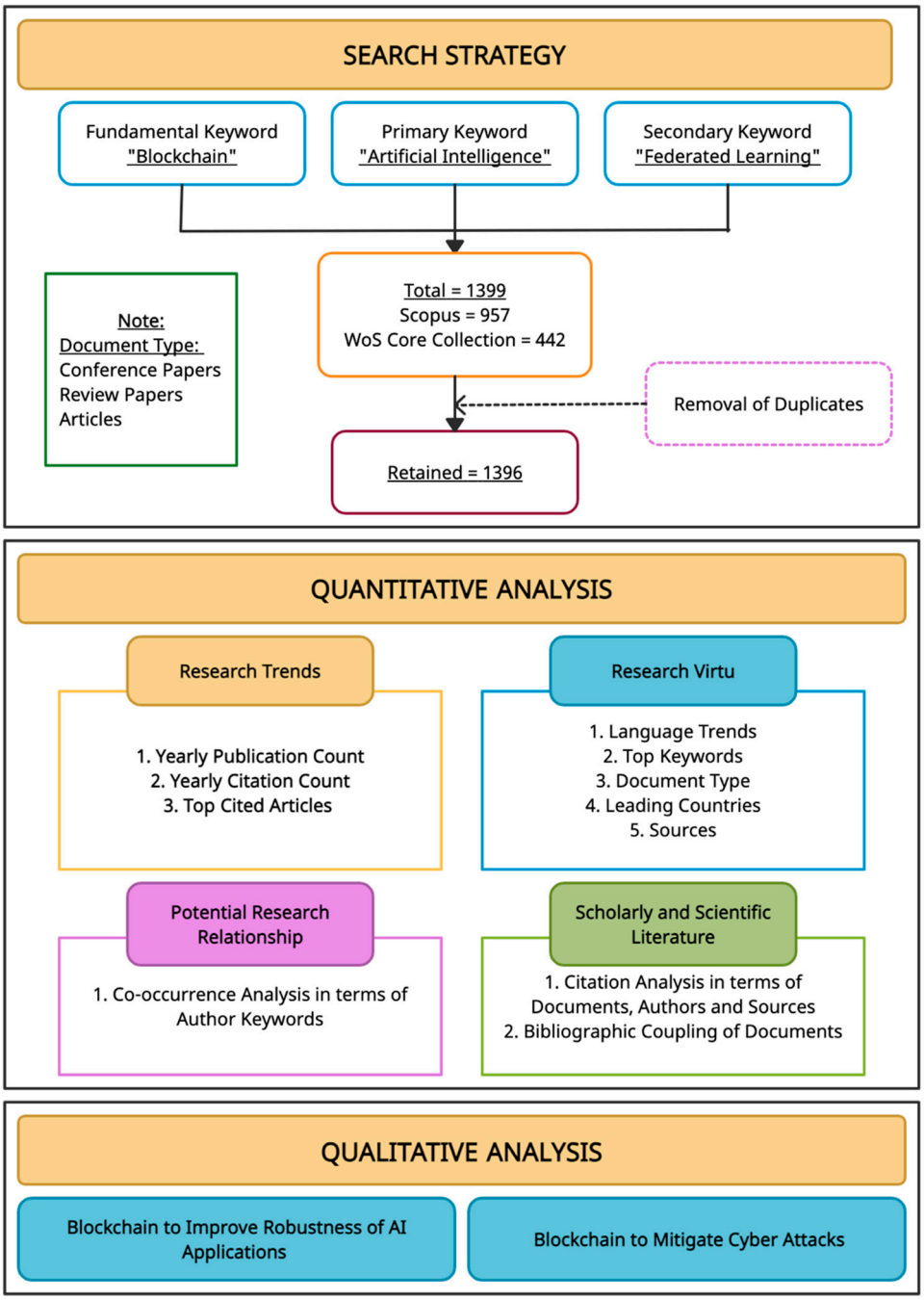

Figure 3. Methodological Framework.

Table 1. List of Primary and Secondary Keywords for Search Query.

Fundamental Keyword	**"Blockchain"**
Primary Keyword Using (AND)	"Artificial Intelligence"
Secondary Keywords Using (OR)	"Federated Learning," "Deep Learning," "Machine Learning," "Privacy," "Secure Sharing," "Authentication," "Cryptography," "Privacy-Preserving," "Access Control," "Adversarial Attack," "Adversarial Machine Learning"

- Query in Scopus is:

(TITLE-ABS-KEY (Blockchain) AND TITLE-ABS-KEY (Artificial AND Intelligence) OR TITLE-ABS-KEY (Federated AND Learning, AND Deep AND Learning, AND Machine AND Learning, AND Privacy, AND Secure AND Sharing, AND Authentication, AND Cryptography, AND Privacy AND Preserving, AND Access AND Control, AND Adversarial AND Attack, AND Adversarial AND Machine AND Learning)) AND (LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "re") OR LIMIT-TO (DOCTYPE, "cr")) AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI") OR LIMIT-TO (SUBJAREA, "BUSI") OR LIMIT-TO (SUBJAREA, "ENER") OR LIMIT-TO (SUBJAREA, "MEDI") OR LIMIT-TO (SUBJAREA, "ENVI") OR LIMIT-TO (SUBJAREA, "ECON") OR LIMIT-TO (SUBJAREA, "CENG") OR LIMIT-TO (SUBJAREA, "AGRI") OR LIMIT-TO (SUBJAREA, "BIOC")).

- Query in Web of Science is:

(Blockchain) AND TOPIC: (Artificial Intelligence*) OR TOPIC: (Federated Learning*, Deep Learning*, Machine Learning*, Privacy, Secure Sharing*, Authentication, Cryptography, Privacy-Preserving*, Access Control*, Adversarial Attack*, Adversarial Machine Learning*).

Refined by: Databases: (WOS) AND DOCUMENT TYPES: (ARTICLE OR REVIEW).

2.2. Data Analysis Procedures

The Bibliometric analysis in combining Blockchain and Artificial Intelligence is conducted by using software tools such as "VoSViewer" and "Gephi". VOSviewer is a popular visualization application for bibliometric network data [16]. The manual states that objects on a map are labeled and can be researched, listed, or published and are represented by circles that are mapped depending on the distance in the network view section. The distance between objects shows their connection, with the most closely associated objects being placed next to each other and being bound by lines. On the other hand, the things associated with weakness are far removed from each other. Gephi is a cross-platform framework since it is written in Java. It makes use of the OpenGL 3D engine. A compatible graphics card is needed for this OpenGL 3D engine. Gephi is kind of Photoshop graph. It allows us to display data collaboratively and productively while also allowing us to configure it according to our needs using properties, scale, consistency, classification, and other graphical management tools [17].

Publication counts and citations were obtained annually to outline the growth pattern of the research. Annual details of publications in the selected filed shed light on quantitative impact on literature by reflecting the growth of popularity and importance of the field in the research domain. Rank ordered tables are generated to represent the productivity considering language trends in the publication, top 10 keywords, type of documents, geographical area wise contribution, and sources preferred for the publication in this study. Co-occurrence analysis of keywords was used to discover the conceptual structure of the field. The units of analysis selected are the author keywords. The co-occurrence analysis mentions the relatedness of items based on the number of documents in which the keywords occur together. Finally, other network analysis performed as citation analysis in terms of documents, sources and authors, bibliographic coupling of documents, and network map of publication title and citation.

3. Quantitative Survey

3.1. Research Trends

3.1.1. Analysis of Documents by Year

Figure 4 represents the yearly analysis of the documents. It was found that research in the field of Blockchain and Artificial Intelligence majorly started in 2019. In 2020, the highest number of publications were recorded for both databases since the advent of a gadget ecosystem that includes Alexa, Siri, and Google Assistant has made AI a part of

everyday life. By 2020, emotion recognition and computer vision are also growing, and the adoption of AI in manufacturing bringing automation became a tradition. Along with this, Blockchain has expanded its applicability in every other filed except cryptocurrencies and finance due to its outstanding features of providing security.

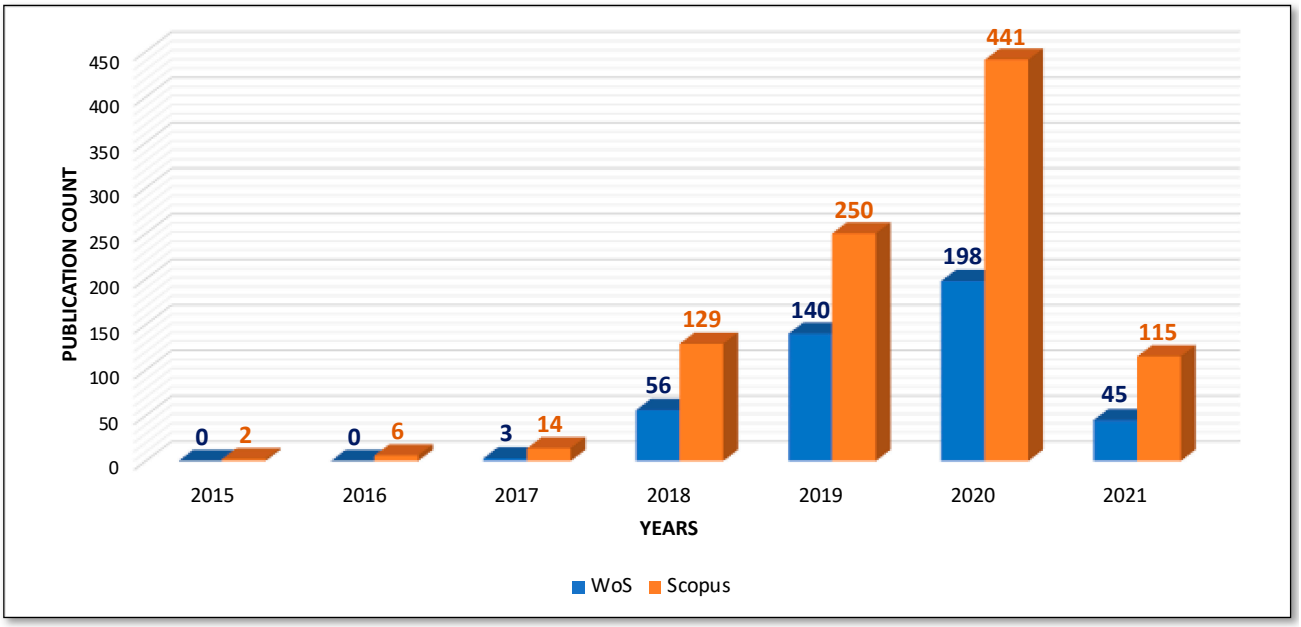

Figure 4. Comparative analysis of documents by years.

3.1.2. Citation Based Analysis

The yearly analysis of the total number of citations for publications from both the databases (Scopus and WoS) is stated in Table 2. It determines an article's relative significance and influence by counting the number of times that article has been referenced by other works. It estimates the significance of research done in the field of Blockchain and artificial intelligence together. The documents published in 2019 gained the most attention from the researchers. Most of the citations are for the documents published in 2020 and 2021.

Table 2. Comparative yearly citation analysis.

Year	<2017	2017	2018	2019	2020	2021	Total
SCOPUS Citations	4	23	179	848	2613	1248	4915
Web of Science Citations	0	1	21	305	1413	593	2333

Here in Table 3 the details of the top 5 documents with the highest number of total citations are given for Scopus and WoS. "Ouroboros: A provably secure proof-of-stake Blockchain protocol" and "Blockchain for AI: Review and Open Research Challenges" had the highest citations from the respective Scopus and Web of Science databases.

The Alluvial diagram was created to collectively perform the analysis of top 20 highly citated documents in the field of study. In Figure 5, the Alluvial diagram depicts the correlation between authors, years, and source titles of highly cited 20 articles. Articles are clustered according to the publication year, and those clusters are sorted in increasing order of total citations received by article. It provides the mapping of contributed authors in respective year to the source of publication. The thickness of waves depends on the citation count. For example, Kiayias A. et al. published an article in 2017 and a highly cited article in the field of Blockchain and artificial intelligence published by the journal *Lecture notes in Computer Science.* Collectively, the highest number of citations were received in

2019. *Lecture notes in Computer Science* and *IEEE Access* were the sources which attracted the most attention from researchers.

Table 3. Details of documents with highest number of citations.

Publication Year	Document Title	Authors	Source	2017	2018	2019	2020	2021	Total
Top 5 Documents from Scopus Database									
2017	Ouroboros: A provably secure proof-of-stake blockchain protocol	Kiayias A., Russell A., David B., Oliynykov R.	Lecture Notes in Computer Science	2	48	130	153	36	369
2019	Blockchain for AI: Review and open research challenges	Salah K., Rehman M.H.U., Nizamuddin N., Al-Fuqaha A.	IEEE Access	0	0	47	89	40	176
2019	6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies	Zhang Z., Xiao Y. et al.	IEEE Vehicular Technology Magazine	0	0	2	122	43	167
2019	Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal	Warner K.S.R., Wäger M.	Long Range Planning	0	0	5	58	48	111
2018	Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare	Mamoshina, P., Ojomoko L. et al.	Oncotarget	0	8	42	49	12	111
Top 5 Documents from Web of Science Database									
2019	Blockchain for AI: Review and Open Research Challenges	Salah K., Rehman M.H.U., Nizamuddin N., Al-Fuqaha A.	IEEE ACCESS	0	0	37	70	24	131
2019	Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal	Warner, Karl S. R., Waeger, Maximilian	LONG RANGE PLANNING	0	0	3	43	31	77
2019	On big data, artificial intelligence, and smart cities	Allam Z., Dhunny Z.	CITIES	0	0	8	48	18	74
2019	State of the Art of Machine Learning Models in Energy Systems, a Systematic Review	Mosavi., Salimi M., et al.	ENERGIES	0	0	14	33	15	62
2020	A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact	Chamola V., Hassija V., Gupta V., et al.	IEEE ACCESS	0	0	0	37	24	61

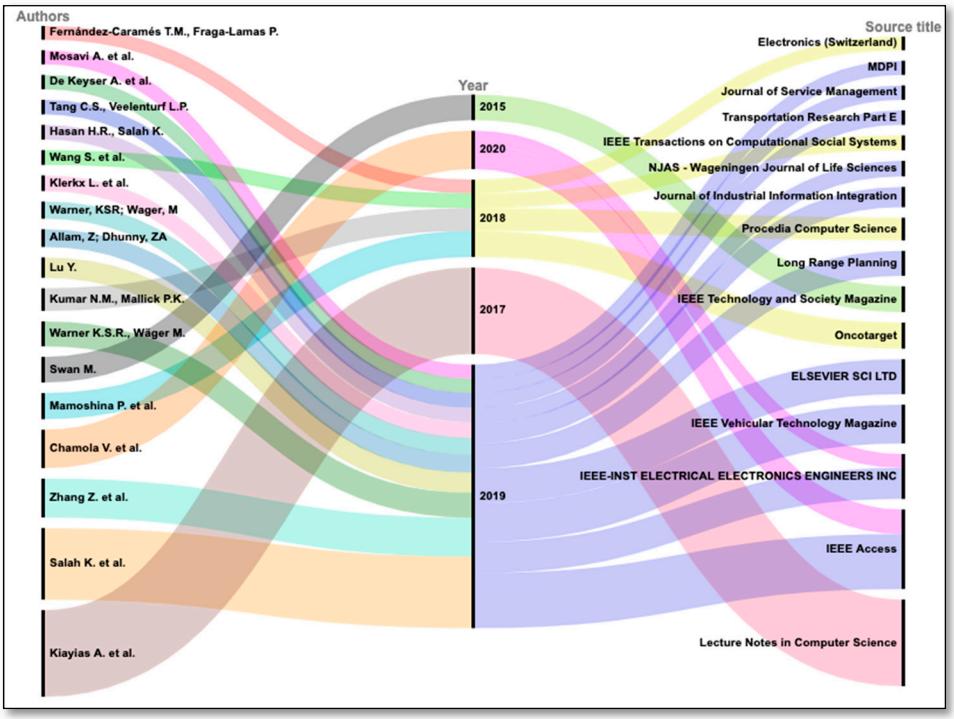

Figure 5. Alluvial diagram showing correlation between authors, years, and source tittles of top 20 highly citated documents.

3.2. Research Virtu

3.2.1. Language Trends of Publication

Table 4 represents the comparative language trends in the publications. It has been identified that, on average, 96% of publications are in the English language for Scopus and Web of Science databases. The countries such as USA, UK, China, and India preferably stick to English language for scientific communication. Since these countries are also leading in research, we observe English the dominant language for publication.

Table 4. Language trends of publication.

Language	Scopus Database	Web of Science Database
English	930	417
Chinese	17	0
French	2	0
German	2	2
Russian	2	10
Turkish	2	1
Korean	1	0
Portuguese	1	2
Spanish	1	7
Ukrainian	0	2
Italian	0	1

3.2.2. Top 10 Keywords from Scopus Database

Following Figure 6 represents the top 10 keywords for the documents retrieved from the Scopus database. Blockchain and artificial intelligence are the two keywords appear most frequently. Keywords mentioned by authors represent the gist of research. The keyword map gives the overview of popular research trends by topic at a glance. The selected documents in this study also expanded to research topics such as IoT, big data, machine learning, digital storage, network security, smart contract and deep learning, except for Blockchain and artificial intelligence.

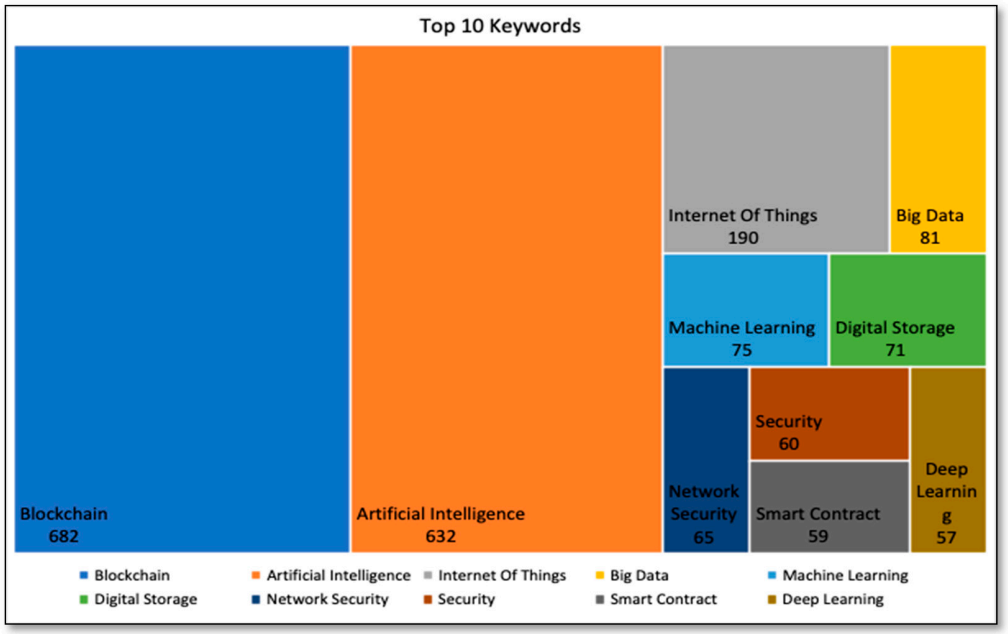

Figure 6. Top 10 keywords from Scopus database.

3.2.3. Analysis by Document Type

Each output of the study has inherent worth and can provide light on the research direction. However, proceeding papers and articles are the most used document type for publishing research work. Hence, documents are refined based on their type. Figures 7 and 8 depict the analysis of publications based on the document type and Tables 5 and 6 represent the respective count. From the Scopus database, more than 50% of the documents are Conference papers. There are moderate numbers of articles available in the Scopus Database, but very few review papers are available. From the Web of Science core collection, more than 60% of the documents are articles, and the moderate number of review papers and conference papers are available.

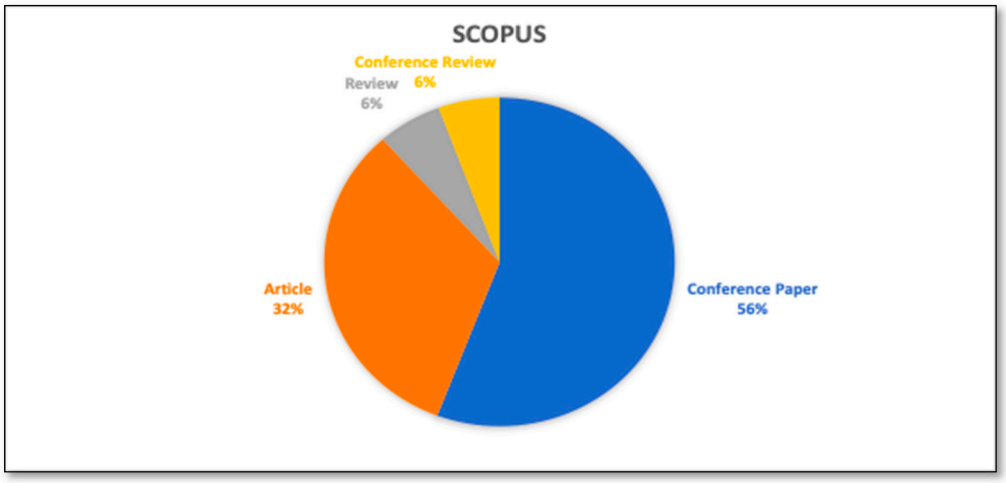

Figure 7. Analysis of documents by type. (Scopus database).

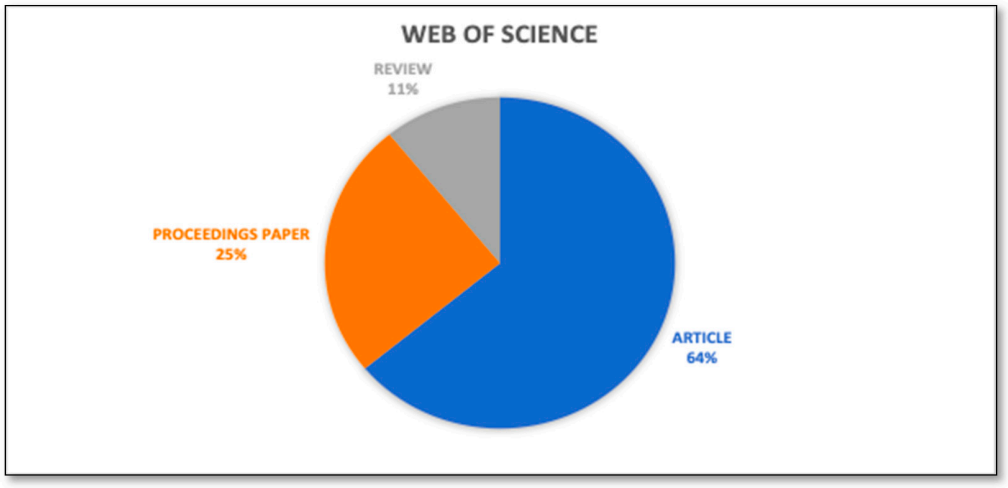

Figure 8. Analysis of documents by type. (WoS core collection).

Table 5. Publication count by document type (Scopus database).

Scopus (Document Type)	Publication Count
Conference Paper	534
Article	312
Review	57
Conference Review	54

Table 6. Publication count by type (WoS core collection).

Web of Science (Document Type)	Publication Count
Article	283
Proceedings Paper	111
Review	48

3.2.4. Analysis by Geographical Area

Figure 9 and Table 7 represent the publication count by geographical area for the Scopus databases. Figure 10 and Table 8 represent the publication count by geographical area for the WoS databases. Through geographical analysis, we can develop our understanding of utilizing and managing resources and opportunities available world-wide in the field of our study. The USA and China are identified as the countries contributing the most to Blockchain and artificial intelligence. From Scopus Database, 207 documents are from China, and 147 documents are from the United States. In the Web of Science core collection, the USA is leading with 96 documents and then China with 69 documents. As most of the world's largest and best-funded AI and Blockchain businesses are based in the United States and China, the rate of investment, business development, and adoption does not appear to be dropping anytime soon. With academic giants and research institutes that proceed to push the frontiers of what is possible with AI, the United States has a highly developed and fully skilled labor population. China provides the resources, including the incubator, to stimulate innovative ideas and is an extremely tech-friendly country. More than 500 Blockchain projects have been registered with China's government.

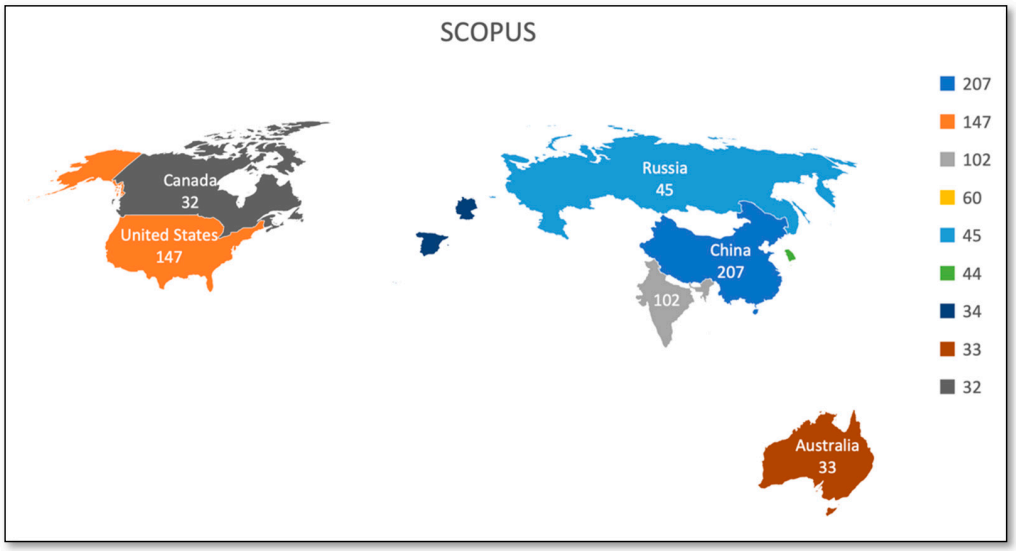

Figure 9. Publications by geographical area (Scopus).

Table 7. Publication count by geographical area (Scopus Database).

Country	Publication Count
China	207
United States	147
India	102
United Kingdom	60
Russian Federation	45
South Korea	44
Spain	34
Germany	34
Australia	33
Canada	32

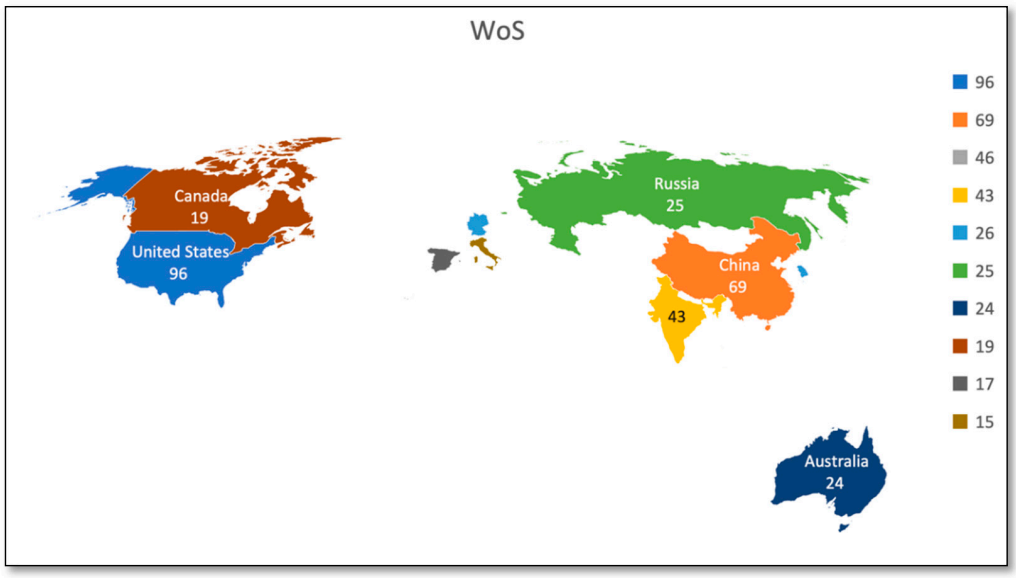

Figure 10. Publications by geographical area (WoS core collection).

Table 8. Publication count by geographical area (WoS core collection).

Country	Publication Count
USA	96
China	69
England	46
India	43
Germany	26
South Korea	26
Russia	25
Australia	24
Canada	19
Spain	17

3.2.5. Analysis of Publications Based on the Source

Figures 11 and 12 represent the top five sources for Blockchain and AI, considering the number of Scopus and Web of Science publications, respectively. The "Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics" is the most preferred source for the publication considering the Scopus database. In the case of the Web of Science core collection, the "IEEE ACCESS" is the most active source, as it yields the most publications.

3.3. Potential Research Relationship

Co-Occurrence Analysis (Author Keywords)

The minimum number of occurrences of a keyword is set to give. Out of 2723 keywords, 163 keywords have met the threshold. Table 9 highlights the top 20 author keywords and their total link strength. As shown in Figure 13, clusters of keywords (Blockchain and Artificial Intelligence) have the highest link strength with 643 and 335, respectively.

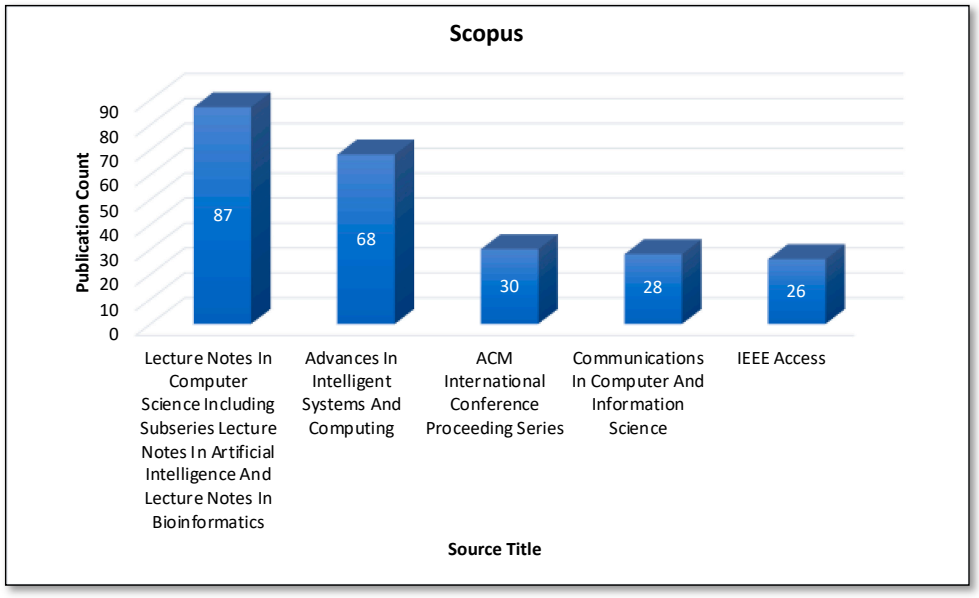

Figure 11. Analysis of publications by source (Scopus database).

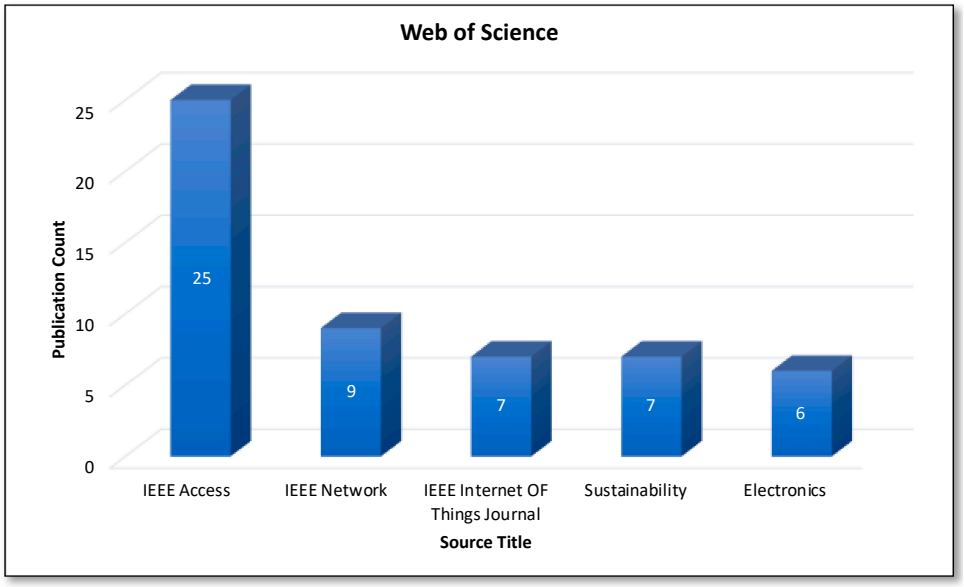

Figure 12. Analysis of publications by source (WoS core collection).

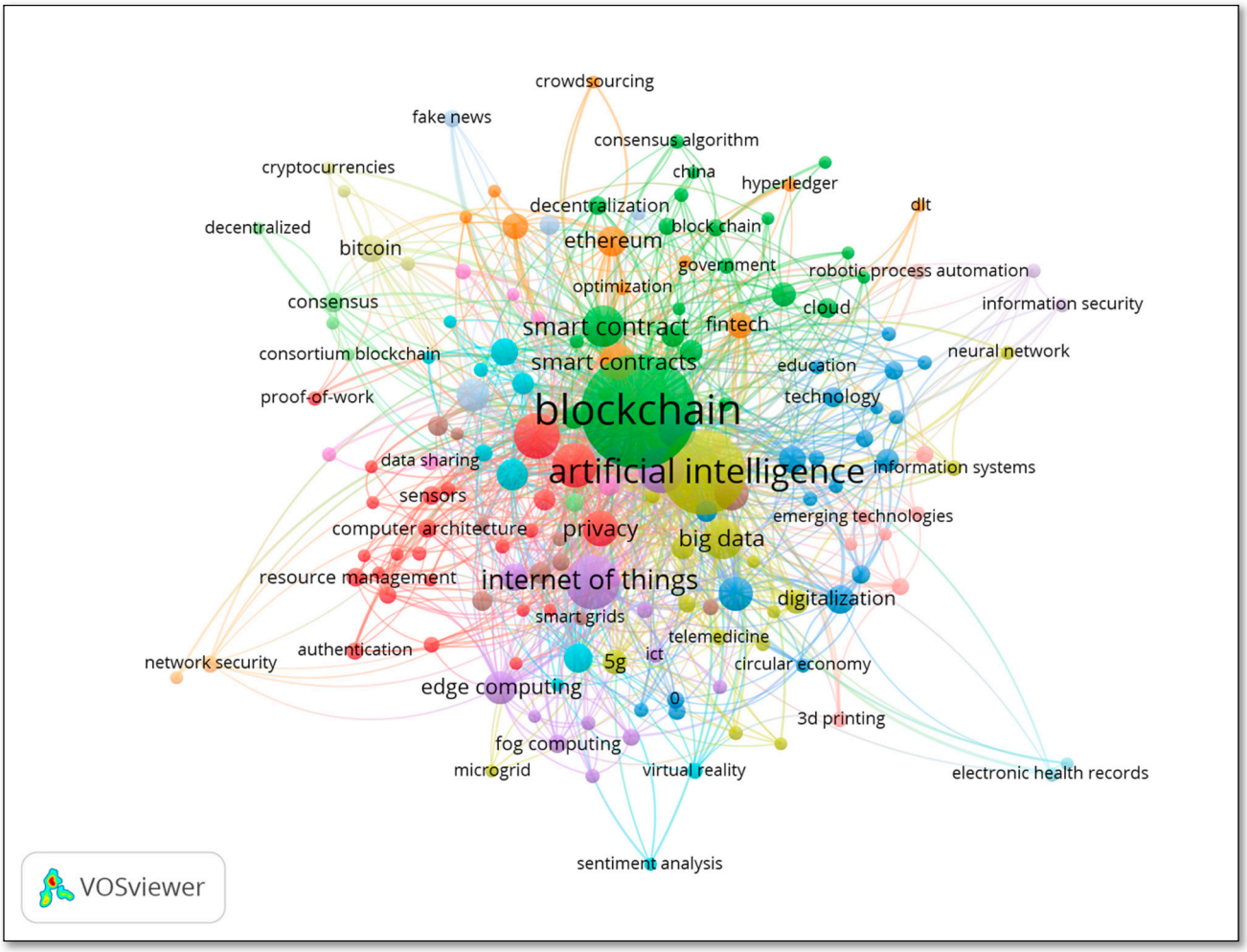

Figure 13. Co-occurrence Analysis (Author Keywords).

Table 9. Links and TLS for co-occurrence analysis (Top 20 author keywords).

	Links	TLS		Links	TLS
Blockchain	159	643	AI	41	46
Artificial Intelligence	133	335	Blockchain Technology	42	45
Internet of Things	101	129	Deep Learning	46	43
Machine Learning	79	86	Edge Computing	47	41
IoT	80	85	Industry 4.0	50	40
Security	69	85	Internet of Things (Iot)	57	38
Big Data	65	66	Ethereum	34	33
Smart Contract	49	66	Cloud Computing	54	31
Smart Contracts	48	50	Digitalization	18	29
Privacy	52	49	Cybersecurity	40	28

3.4. Scholarly and Scientific Literature

3.4.1. Citation Analysis of Documents

The minimum number of citations of a document is considered as 10. Out of 1396 documents, 167 met the threshold which is defined as minimum number of citations of a document. This threshold value is selected for limiting the quantity and quality of documents for analysis. Table 10 represents the measures of citation analysis of documents. The largest set of the connected items consist of 11 items and only those shown in Figure 14. Salah K. (2019) has the highest number of citations (i.e., 172) with the highest six links.

Table 10. Links, citations, and pub. year for citation analysis (documents).

	Links	Citations	Pub. Year		Links	Citations	Pub. Year
Salah K. (2019)	6	172	2019	Zheng X. (2018)	1	34	2018
Zhang Z. (2019)	1	165	2019	Dimitrov D.V. (2019)	1	30	2019
Mamoshina P. (2018)	3	111	2018	Kumari A. (2020)	1	24	2020
Dinh T.N. (2018)	4	53	2018	Khan L.U. (2020)	2	19	2020
Singh S.K. (2020)	1	42	2020	Gammon K. (2018)	1	13	2018
Gupta R. (2020)	3	40	2020				

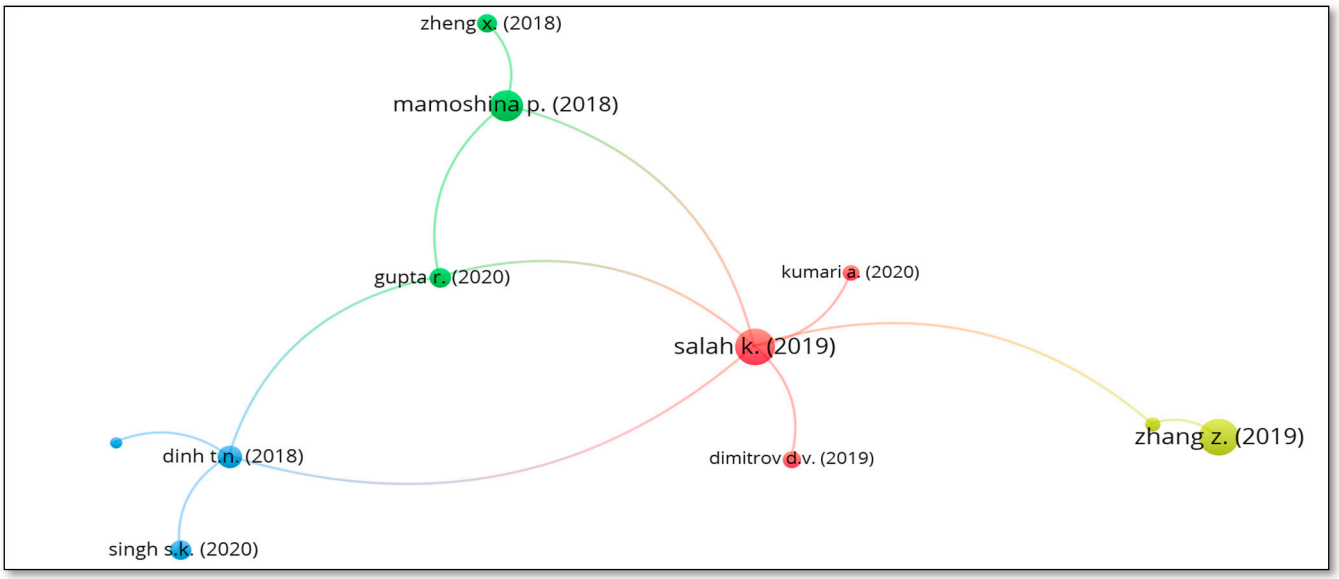

Figure 14. Citation analysis of documents.

3.4.2. Citation Analysis of Sources

Citation analysis of sources is obtained by considering the threshold of three documents per source. Out of the 592 sources, only 92 met the threshold. The largest set of connected items consists of 17 items. Only those are shown here in Figure 15. Table 11 shows that IEEE Access has highest total link strength of 16. The "Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics" has the maximum citations of 580.

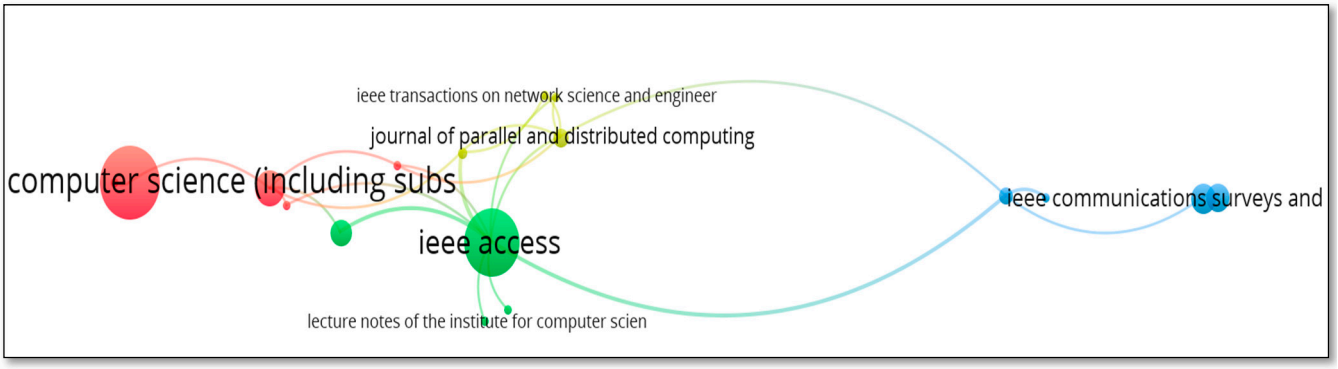

Figure 15. Citation Analysis of Source.

Table 11. Links, TLS, documents and citations for citation analysis (sources).

	Links	TLS	Documents	Citations
IEEE Access	9	16	26	483
Future Internet	4	7	4	19
Transactions on Emerging Telecommunications Technologies	4	7	4	8
Journal of Parallel and Distributed Computing	6	6	4	26
Future Generation Computer Systems	5	5	3	112
ACM International Conference Proceeding Series	2	4	30	57
IEEE Transactions on Network Science and Engineering	3	4	4	1
Peer-To-Peer Networking and Applications	3	4	3	0
IEEE Internet of Things Journal	3	3	6	4
IEEE Communications Surveys and Tutorials	2	2	3	78
IEEE Network	1	2	10	5
Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	2	2	87	580
Proceedings—2020 IEEE International Conference on Blockchain, Blockchain 2020	2	2	5	1
2020 IEEE/ITU International Conference on Artificial Intelligence for Good, Ai4g 2020	1	1	3	0
IEEE Transactions on Industrial Informatics	1	1	4	61
IFIP Advances in Information and Communication Technology	1	1	3	1
Lecture Notes of The Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST	1	1	7	1

3.4.3. Citation Analysis of Authors

The threshold considered here is three documents per author. A total of 110 authors met the threshold amongst the total of 2997 authors. The largest set of connected items consist of 44 items. Table 12 represents measures of Citation analysis of authors. Gupta R. has highest total link strength of 31. Salah K. has the maximum citations of 286 with a total link strength of 24. Figure 16 represents the citation analysis of authors.

Table 12. Links, TLS, Documents and Citations for Citation Analysis (Authors).

	Links	TLS	Documents	Citations		Links	TLS	Documents	Citations
Gupta R.	7	31	6	67	Huang J.	3	3	3	3
Tanwar S.	7	31	6	67	Kumar P.	2	3	4	9
Salah K.	17	24	4	286	Kumar R.	2	3	3	8
Kumar N.	5	17	4	24	Li W.	3	3	7	1
Wang F.-Y.	7	14	6	147	Liu W.	3	3	6	2
Al-Turjman F.	6	11	3	40	Wang X.	3	3	13	84
Yuan Y.	7	11	4	125	Yang C.	3	3	3	5
Wang Z.	9	9	6	4	Guo Y.	2	2	3	88
Park J.H.	7	8	6	62	Wang J.	2	2	7	72
Singh S.K.	7	8	3	50	Wang S.	2	2	7	76
Li J.	7	7	11	71	Yang X.	1	2	4	0
Zhang J.	3	7	8	25	Aloqaily M.	1	1	3	44
Fang J.	6	6	3	1	Kumar S.	1	1	6	25
Kochovski P.	3	6	3	36	Kumar V.	1	1	3	26
Lei K.	6	6	3	1	Qiu C.	1	1	4	5
Stankovski V.	3	6	3	36	Ridhawi I.A.	1	1	3	44
Wu J.	5	5	3	53	Wang W.	1	1	5	11
Yang W.	5	5	3	52	Wang Y.	1	1	14	10
Zhang Z.	5	5	3	173	Yu F.R.	1	1	3	3
Srivastava G.	3	4	3	44	Zhang K.	1	1	5	1
Wang L.	3	4	5	13	Zhang N.	1	1	3	3
Chen H.	3	3	4	0	Zhang X.	1	1	5	6

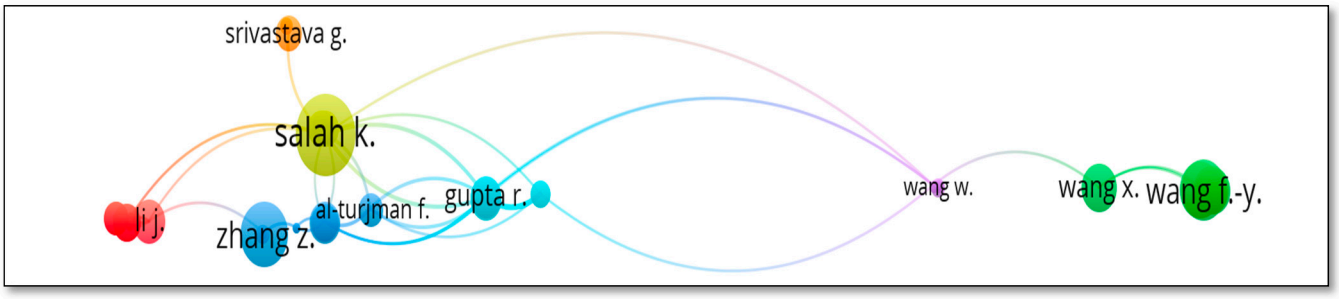

Figure 16. Citation analysis of authors.

3.4.4. Bibliographic Coupling of Documents

Considering five citations of a document as a minimum threshold value. Out of the total 1396 documents, 291 documents met the threshold criteria. Table 13 depicts he top 20 documents considering total link strength along with respective measures for bibliographic coupling of documents. Lu Y. (2019) has the highest link strength of 45.33. Figure 17 represents Bibliographic coupling of the documents.

Table 13. Links, TLS, and citations for bibliographic coupling of documents.

	Links	TLS	Citations		Links	TLS	Citations
Lu Y. (2019a)	48	45.3333	86	De Keyser A. (2019)	13	15	61
Salah K. (2019)	53	40.3333	172	Lu Y. (2019b)	17	15	57
Gupta R. (2020)	17	21	40	Kumar A. (2020)	14	15	8
Singh S. (2020)	20	20.5	24	Wang S. (2018)	19	14	63
Yuan Y. (2017)	12	18	49	Moll J. (2019)	21	14	29
Singh S.K. (2020)	23	18	42	Acharjamayum I. (2019)	48	14	5
Tiberius V. (2019)	19	18	13	Qadri Y.A. (2020)	13	12	49
Ahad M.A. (2020)	16	16	33	Varga P. (2020)	18	12	27
Wang F.-Y. (2018)	8	16	8	Nguyen T. (2020)	43	12	9
Rahouti M. (2018)	23	15.3333	24	Azzaoui A.E. (2020)	17	12	6

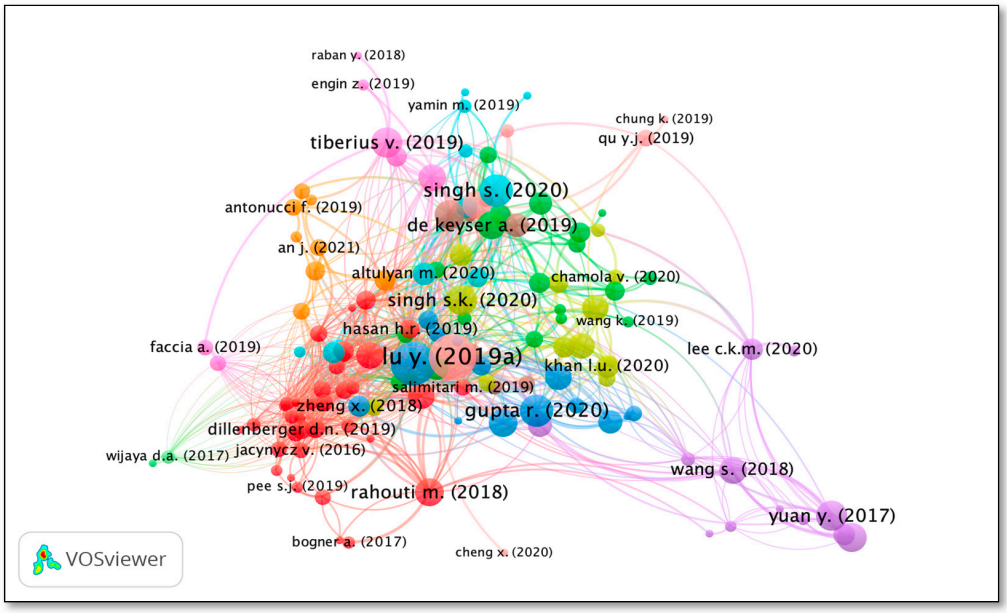

Figure 17. Bibliographic coupling of documents.

3.4.5. Network Map of Publication Title and Citation

The visualization in Figure 18 depicts a network map of publication titles and citations. Different colors represent the different clusters of documents sharing the similarity in citation count. Nodes in same cluster are connected with line of same color. The publication titles are represented by 441 nodes, which is a collective effort by the researchers. It has 482 undirected edges, which means it has 482 links. The shades yellow and red signify the publications that have received the most citations. This illustration was created using Gephi's Fruchterman Reingold layout. Clustered network analysis of authors with their co-authors, source titles, and publication titles is based on the modularity measure from Scopus and Web of Science. The strength of the division of a network is measured by the modularity of a structure of nodes connected in the network.

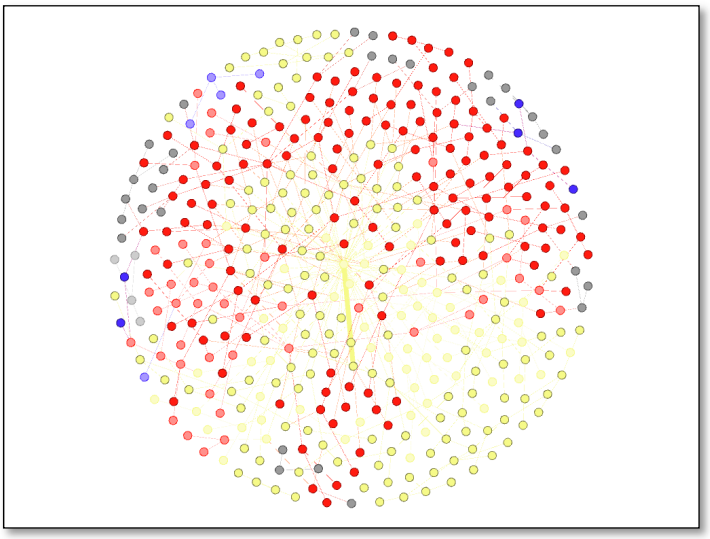

Figure 18. Publication Title and Citations-Network Visualization.

4. Qualitative Survey

For the Qualitative survey, results are further refined based on how Blockchain is used to improve AI/machine learning/deep learning applications. The qualitative research is

conducted on a limited number of articles selected manually and are relevant to Blockchain as a solution for the challenges in artificial intelligence. In the future, a more comprehensive review of articles from well-known scientific databases may be added for study in this area.

4.1. Background

Blockchain maintains a distributed ledger (series of blocks) located at the heart of Blockchain Technology. The distributed ledger can keep all the transactional data verified and immutable due to cryptographic hash and digital signature algorithms [18]. Since many copies of ledger available at every node in the network are computer-generated and an attacker would never attack all the nodes in a Blockchain network, updating and deleting ledger data is not possible on a distributed server. Therefore, providing secure, transparent, and reliable services to Blockchain is a modern need. A secured ledger is maintained by Blockchain, which comprises a series of blocks in a growing list of transaction records. Each block is secretly linked (via hash function, digital signature, Merkle tree, etc.) and other blocks in the chain. This ensures the strict integrity of the transaction details stored in the ledger. To find a new commitment to globalization, the process of consensus needs to be followed. The collaborative process is carried out by the miners on the network and is responsible for: (i) the addition of new blocks to the blockchain; (ii) the legislation ensuring the block chain's security; and (iii) the compatibility of data content records contained in each ledger replica maintained on every node. Once the new block is bound to the chain, no one can change the block or remove the block. Therefore, it has confirmed the integrity of the data. Consistency, integrity, availability, and restriction on double spending are some of the features of Blockchain [18,19]. There are three main types of Blockchain: (1) Public Blockchain, (2) Private Blockchain, and (3) Consortium Blockchain [20]. Bitcoin and Ethereum are social Blockchain platforms where anyone can read, write, and participate in the network. Ripple and Hyperledger support a private Blockchain that prevents performance, documenting tasks as an access control set by the organization. Quorum and Corda are Consortium Blockchain platforms known as the Hybrid Blockchain. It supports the operation of the public and private Blockchains as required by various organizations.

4.2. Taxonomy of Literature Selected for Review

Considering the Blockchain for making AI more robust, the following literature is refined from all the documents retrieved from Scopus and WoS. It has been observed that most papers have discussed the trustworthiness and privacy of data in AI applications [21–24]. Securing the explanations generated by explainable AI with the help of Blockchain also gained more attention [25]. Model poisoning attack in AI can be mitigated by Blockchains [13,26]. Also, Blockchains can provide a solution to data poisoning attacks in AI [27,28]. The following section elaborates the selected application areas wherein Blockchain technology is suggested as a solution for adapting artificial intelligence solutions.

4.2.1. Application Areas—The Amalgamation of Blockchain and AI

- Recommender System

Recommender Systems collect the opinions and preferences related to any item, and then after processing those, it builds personalized information access. The traditional recommender systems have a centralized architecture. Thus, to provide with more transparent and trusted service, a Blockchain platform is used which runs without any centralized authority and supports decentralized rating and ranking. For implementation, Ethereum Blockchain is used, and smart contracts are developed in Solidity. In this application, user, item, and rating are considered the assets, and through the smart contract, these assets are created and processed. The advantages of this Smart Contract-Based Recommender System will be the ratings will be visible to all users, and no centralized authority can manage the rate and score of items. The user-submitted ratings and rating function will be tamper-proof. Customization in rating function is possible through defining meth-

ods through smart contracts [29,30]. Table 14 gives overview of Blockchain for AI based recommender systems.

Table 14. Blockchain for AI based recommender systems.

Ref.	Framework	Integrity	Privacy	Public Availability of Ratings	Auditability	Incentives	Reputation
[31]	Decentralized Rating Framework	✔	×	✔	✔	✔	✔
[32]	Decentralized Recommender System	✔	×	✔	✔	✔	✔
[33]	Decentralized Knowledge Graph	✔	×	×	✔	✔	×
[34]	Decentralized Privacy Preserved Recommender System	✔	✔	×	✔	✔	✔
[35]	Recommendation system based on consortium blockchain	✔	×	×	✔	✔	✔
[36]	Blockchain based privacy protection strategy for Internet Financial product recommendation system.	✔	✔	×	✔	×	✔
[37]	Privacy Preserving Platform for Recommender Framework	✔	✔	×	✔	✔	✔

- IoV Based Smart City Deployment

Vehicles on the Internet of Vehicles (IoV) can collect and distribute data in a smart city network. But there can be insecure communication within various entities in the network. Hence the Blockchain-based batch authentication protocol is designed for IoV-based smart city implementation, which AI envisions. After a proper authentication process, roadside units can gather data from their vehicles. This transaction block is created and mined using a voting-based Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. Hence, data that is real and authentic will be available in Blockchain, which is further utilized by AI algorithms. This scheme proved effective after experimental setups using Hyperledger Sawtooth [21,38]. Table 15 gives overview of Blockchain for AI based IoV applications.

- Energy Market

In energy trading systems (ETS), all of the transactions are recorded digitally, and those constitute a tremendous amount. It won't be easy to manage such a vast amount of data centrally. Certain challenges, such as the variability of prosumer demands, the versatility of usage, and generational instability, create bottlenecks when solving decision, regulation, security, and privacy issues. Hence app lying emerging technologies such as Blockchain and AI can jointly solve data modeling and security issues in ETS. With the help of the Blockchain layer, all of the transactions within the traders can be validated. This will assure the trust and privacy of historical data for AI-based learning and predictions. IOTA and sharding techniques are implemented for the same scenario [22]. Table 16 gives overview of Blockchain for AI based energy market applications.

Table 15. Blockchain for AI based IoV.

Ref.	Framework	Objective	Secure	Fault Tolerant	Scalable	Privacy	Minimized Latency
[39]	blockchain-based federated learning pool (BFLP) framework	To address data silos and poor privacy preservation.	✔	✔	✔	✔	✔
[40]	Blockchain enabled IoV with multi-access edge computing	To enhance the performance of Video applications in IoV.	✔	✔	✔	✔	✔
[41]	Deep Learning and Blockchain scheme, DwaRa	To resolve the dynamic pricing and secure automated funds transfer.	✔	✔	✔	✔	✔
[42]	Blockchain-enabled vehicular crowdsensing system	To protect user privacy and data safety in 5G Internet of Vehicles (IoV).	✔	✔	✔	✔	✔
[43]	blockchain-enabled Internet of Vehicles (IoV) with Cooperative Positioning	To improve vehicular GPS positioning accuracy, system robustness, and security.	✔	✔	✔	✔	×
[44]	a Deep Reinforcement Learning (DRL) and Blockchain empowered Spatial Crowdsourcing System (DB-SCS)	To address privacy of the task providers and receivers during the spatial crowdsourcing process.	✔	✔	✔	✔	✔

Table 16. Blockchain for AI based energy market applications.

Ref.	Framework	Objective	Use Case
[22]	Blockchain-AI integration in Energy Trading System.	To address uncontrolled disclosure of information.	Energy Trading
[45]	Decentralized blockchain-enabled energy trading scheme	To address cross-domain energy trading and location privacy protection in centralized vehicular energy networks.	Energy Trading
[46]	Decentralized blockchain application and adaptive learning.	To address a diverse energy market transaction and a comprehensive energy usage.	Multi-Energy Market

- AI-Based Healthcare Application

Many health care organizations do not want to share their data with third parties considering privacy issues [47]. This makes it difficult to build a robust AI model and apply it for real-time environments if the patient data is fragmented over different users. Then it won't be easy to build a generalized prediction model. Hence, to solve this problem, Blockchain can be integrated with AI to protect data access and secure the implementation of federated learning in healthcare applications. Through smart contracts, access control rules will be imposed on the data access from different data holders for secure data sharing [27,48–55]. Table 17 gives overview of some Blockchain for AI based healthcare applications.

Table 17. Blockchain for AI based healthcare.

Ref.	Framework	Objective	Fault Tolerant	Authenticity	Privacy	Anonymity	Integrity	Availability
[56]	B5G-enabled smart health care framework	To battle pandemics like COVID-19.	✔	×	×	×	✔	✔
[57]	Chained Distributed Machine learning (C-DistriM)	To address paucity of transparency, which makes it difficult to trust the data utilized in the analysis.	✔	✔	×	×	✔	-
[58]	Blockchain and AI-empowered telesurgery system towards 6G (BATS)	To address challenges like security, throughput, reliability, trust, and transparency.	✔	✔	✔	×	✔	✔
[59]	Deep Learning with Blockchain assisted secure image transmission and diagnosis model for the IoMT environment.	To address security, Privacy, and inadequate data.	✔	✔	✔	✔	✔	✔
[60]	deep-learning-based secure blockchain (ODLSB) enabled intelligent IoT and healthcare diagnosis model	To address centralized architecture, security, and privacy, resource constraints, and the lack of adequate training data.	✔	✔	✔	✔	✔	✔

- Mobile Edge Network

Unmanned Aerial Vehicles (UAVs) have been making a huge impact and gaining interest in various military and civil applications such as communications, disaster management, search and rescue, security, control, agriculture, and the Internet of Things (IoT) in the current fifth generation (5G) and Beyond 5G (B5G) era. To tackle a challenging hurdle to compute offloading and resource allocations in a dynamic environment, a deep reinforcement learning approach can be used. Furthermore, blockchain can secure and optimize offloading issues in multi-UAV (unmanned aerial vehicles) aided mobile edge computing architecture [61–64].

4.2.2. Discussion on Amalgamation of Blockchain and AI

Deep learning models can perform exceptionally well and precisely when trained with enormous data. In the case of healthcare applications, having a large amount of data in one location is challenging. Data available with different hospitals, laboratories, and research centers can be collaboratively used to train deep learning models. However, privacy is a major concern, which restricts sharing of medical data within different organizations. The execution of deep learning models over Blockchain is the solution for this kind of issue. As Blockchain itself has storage constraints, all data cannot be mounted on Blockchain. It stores and shares only weights of the locally trained model at individual places using smart contracts, enabling Blockchain decentralized networks to train a global model [65]. In some scenarios, all the transactions to access data for deep learning models can be recorded in the Blockchain. Through smart contracts, it can execute access control rules to avoid data misuse [66].

Researchers [67–69] are extremely interested in blockchain technology for Artificial Intelligence featured 5G networks. As 5G is now a heterogeneous network and supports a wide variety of IoT devices, the amount of data communicated and generated will be massive, putting a strain on AI. The combination of Blockchain and AI would provide a great outcome in terms of 5G network protection and efficiency. Blockchain ledger maintains immutable records of transactions among users and network providers, which

solves automatic billing problems. Learning algorithms and information exploration could be performed automatically based on the network state due to blockchain-featured smart contracts. To estimate and recognize the channel, Blockchain can also store active search traces and traversal paths permanently and stably, which will improve search strategies for different operations.

In case of federated learning, users conduct local training on their own data, which is commonly done using the gradient descent optimization process. Users preserve their data but transfer the parameters to server for consolidation in a federated learning. This creates a parallel system for users to cooperatively learn a global model while maintaining personal data privacy. Thus, federated learning delivers ambient intelligence by learning from distributed data while maintaining privacy, and uses blockchain to create a guaranteed collaborating framework for efficient sharing across untrustworthy participants. Blockchain will improve the privacy level by sharing local gradients through distributed ledger and in further establishes trust in federated learning [14,38,70,71].

With the help of federated learning, the raw training data can be kept on a local machine and can have privacy-preserved distributed AI. There is a need to handle security and trust problems within the network while implementing federated learning on mobile edge networks. Federated learning can use Blockchain to provide protection and productivity and prevent mobile edge computing nodes from failing. Through smart contracts, an incentive mechanism can be implemented to reward the trustful entities. In this case study, the system is built upon the Hyperledger Fabric platform, a private Blockchain [23,72].

In case of any catastrophic failure of AI-based applications, regulators can audit the explanations generated by explainable AI. However, these explanations are stored in centralized servers. They do not provide security and trackability so that owner can tamper with the data. Blockchain can overcome these security limitations. IPFS can store all these explanations, and those can be retrieved from the Ethereum blockchain. Storing and retrieving the explanations can be done through the smart contract. The Hash value can be calculated for each explanation, which can be stored in the Blockchain to impose more security [25]. Figure 19 summarizes how Blockchain can mitigate challenges in AI.

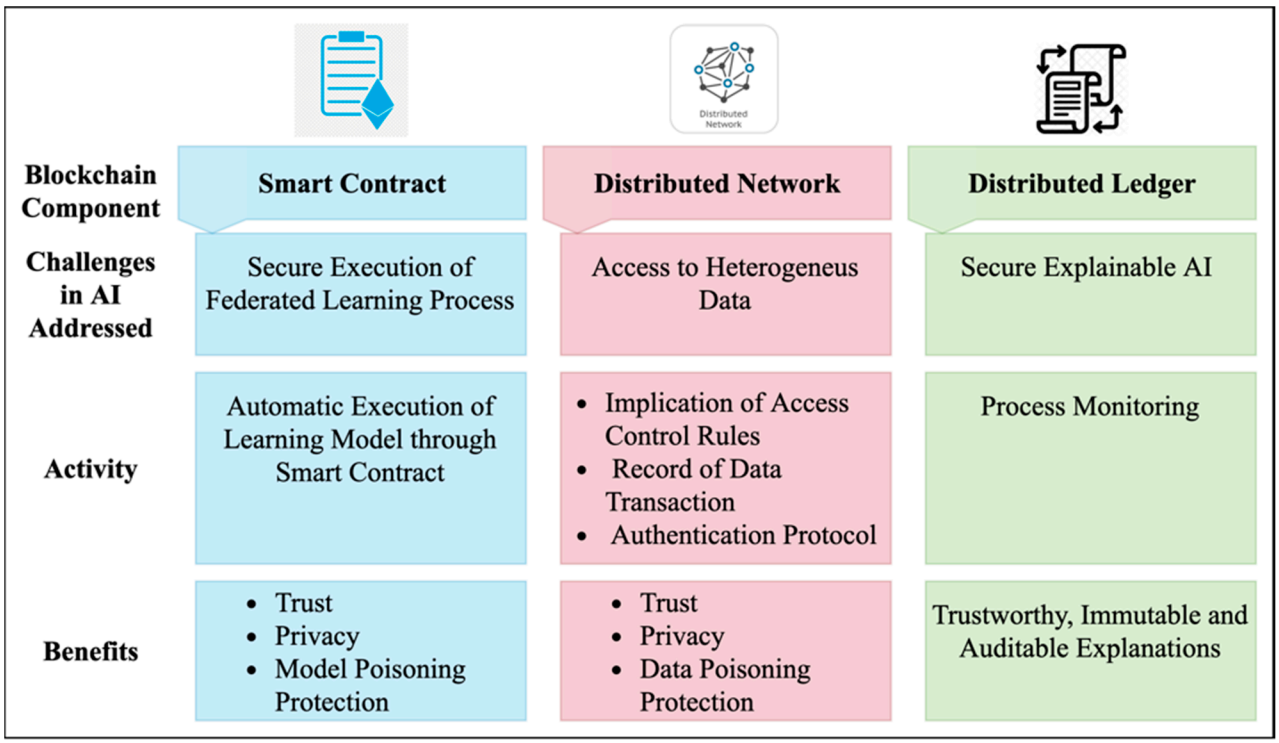

Figure 19. Blockchain solution for challenges in AI.

Table 18 highlights the challenges in AI, Blockchain solution for the same, Blockchain platform used, security analysis, and application in the selected papers. The AI applications can take benefit of Blockchain features such as immutability, transparency, privacy, trust, and security, as illustrated in Figure 20.

Table 18. Blockchain solution for challenges in AI.

Reference	Challenges in AI Addressed	Blockchain Solution	Blockchain Platform	Security Analysis	Application	Limitations
[29]	A centralized architecture provides the service.	Since there is no centralized authority, blockchain technology allows for decentralized ratings and ranking of various products.	Ethereum	Rating technique that is more straightforward and decentralized.	Recommender System	It does not affect collusion between the consumer and the owner of the products. Shilling attacks are a challenge.
[26]	Bias and adversarial attacks on AI implementations can poison the learning and inference processes.	The explanation is audited in a way that is immutable, tamper-proof, and distributed, as well as traceable and trackable with high reliability and resilience.	IPFS	XAI system that is more resilient, trustworthy, and capable of reducing discrimination and adversarial attacks.	Trustworthy AI Applications	Many more infrastructural prerequisites such as Security, Privacy, Dependability, Accessibility, Efficiency, and Governance are essential.
[21]	Lack of confidence among the participants and RSU, TA, and computational vehicle capacity, Data Poisoning Attack.	Blockchain-based batch authentication scheme for IoV.	Hyperledger Sawtooth. Voting-based Practical Byzantine Fault Tolerance (PBFT) consensus algorithm.	Data poisoning attacks are thwarted by preventing malicious transactions from being injected into the blocks and computing time effectiveness.	Blockchain-enabled batch authentication scheme in AI-envisioned IoV-based Smart City deployment	Not Mentioned
[22]	For learning and prediction, historical data should be trusted, explainable, and private.	The BC layer validates and handles the trading entities' transactions.	PoA algorithm IOTA and "sharding."	In a distributed network, it needed a trustworthy system to enable real-time security and transaction management.	Energy Market	Privacy and Data Access in Public Blockchain, Scalability and Accuracy, Security and Suitability, Lack of standards, interoperability, and regulations Cross-domain Research, Lack of Acceptance.
[13]	Model Poisoning Attack	Smart Contract in Blockchain executes Federated Learning process to protect against model poisoning.	Open-source Blockchain Platform	The falsified model updates are identified correctly, and model accuracy can satisfy in the presence of 30% of adversaries.	Federated Learning Application	Never tested for all the different parameters and not implemented in Open Source Blockchain Platform.

Table 18. *Cont.*

Reference	Challenges in AI Addressed	Blockchain Solution	Blockchain Platform	Security Analysis	Application	Limitations
[23]	When using FL over mobile edge networks, there are security and trust problems to consider.	A two-layered architecture of blockchains: Local Model Update Chain (LMUC) assisted by Device-to-Device (D2D) communication and Global Model Update Chain (GMUC) supporting task sharding.	Hyper-ledger Fabric	It has been proven to effectively lower the time delay while maintaining a stable efficiency as the number of FL participants grows.	Mobile Edge Network	Local system mobility in the LMUC and complex network attack scenarios.
[25]	Since centralized systems lack security and traceability, the respective owner can temper the Explainable Artificial Intelligence (XAI) created explanations for his convenience to avoid any penalties.	Inter Planetary File System (IPFS) stores the explanations, and Smart Contract is designed for supervising the Ethereum Blockchain for storing and retrieving explanations. The Hash of explanations stored over Blockchain.	IPFS and Ethereum Blockchain	Integrity, authorization, transparency, availability, and non-repudiation are all primary security features of the proposed Blockchain-based solution.	XAI decisions Storage	Smart contract-based storage and retrieval functions take time and money to execute.
[27]	Privacy concerns in sharing healthcare records with third parties to make the AI model more Robust. Difficulty in building generalized prediction model for fragmented data.	Establishing access control rules through the smart contract for transacting personal healthcare records.	Blockchain—Smart contract	Helps in building robust AI models and sharing personal healthcare records without being compromised.	AI-Based Healthcare Application	The application is not yet developed and tested.
[73]	Distributed AI on IoT devices that are low-power and low-cost.	A Blockchain-based architecture supports DAI on low-power and low-cost IoT devices that are distributed, decentralized, and stable.	Public Blockchain platform, Honesty-based Distributed Proof of Authority via Scalable Work (HDPoA)	The implemented DAI has an accuracy of 92%-98%, with an energy cost of 0.12 joules (J) with Raspberry Pi to run one neuron.	Distributed Artificial Intelligence (DAI) using hardware platforms provided by the Internet of Things (IoT)	The effectiveness of using an Off-Chain solution, which could be suitable for applications that involve near-real-time response.

Table 18. *Cont.*

Reference	Challenges in AI Addressed	Blockchain Solution	Blockchain Platform	Security Analysis	Application	Limitations
[28]	To establish a heterogeneous network for collecting a huge amount of data to combat COVID-19.	The encrypted transfer of patient data in the edge using blockchain technology.	Private Blockchain	The highest accuracy obtained by ResNet101was 97.1%	Pandemic (COVID-19) Screening and Diagnosis System.	To reduce the number of weights in the model by using mobile DL models. To use parallel processing in the edge computers.

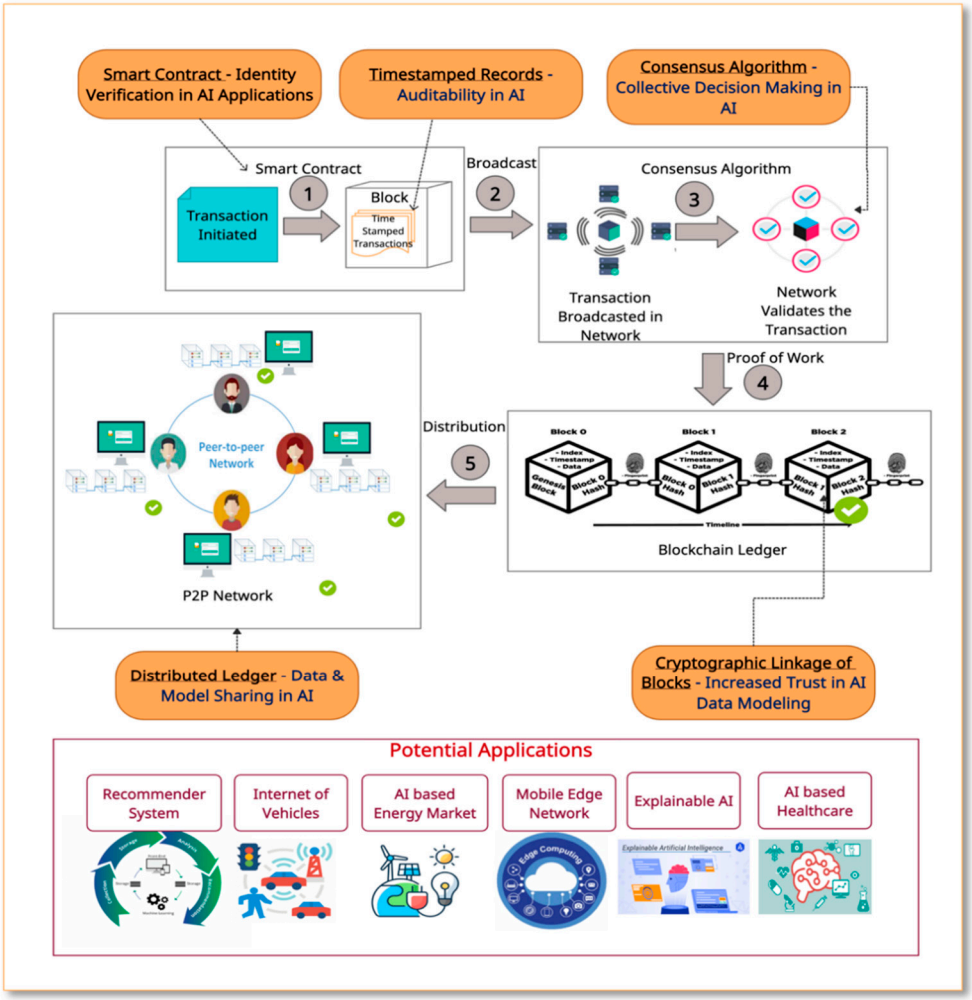

Figure 20. Step by step working of Blockchain reflecting its benefits in AI applications.

4.3. Blockchain as a Solution to Detect and Mitigate Different Attacks

If we consider content filtering application, which is applied to digital assets, has the threat of "imperceivable unput attack." This attack will simply make certain sensitive content get skipped from filtering. These attacks will not get detected such as other cyber-attacks. The military applications of AI are also very sensitive and critical. The attacks on AI can be weaponized for war in the case of the military. Autonomous vehicles are also becoming targeted by such attacks. Computer vision systems will get fooled by attacks, and vehicles will make mistakes in identifying traffic signals, the crowd on a road, or any other such obstacles. The consequence of such attacks on the inputs can affect the outputs and may lead to inadequate or sometimes wrong decisions. Consequently, the decision

could affect patient wellbeing and health. In healthcare applications, such attacks could mislead the detection of disease and treatment. Patients' lives will be at stake if we blindly trust decisions made by AI systems in healthcare [74]. This problem is not simply limited to healthcare, but spread across a whole host of applications, where the consequence of a wrong decision could cost a life and a business's continuity, among other such scenarios.

The attacks in AI applications are not the same as cyberattacks. Rather, these are purposeful manipulation or perturbation either at the data or model level. Ultimately, the goal is to make AI applications malfunction. Attacking such critical application areas may not even require a computer, so existing cybersecurity policies cannot address these attacks [75]. There is a need for new approaches and solutions for input attacks on AI systems and making robust AI. As data are weaponized, we need advanced and secure strategies to collect, store, and use data. Table 19 differentiates the attacks on AI from cyberattacks. Due to its transparency, confidentiality, immutability, protection, and privacy features, Blockchain, as a decentralized framework, provides benefits AI for data management. All the transactions to access AI datasets can be recorded in Blockchain for auditing in immutable form. Through smart contracts, we can also imply access control rules or execute AI models. In the case of distributed machine learning, Blockchain can be used to store local gradients.

Table 19. Cyberattack vs. attacks on AI.

Parameters	Cyber Attacks	Attacks on AI
Goal	Modify, obstruct, erase, handle, or steal data stored in computer systems by disabling, disrupting, destroying, or controlling them.	To make AI application malfunction that is wrong prediction or wrong classification.
Need of Computer	Yes	It may not be required.
Types of Attack	Brute Force Attack, Malware, Phishing, Denial of Service (DoS)	Input Attack, Poisoning Attack (Data/Algorithm/Model), Evasion Attacks
Causes	Bug, Human mistakes in code, Malicious Program	Adversarial Data, Intrinsic Model/Algorithm itself
Vulnerabilities in the system that cause an attack	Hidden Backdoor Programs. Unencrypted Data on the Network. Malware/Virus Checks are not performed on automated scripts. Security flaws that have yet to be discovered.	Machine Learning "learns" fragile patterns that function very well but can be easy to misunderstand. Dependency is mainly on data to corrupt a learning model. Auditing state-of-the-art algorithms are difficult due to their black box existence.
Need of Hacking	Yes	It may not be required.
Countermeasures	Cybersecurity Policies	Require Innovative Approaches and Solutions.

The adversarial attacks on AI models make systems generate malicious results. In the case of AI-enabled critical decision-making systems such as security, finance, and healthcare, blind acceptance of wrong decisions or predictions cannot be tolerated. Hence, there should be some measures to have trusted AI models representing trustworthy explanations regarding the output result. The platform developed using Blockchain smart contracts to record, regulate interactions and provide consensus for AI predictions and outcomes among AI and XAI Oracles to accomplish explainable and trustworthy AI [26].

Blockchain can also be used as a defense mechanism for various kinds of attacks [76]. Table 20 represents what kind of attacks are detected and mitigated with the help of Blockchain technology.

Table 20. Blockchain as a solution to detect and mitigate different attacks.

Author	Attacks	Type of Solution	Blockchain Platform	Application	Limitation
[77]	Sybil attack	Detection	Proof-of-Work Public Blockchain	Energy Trading	The reliability of the Blockchain system would be further assessed by calculating the number of transactions per second to increase the number of validators.
[78]	Sybil attack, Node replication attack, Wormhole attack, Sinkhole attack, Replay attack, Man-in-the-middle attack, Impersonation attack, Privileged-insider attack, Ephemeral Secret Leakage (ESL) attack	Detection & Mitigation	PBFT ECDSA signature verification Algorithm Public Blockchain	Internet of Everything	Not Mentioned
[79]	DDoS attack	Mitigation	Hyperledger Fabric	Multi-domain SDN network	A single client generates all transactions in the Blockchain network.
[80]	DDoS Attacks	Mitigation	Ethereum	IoT	Not Mentioned
[81]	Ransomware Attack	Defense	Hyperledger Fabric	Edge Computing	Determination of the size of the record is critical.
[82]	Byzantine Attacks	Defense	Secure Learning Chain Practical Byzantine Fault Tolerance (IPBFT) Consensus Algorithm	Distributed Machine Learning	Not Mentioned
[83]	Insider attacks (Betrayal attack, PMFA attack)	Intrusion Detection	Proof-of-Concept Blockchain	IoT	Scalability, Not tested for advanced insider attacks.

- When the intruder impersonates many people at once, this is known as Sybil's attack. As a result, when connecting to a P2P network, this becomes a big issue. To participate in the mining process, each node must solve a complex cryptographic puzzle. It is still possible to increase ownership but having the computing resources to solve the puzzle is difficult. With the addition of leading zeros, the Cryptographic problem becomes more complicated. Therefore, PoW is a balanced way to combat Sybil's attacks during mining [77].
- A Blockchained access control framework can significantly reduce the data poisoning attack in the IoE environment. Data can be securely communicated within fog servers and IoT smart devices [78].
- A secure distributed model can be facilitated for Cyber threat intelligence sharing among diverse participants using Blockchain technology. It will ensure tamper-proof electronic records and immutable execution by smart contracts [79].
- Rogue devices can be prevented from gaining access to the server by integrating IoT with Ethereum. Static resource allocation for the devices can address DDoS attacks [80].

- Malware injection attacks (e.g., Ransomware attacks) are network attacks triggered by encrypting sensitive victim files, resulting in abnormal behavior on its system or unexpected program closure. To save files or activate the application, you need a configuration key to be obtained by paying to use it. With a distributed blockchain ledger and its tamper-proof feature, a consortium Blockchain was introduced on the IoT network to address this security issue [81].

Secure Learning Chain (SLC) is a framework designed for securing distributed machine learning by using permissioned Blockchain. To protect against malicious central servers, and the Identifiable Practical Byzantine Fault Tolerance (IPBFT) consensus algorithm has been used. This algorithm can also be used to detect malicious central servers and simplify communication. Malicious personnel may use a Mixed Acc-based multi-Krum Aggregation (MAKA) algorithm to avoid Byzantine attacks [82].

5. Discussion

Blockchain and Artificial Intelligence are the trending technologies that help to solve many complex problems almost in every field. Rather than taking benefits of these individual technologies, combining them brings double advantage, as these two technologies are very complimentary with one another [84–86]. Challenges in both technologies can be mitigated by combining them. This study has focused on researching the applications where Blockchain and artificial intelligence are merged. The analysis is mainly conducted for the attributes such as language, year of publication, type of document, geographical location, sources, and citations. The network analysis was conducted for co-occurrence analysis in terms of author keywords, citation analysis of documents, authors, sources, and Bibliographic coupling of the documents. This study will be helpful to identify and get connected with the potential researchers, find good sources to publish the articles, and explore new ideas using the keywords in the same research field.

The important findings of the Bibliometric analysis for combination of Blockchain and artificial intelligence are as follows:

- Most of the literature is available in the English language from Scopus and the Web of Science core collection.
- The year 2020 acknowledged the progressive rise in the research of Blockchain and AI together.
- Conference papers and articles are in big number as compared to other review articles considering both databases.
- China and the USA are the leading countries in the research contribution. Also, India has a good number of publications.
- The most preferred source for publishing the research work is *Lecture Notes in Computer Science* including subseries *Lecture Notes in Artificial Intelligence* and *Lecture Notes in Bioinformatics*.
- "Ouroboros: A provably secure proof-of-stake blockchain protocol," an article retrieved from the Scopus database, has gained more citations. From Web of Science core collection "Blockchain for AI: Review and Open Research Challenges" cited by most researchers.
- "Blockchain" and "Artificial Intelligence" have the highest keyword co-occurrence link strength.
- "Salah K." has contributed a lot to the research of Blockchain and Artificial Intelligence.

5.1. Limitations in Integrating Blockchain with Artificial Intelligence

5.1.1. Technical

- Scalability:

One of the key problems for today's blockchain platform is scalability. The bitcoin blockchain can process four transactions per second on average, while Ethereum can process twelve transactions per second. In time-critical applications, such performance is

just unacceptable. Many new types of blockchains are improving consensus algorithms significantly and introducing techniques such as sidechain to improve the performance of the Blockchain transactions. However, additional efforts are needed to increase Blockchain's scalability while integrating it with AI. As AI itself a complex technology, addition of blockchain will degrade the performance of the system.

- Interoperability:

Blockchain Developers sometimes violate standards in order to obtain more freedom. However, this can lead to interoperability and communication issues. The most important impediment to interoperability is the existence of many blockchain networks with different features such as consensus models, smart contract functionality, and transaction mechanisms. Establishing connection within two different AI applications, where each has different kind of Blockchain, becomes difficult.

- Privacy:

Public blockchain ledgers provide for safe and authentic data processing, but the data acquired is public and open to all users. This can be a source of privacy violation. By enabling encryption and permitting regulated access to private blockchain ledgers, data privacy may be assured. However, private blockchain platforms will restrict access to and disclosure of massive amounts of data that will affect AI's ability to analyze and perform accurate and precise decision making and analytics. Since privacy enhancing techniques are improving and also distributed learning or federated learning evolving, privacy issues can be mitigated to a certain level.

- Energy Consumption:

The proof-of-work method is used to validate transactions and assure their credibility before they are added to the network. This method demands a significant amount of processing power in order to analyze, verify, and, most importantly, secure the whole network. AI technology also require tremendous computational power to work on huge data and introducing Blockchain in AI application can worsen the situation. It will need lot of energy. As researchers are achieving advancements in Blockchain's consensus algorithm and designing lightweight Blockchains, in future this issue can be resolved.

- Blockchain Security:

Cybercriminals disrupt blockchains in four ways: phishing, routing, Sybil, and a 51 percent attack. Phishing is a deceptive way of acquiring a user's credentials. Gaining access to a user's credentials and other sensitive information might result in losses for both the individual and the blockchain network. Blockchains rely on enormous real-time data transmission. Data may be monitored while it is transferred to internet service providers by attackers. In a Sybil attack, hackers create and use numerous false network identities to overwhelm the network and destroy the system. Mining, especially for large public blockchains, demands a lot of computer power. A miner or a group of miners, on the other hand, might control more than 50% of the mining power on a blockchain network if they pooled enough resources. Controlling the ledger and having the ability to change it gives you more than half of the power. Private blockchains, on the other hand, are protected from a 51 percent attack. The aforementioned types of attacks must be prevented while integrating blockchain with AI.

5.1.2. Legal

- Smart Contract:

Smart contracts are the next step in creative technology, having the potential to save billions of dollars in administrative costs while increasing overall system efficiency. However, regulatory challenges exist, notably in India, where no standards regulate the fundamental parts of a smart contract. Though there has been some progress in terms of legislation and the business sector adopting the smart contracts, the law remains in a grey

area, and building a precise structure to oversee the operation of smart contracts in India would require a lot of hard work. While integrating Blockchain with AI application, smart contracts must be designed and validated by professionals from the area of application.

5.1.3. Regulatory

- Governance:

Due to the infrastructure's extreme decentralized nature, there is no one owner, making governance more challenging. Since there is no longer a trusted third party to govern the operations or stop existing behavior, it sparked concerns about a wide range of regulatory and governance issues. AI is basically reliant on third party data, and hence while integrating Blockchain with AI, the right combination of consortium Blockchain needs to be used.

5.1.4. Ethical

- Over-hype Technical Potential:

Developers of Blockchain should not overestimate the technology's capabilities and then overpromise on what it can offer. Working with professions in medical research can demonstrate the dangers of doing either. While integrating Blockchain with AI, developers must evaluate the complexity and performance of the system.

5.2. Open Innovation, Artificial Intelligence and Blockchain

Open Innovation promotes the use of deliberate incoming and outgoing knowledge to enhance organizational growth and increase opportunities for public use of technology. Open innovation is the polar opposite of traditional strategic alliances, in which internal R&D results in exclusively produced goods that are subsequently marketed by the company. Open innovation results in developing new services and products, reconstructing old products, strong team building, cost cutting, and risk mitigation strategies.

AI is an engineering technology that deals with cognitive activities that are traditionally reserved for human intellect, such as learning, problem-solving, and pattern recognition, data gathering, and processing. The effectiveness of artificial intelligence is determined by the open innovation adaptability of the firms, which enhances their capability to deploy AI and generates a possible cumulative influence on company competition in the global market. It is important to have access to a broad range of data, not just a certain section of the dataset, in order to use AI technology successfully. As a result, open innovation enables businesses to exchange data in a safe environment, protects information, and guarantees that members may freely share it on an ongoing basis in order to grow the market.

Putting in place an open innovation approach comes with a variety of risks and obstacles such as the possibility of disclosing information that was not intended to be shared. As a result of exposing intellectual property, the hosting company may lose its competitive edge. Controlling innovation and managing how contributions impact a project has become more difficult, creating a system for identifying and incorporating external innovation. Blockchain technology, which was created to power cryptocurrency, is increasingly showing its use in a variety of different applications. At the same time, new definitions of open innovation characterize it as a distributed product which can be backed by Blockchain technology due to its distributed working strategy, smart contracts, and consensus protocols.

5.3. Future Directions in Blockchain for Artificial Intelligence

To bring technological evolution in AI security with Blockchain, a thorough understanding of Blockchain's security and privacy structures and improving trust diversity of services are both required. Designing lightweight techniques for consensus algorithms will be an important contribution to Blockchain's technology development. As there will be an increase in dynamic applications (dAPP), the risk of leaks and privacy will be there. Future

work may include network latency testing, power integration, and data packet flow of AI/FL models based on Blockchain. Following Table 21 provides thorough understanding of Blockchain for securing AI along with future directions.

Table 21. Research Gap and Future Research Directions in Blockchain for AI.

Security Triad	AI Security Requirement	Blockchain Solution	Blockchain Component	Description	Research Gap	Future Directions
Confidentiality	Access to Heterogeneous Data	Implications of Access Control Rules through Smart Contract	Smart Contract, Encrypted Block Data	Access to heterogeneous data can be controlled through smart contracts in Blockchain. Data owners can make data available to AI models/third parties while maintaining privacy and security.	Private Blockchain implies restrictions on access and exposure of the data, limiting AI to make correct decisions and analytics on limited data.	There should be some research in Private Blockchains for AI along with homomorphic encryption techniques.
	Data Owner Identity	User Authentication through Blockchain		Digital Identities and Digital Signature of users/devices can be created and managed through Blockchain. It will protect the privacy of User/Device identity.		
Integrity	Trust on Data	Data Owner authentication along with traces of access.	Smart Contract, Mining, Cryptographic Linkage of Blocks, Encrypted Block Data,	The transaction of access to distributed data will be recorded in the Blockchain, which further helps to audit a transaction trail.	Public Blockchains are at high risk. In Public Blockchain, every transaction and user identity are publicly available in the network. The attacker may take advantage of this information to implement a 51% attack.	The computational environment at the Miner side is not protected and not under control. There should be a strategy to protect Hashing power of the miner.
	Trust on Model	Storing Local Gradients from Federated Model in Blockchain		This will create a tamper-proof record of gradients, preventing Federated Learning Model from poisoning attack and establishing trust in the system. The accurate gradients without any alteration by the attacker are fed to the global learning model, ultimately promoting trusted prediction/classification. Consensus algorithm in the Blockchain helps the unreliable nodes in the network to achieve an agreement on data to make the network reliable.		
		Execution of Learning Model through smart contracts		Execution of learning models can be controlled through smart contracts, as smart contracts are executable logic, which automatically gets triggered when any transaction in the network is initiated. This will prevent any attack on learning models and establish trust.		
		Storing Explanations generated by XAI in Blockchain		Blockchain can maintain a tamper-proof, immutable trail of explanations generated by XAI in the distributed ledger. This will improve the functionality of XAI and brings transparency and trust to the AI system.		

Table 21. *Cont.*

Security Triad	AI Security Requirement	Blockchain Solution	Blockchain Component	Description	Research Gap	Future Directions
Availability	Availability of Data/Model	Peer-to-Peer architecture and Distributed Ledger promotes high availability.	P2P Distributed Network, Distributed Ledger	With Peer-to-Peer Architecture of Network, highest level of availability is achieved. Failure of single node does not affect the network. Blockchain replica is available at every node in the network in the form of Distributed Ledger.	Consensus algorithms consume time to commit a block in the ledger after validating it. Integrating Blockchain with AI can introduce a delay in the system.	The research in developing light weight consensus algorithm should receive more exposure.
					Integrating Blockchain with AI doubles the need of computational resources as both are complex technologies.	Future research directions can be optimizing resource utilization for AI and Blockchain.

6. Conclusions

This study highlighted that Blockchain technology is not just for financial transactions or cryptocurrencies. Rather, Blockchain is seen as an emerging technology for securing crucial applications. Since 2019, there has been massive growth in the publications in the Blockchain domain. Many countries contribute to the research of Blockchain and its applicability, but China and the United States are leading in the contribution. Bibliometric analysis was conducted for "Blockchain" AND "Artificial Intelligence" publications. Most of the literature was available in the English language. About 930 documents out of 957 documents were retrieved from Scopus, and 417 documents out of 442 documents were from Web of Science core collection (and are in English language only). For analysis, documents from all of the languages are considered. Network analysis was completed by using the VoSviewer tool for co-citation, co-occurrence, citation, and bibliographic coupling analysis based on documents, authors, sources etc. Each technology has its degree of complexity, but both Blockchain and AI are in situations where they can benefit from each other and help one another. The integration of machine learning and AI into blockchain, and vice versa, can improve basic Blockchain architecture and increase AI capabilities, respectively. In this study, the focus is Blockchain for Secure AI and open innovation. It can make AI more coherent and understandable, and we can track and determine why decisions are made in learning models and how much trustworthy they are. Blockchain and its ledger can record all data and variables that go through a decision made under AI models. AI can securely access heterogeneous data through Blockchain while maintaining the privacy of data providers and data.

Author Contributions: Conceptualization, R.S. and S.P.; methodology, R.S. and S.P.; software, R.S.; validation, R.S., S.P., K.K. and K.R.; formal analysis, R.S.; investigation, R.S.; resources, R.S.; data curation, R.S., and S.P.; writing—original draft preparation, R.S.; writing—review and editing, S.P., and K.R.; visualization, R.S.; supervision, K.K.; project administration, S.P.; funding acquisition, K.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Research Support Fund (RSF) of Symbiosis International (Deemed University), Pune, India.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Casino, F.; Dasaklis, T.K.; Patsakis, C. A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
2. di Francesco Maesa, D.; Mori, P. Blockchain 3.0 Applications Survey. *J. Parallel Distrib. Comput.* **2020**, *138*, 99–114. [CrossRef]
3. Mcbee, M.P.; Wilcox, C. Blockchain Technology: Principles and Applications in Medical Imaging. *J. Digit. Imaging* **2020**, *33*, 726–734. [CrossRef] [PubMed]
4. Park, H.S. Technology Convergence, Open Innovation, and Dynamic Economy. *J. Open Innov. Technol. Mark. Complex.* **2017**, *3*, 24. [CrossRef]
5. Yun, J.J.; Zhao, X.; Jung, K.; Yigitcanlar, T. The Culture for Open Innovation Dynamics. *Sustainability* **2020**, *12*, 5076. [CrossRef]
6. Cockburn, I.; Henderson, R.; Stern, S. *The Impact of Artificial Intelligence on Innovation*; National Bureau of Economic Research: Cambridge, MA, USA, 2018. [CrossRef]
7. João, M.; Correia, M. The Impact of Artificial Intelligence on Innovation Management-A Case Study of Aveiro Region. Ph.D. Thesis, ISCTE Business School, Lisboa, Portugal, 2020.
8. Schenk, E.; Schaeffer, V.; Pénin, J. Blockchain and the Future of Open Innovation Intermediaries: The Case of Crowdsourcing Platforms. In *Managing Digital Open Innovation*; World Scientific Publishing Co.: Singapore, 2020. [CrossRef]
9. Narayan, R.; Tidström, A. Blockchains for Accelerating Open Innovation Systems for Sustainability Transitions. In *Blockchain Economics: Implications of Distributed Ledgers: Markets, Communications Networks, and Algorithmic Reality*; World Scientific Publishing Company: Singapore, 2019. [CrossRef]
10. Lluis De La Rosa, J.; Torres-Padrosa, V.; El-Fakdi, A.; Gibovic, D.; Hornyák, O.; Maicher, L.; Miralles, F. A Survey of Blockchain Technologies for Open Innovation. Available online: http://eia.udg.edu/~{}aelfakdi/papers/woic17.pdf (accessed on 13 August 2021).
11. Comiter, M. Attacking Artificial Intelligence AI's Security Vulnerability and What Policymakers Can Do about It. 2019. Available online: https://www.belfercenter.org/publication/AttackingAI (accessed on 13 August 2021).
12. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A Survey on Security and Privacy of Federated Learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
13. Short, A.R.; Leligou, H.C.; Papoutsidakis, M.; Theocharis, E. Using Blockchain Technologies to Improve Security in Federated Learning Systems. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020, Madrid, Spain, 13–17 July 2020; Institute of Electrical and Electronics Engineers Inc.: Manhattan, NY, USA, 2020; pp. 1183–1188. [CrossRef]
14. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated Learning. *Synth. Lect. Artif. Intell. Mach. Learn.* **2020**, *13*. [CrossRef]
15. Ebrahim, N.A. How to Write a Bibliometric Paper. *Res. Visibility Impact* **2017**. Available online: https://figshare.com/articles/presentation/How_to_Write_a_Bibliometric_Paper/5374615/1 (accessed on 13 August 2021). [CrossRef]
16. Van Eck, N.J.; Waltman, L. Software Survey: VOSviewer, a Computer Program for Bibliometric Mapping. *Scientometrics* **2010**, *84*, 523–538. [CrossRef]
17. Bokhare, A.; Metkewar, P.S. Visualization and Interpretation of Gephi and Tableau: A Comparative Study. In *Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2020*; Springer: Singapore, 2021. [CrossRef]
18. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain Technology Overview. In *NIST Interagency/Internal Report (NISTIR)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019. [CrossRef]
19. Xu, M.; Chen, X.; Kou, G. A Systematic Review of Blockchain. *Financ. Innov.* **2019**, *5*, 27. [CrossRef]
20. Zhang, R.; Xue, R.; Liu, L. Security and Privacy on Blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
21. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-Based Batch Authentication Protocol for Internet of Vehicles. *J. Syst. Archit.* **2021**, *113*, 101877. [CrossRef]
22. Jogunola, O.; Adebisi, B.; Ikpehai, A.; Popoola, S.I.; Gui, G.; Gacanin, H.; Ci, S. Consensus Algorithms and Deep Reinforcement Learning in Energy Market: A Review. *IEEE Internet Things J.* **2021**, *15*, 4211–4227. [CrossRef]
23. Feng, L.; Yang, Z.; Guo, S.; Qiu, X.; Li, W.; Yu, P. Two-Layered Blockchain Architecture for Federated Learning over Mobile Edge Network. *IEEE Netw.* **2021**. [CrossRef]
24. Baranwal Somy, N.; Kannan, K.; Arya, V.; Hans, S.; Singh, A.; Lohia, P.; Mehta, S. Ownership Preserving AI Market Places Using Blockchain. In Proceedings of the 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, 14–17 July 2019; pp. 156–165. [CrossRef]
25. Malhotra, D.; Srivastava, S.; Saini, P.; Singh, A.K. Blockchain Based Audit Trailing of XAI Decisions: Storing on IPFS and Ethereum Blockchain. In Proceedings of the 2021 International Conference on COMmunication Systems and NETworkS, COMSNETS 2021, Bangalore, India, 5–9 January 2021. [CrossRef]
26. Nassar, M.; Salah, K.; ur Rehman, M.H.; Svetinovic, D. Blockchain for Explainable and Trustworthy Artificial Intelligence. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2020**, *10*, e1340. [CrossRef]

27. Aich, S.; Sinai, N.K.; Kumar, S.; Ali, M.; Choi, Y.R.; Joo, M.I.; Kim, H.C. Protecting Personal Healthcare Record Using Blockchain Federated Learning Technologies. In Proceedings of the International Conference on Advanced Communication Technology, ICACT, Pyeongchang, Korea, 7–10 February 2021; pp. 109–112. [CrossRef]
28. Muhammad, G.; Hossain, M.S. A Deep-Learning-Based Edge-Centric COVID-19-Like Pandemic Screening and Diagnosis System within a B5G Framework Using Blockchain. *IEEE Netw.* **2021**, *35*, 74–81. [CrossRef]
29. Lisi, A.; de Salve, A.; Mori, P.; Ricci, L. A Smart Contract Based Recommender System. In *International Conference on the Economics of Grids, Clouds, Systems, and Services*; Springer: Cham, Switzerland, 2019. [CrossRef]
30. Yeh, T.-Y.; Kashef, R. Trust-Based Collaborative Filtering Recommendation Systems on the Blockchain. *Adv. Internet Things* **2020**, *10*, 37–56. [CrossRef]
31. Lisi, A.; de Salve, A.; Mori, P.; Ricci, L.; Fabrizi, S. Rewarding Reviews with Tokens: An Ethereum-Based Approach. *Future Gener. Comput. Syst.* **2021**, *120*, 36–54. [CrossRef]
32. Lisi, A.; de Salve, A.; Mori, P.; Ricci, L. Practical Application and Evaluation of Atomic Swaps for Blockchain-Based Recommender Systems. In *ACM International Conference Proceeding Series*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 67–74. [CrossRef]
33. Wang, S.; Huang, C.; Li, J.; Yuan, Y.; Wang, F.Y. Decentralized Construction of Knowledge Graphs for Deep Recommender Systems Based on Blockchain-Powered Smart Contracts. *IEEE Access* **2019**, *7*, 136951–136961. [CrossRef]
34. Casino, F.; Patsakis, C. An Efficient Blockchain-Based Privacy-Preserving Collaborative Filtering Architecture. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1501–1513. [CrossRef]
35. Zhao, T.; Sun, G.; Feng, X.; Wang, L. Design of Educational Resources-Oriented Fair Recommendation System Based on Consortium Blockchain. In Proceedings of the 2020 International Conference on Networking and Network Applications, NaNA 2020, Haikou, China, 10–13 December 2020; pp. 448–453. [CrossRef]
36. Wang, J.; Wu, Q. Research on the Blockchain-Based Privacy Protection for Internet Financial Product Recommendation Systems. In Proceedings of the 2020 International Conference on Computer Science and Management Technology, ICCSMT 2020, Shanghai, China, 20–22 November 2020; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2020; pp. 310–313. [CrossRef]
37. Omar, A.A.; Bosri, R.; Rahman, M.S.; Begum, N.; Bhuiyan, M.Z.A. Towards Privacy-Preserving Recommender System with Blockchains. In *Communications in Computer and Information Science*; Springer: Singapore, 2019; Volume 1123, pp. 106–118. [CrossRef]
38. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. [CrossRef]
39. Peng, Y.; Chen, Z.; Chen, Z.; Ou, W.; Han, W.; Ma, J. BFLP: An Adaptive Federated Learning Framework for Internet of Vehicles. *Mob. Inf. Syst.* **2021**, *2021*, 6633332. [CrossRef]
40. Jiang, X.; Ma, Z.; Richard Yu, F.; Song, T.; Boukerche, A. Edge Computing for Video Analytics in the Internet of Vehicles with Blockchain. In Proceedings of the DIVANet 2020—Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Aliante, Spain, 22–26 November 2021; pp. 1–7. [CrossRef]
41. Shukla, A.; Bhattacharya, P.; Tanwar, S.; Kumar, N.; Guizani, M. DwaRa: A Deep Learning-Based Dynamic Toll Pricing Scheme for Intelligent Transportation Systems. *IEEE Trans. Veh. Technol.* **2020**, *69*, 12510–12520. [CrossRef]
42. Wang, S.; Sun, S.; Wang, X.; Ning, Z.; Rodrigues, J.J.P.C. Secure Crowdsensing in 5G Internet of Vehicles: When Deep Reinforcement Learning Meets Blockchain. *IEEE Consum. Electron. Mag.* **2020**, *10*, 72–81. [CrossRef]
43. Song, Y.; Fu, Y.; Yu, F.R.; Zhou, L. Blockchain-Enabled Internet of Vehicles with Cooperative Positioning: A Deep Neural Network Approach. *IEEE Internet Things J.* **2020**, *7*, 3485–3498. [CrossRef]
44. Lin, H.; Garg, S.; Hu, J.; Kaddoum, G.; Peng, M.; Shamim Hossain, M. Blockchain and Deep Reinforcement Learning Empowered Spatial Crowdsourcing in Software-Defined Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3755–3764. [CrossRef]
45. Long, Y.; Chen, Y.; Ren, W.; Dou, H.; Xiong, N.N. DePET: A Decentralized Privacy-Preserving Energy Trading Scheme for Vehicular Energy Network via Blockchain and K—Anonymity. *IEEE Access* **2020**, *8*, 192587–192596. [CrossRef]
46. Wang, L.; Liu, J.; Yuan, R.; Wu, J.; Zhang, D.; Zhang, Y.; Li, M. Adaptive Bidding Strategy for Real-Time Energy Management in Multi-Energy Market Enhanced by Blockchain. *Appl. Energy* **2020**, *279*, 115866. [CrossRef]
47. Patil, S.; Joshi, S. Improved Privacy Preservation of Personal Health Records via Tokenization. *Int. J. Pure Appl. Math.* **2018**, *118*, 3035–3045.
48. Bhattacharya, P.; Tanwar, S.; Bodke, U.; Tyagi, S.; Kumar, N. BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications. *IEEE Trans. Netw. Sci. Eng.* **2019**, *8*, 1242–1255. [CrossRef]
49. Chukwu, E.; Garg, L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access* **2020**, *8*, 21196–21214. [CrossRef]
50. Farouk, A.; Alahmadi, A.; Ghose, S.; Mashatan, A. Blockchain Platform for Industrial Healthcare: Vision and Future Opportunities. In *Computer Communications*; Elsevier B.V.: Amsterdam, The Netherlands, 2020; pp. 223–235. [CrossRef]
51. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
52. Sookhak, M.; Jabbarpour, M.R.; Safa, N.S.; Yu, F.R. Blockchain and Smart Contract for Access Control in Healthcare: A Survey, Issues and Challenges, and Open Issues. *J. Netw. Comput. Appl.* **2021**, *178*, 102950. [CrossRef]

53. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef]
54. Cernian, A.; Tiganoaia, B.; Sacala, I.S.; Pavel, A.; Iftemi, A. PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records. *Sensors* **2020**, *20*, 6538. [CrossRef] [PubMed]
55. Pandey, P.; Litoriya, R. Securing E-Health Networks from Counterfeit Medicine Penetration Using Blockchain. *Wirel. Pers. Commun.* **2020**, *117*, 7–25. [CrossRef]
56. Shamim Hossain, M.; Muhammad, G.; Guizani, N. Explainable AI and Mass Surveillance System-Based Healthcare Framework to Combat COVID-I9 like Pandemics. *IEEE Netw.* **2020**, *34*, 126–132. [CrossRef]
57. Zerka, F.; Urovi, V.; Vaidyanathan, A.; Barakat, S.; Leijenaar, R.T.H.; Walsh, S.; Gabrani-Juma, H.; Miraglio, B.; Woodruff, H.C.; Dumontier, M.; et al. Blockchain for Privacy Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging (C-DistriM). *IEEE Access* **2020**, *8*, 183939–183951. [CrossRef]
58. Gupta, R.; Shukla, A.; Tanwar, S. BATS: A Blockchain and AI-Empowered Drone-Assisted Telesurgery System towards 6G. *IEEE Trans. Netw. Sci. Eng.* **2020**. [CrossRef]
59. Alqaralleh, B.A.Y.; Vaiyapuri, T.; Parvathy, V.S.; Gupta, D.; Khanna, A.; Shankar, K. Blockchain-Assisted Secure Image Transmission and Diagnosis Model on Internet of Medical Things Environment. *Pers. Ubiquitous Comput.* **2021**. [CrossRef]
60. Veeramakali, T.; Siva, R.; Sivakumar, B.; Senthil Mahesh, P.C.; Krishnaraj, N. An Intelligent Internet of Things-Based Secure Healthcare Framework Using Blockchain Technology with an Optimal Deep Learning Model. *J. Supercomput.* **2021**. [CrossRef]
61. Mohammed, A.; Nahom, H.; Tewodros, A.; Habtamu, Y.; Hayelom, G. Deep Reinforcement Learning for Computation Offloading and Resource Allocation in Blockchain-Based Multi-UAV-Enabled Mobile Edge Computing. In Proceedings of the 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 18–20 December 2020. [CrossRef]
62. Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. *Big Data Cogn. Comput.* **2020**, *4*, 28. [CrossRef]
63. Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet* **2021**, *13*, 24. [CrossRef]
64. Dhelim, S.; Ning, H.; Farha, F.; Chen, L.; Atzori, L.; Daneshmand, M. IoT-Enabled Social Relationships Meet Artificial Social Intelligence. *IEEE Internet Things J.* **2021**. [CrossRef]
65. Kumar, R.; Wang, W.Y.; Kumar, J.; Yang, T.; Khan, A.; Ali, W.; Ali, I. An Integration of Blockchain and AI for Secure Data Sharing and Detection of CT Images for the Hospitals. *Comput. Med. Imaging Graph.* **2021**, *87*, 101812. [CrossRef]
66. Krittanawong, C.; Rogers, A.J.; Aydar, M.; Choi, E.; Johnson, K.W.; Wang, Z.; Narayan, S.M. Integrating Blockchain Technology with Artificial Intelligence for Cardiovascular Medicine. *Nat. Rev. Cardiol.* **2020**, *17*, 259–260. [CrossRef] [PubMed]
67. Azzaoui, A.E.; Singh, S.K.; Pan, Y.; Park, J.H. Block5GIntell: Blockchain for AI-Enabled 5G Networks. *IEEE Access* **2020**, *8*, 145918–145935. [CrossRef]
68. Kashif, H.; Sarwar, B.I.; Nadeem, S.; Waheed, A.; Zaigham, M.; Tayyaba, R. Integration of 5G and Block-Chain Technologies in Smart Telemedicine Using IoT. *J. Healthc. Eng.* **2021**, *21*, 8814364. [CrossRef]
69. Zhou, S.; Huang, H.; Chen, W.; Zheng, Z.; Guo, S. Pirate: A Blockchain-Based Secure Framework of Distributed Machine Learning in 5G Networks. *IEEE Netw.* **2020**, *34*, 84–91. [CrossRef]
70. Kim, H.; Park, J.; Bennis, M.; Kim, S.L. Blockchained On-Device Federated Learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [CrossRef]
71. Qu, Y.; Pokhrel, S.R.; Garg, S. A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2964–2973. [CrossRef]
72. Yang, W.; Lim, B.; Luong, N.C.; Hoang, D.T. Federated Learning in Mobile Edge Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2031–2063. [CrossRef]
73. Alrubei, S.; Ball, E.; Rigelsford, J. The Use of Blockchain to Support Distributed AI Implementation in IoT Systems. *IEEE Internet Things J.* **2021**. [CrossRef]
74. Yamin, M.M.; Ullah, M.; Ullah, H.; Katt, B. Weaponized AI for Cyber Attacks. *J. Inf. Secur. Appl.* **2021**, *57*, 102722. [CrossRef]
75. Ren, K.; Zheng, T.; Qin, Z.; Liu, X. Adversarial Attacks and Defenses in Deep Learning. *Engineering* **2020**, *6*, 346–360. [CrossRef]
76. Kamat, P.; Gite, S.; Patil, S. Mobile Agent Communication, Security Concerns, and Approaches: An Insight into Different Kinds of Vulnerabilities a Mobile Agent Could Be Subjected to and Measures to Control Them. In *Research Anthology on Securing Mobile Technologies and Applications*; IGI Global: Hershey, PA, USA, 2021; pp. 23–34.
77. Asfia, U.; Kamuni, V.; Sutavani, S.; Sheikh, A.; Wagh, S.; Singh, N.M. A Blockchain Construct for Energy Trading against Sybil Attacks. In Proceedings of the 2019 27th Mediterranean Conference on Control and Automation (MED), Akko, Israel, 1–4 July 2019. [CrossRef]
78. Bera, B.; Das, A.K.; Obaidat, M.; Vijayakumar, P.; Hsiao, K.F.; Park, Y. AI-Enabled Blockchain-Based Access Control for Malicious Attacks Detection and Mitigation in IoE. *IEEE Consum. Electron. Mag.* **2020**. [CrossRef]
79. Hajizadeh, M.; Afraz, N.; Ruffini, M.; Bauschert, T. Collaborative Cyber Attack Defense in SDN Networks Using Blockchain Technology. In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020. [CrossRef]

80. Javaid, U.; Siang, A.K.; Aman, M.N.; Sikdar, B. Mitigating IoT Device Based DDoS Attacks Using Blockchain. In Proceedings of the CRYBLOCK 2018—Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018, Munich, Germany, 15 June 2018; pp. 71–76. [CrossRef]
81. Lei, I.S.; Tang, S.K.; Tse, R. Integrating Consortium Blockchain into Edge Server to Defense against Ransomware Attack. In *Procedia Computer Science*; Elsevier B.V.: Amsterdam, The Netherlands, 2020; Volume 177, pp. 120–127. [CrossRef]
82. Liang, L.; Cao, X.; Zhang, J.; Sun, C. SLC: A Permissioned Blockchain for Secure Distributed Machine Learning against Byzantine Attacks. In Proceedings of the 2020 Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020. [CrossRef]
83. Meng, W.; Li, W.; Yang, L.T.; Li, P. Enhancing Challenge-Based Collaborative Intrusion Detection Networks against Insider Attacks Using Blockchain. *Int. J. Inf. Secur.* **2020**, *19*, 279–290. [CrossRef]
84. Salah, K.; Member, S.; Rehman, M.H.U.R. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
85. Dinh, T.N.; Thai, M.T. AI and Blockchain: A Disruptive Integration. *Computer* **2018**, *51*, 48–53. [CrossRef]
86. Corea, F. The Convergence of AI and Blockchain. In *Applied Artificial Intelligence: Where AI Can Be Used in Business*; Springer: Cham, Switzerland, 2019. [CrossRef]