*electronics*

*Review*

# Blockchain Systems in Embedded Internet of Things: Systematic Literature Review, Challenges Analysis, and Future Direction Suggestions

**Mehdi Darbandi [1], Hamza Mohammed Ridha Al-Khafaji [2], Seyed Hamid Hosseini Nasab [3,4], Ahmad Qasim Mohammad AlHamad [5], Beknazarov Zafarjon Ergashevich [6] and Nima Jafari Navimipour [7,8,*]**

[1] Department of Electrical Engineering, Eastern Mediterranean University, Gazimagusa 34325, Turkey
[2] Biomedical Engineering Department, Al-Mustaqbal University College, Hillah 51001, Iraq
[3] Department of Management, Payame Noor University (PNU), Tehran P.O. Box 19395-4697, Iran
[4] Department of Computing & Information Technology, Payame Noor University (PNU), Tehran P.O. Box 19395-4697, Iran
[5] College of Business Administration, University of Sharjah, Academic City, Sharjah 27272, United Arab Emirates
[6] Department of Insurance and Pension, Tashkent Institute of Finance, Tashkent 100000, Uzbekistan
[7] Future Technology Research Center, National Yunlin University of Science and Technology, Douliou, Yunlin 64002, Taiwan
[8] Department of Computer Engineering, Faculty of Engineering and Natural Sciences, Kadir Has University, Istanbul 34083, Turkey
* Correspondence: jnnima@yuntech.edu.tw or nima.navimipour@khas.edu.tr

**Citation:** Darbandi, M.; Al-Khafaji, H.M.R.; Hosseini Nasab, S.H.; AlHamad, A.Q.M.; Ergashevich, B.Z.; Jafari Navimipour, N. Blockchain Systems in Embedded Internet of Things: Systematic Literature Review, Challenges Analysis, and Future Direction Suggestions. *Electronics* **2022**, *11*, 4020. https://doi.org/10.3390/electronics11234020

Academic Editor: Juan Antonio López Ramos

Received: 21 October 2022
Accepted: 30 November 2022
Published: 4 December 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

**Abstract:** Internet of Things (IoT) environments can extensively use embedded devices. Without the participation of consumers; tiny IoT devices will function and interact with one another, but their operations must be reliable and secure from various threats. The introduction of cutting-edge data analytics methods for linked IoT devices, including blockchain, may lower costs and boost the use of cloud platforms. In a peer-to-peer network such as blockchain, no one has to be trusted because each peer is in charge of their task, and there is no central server. Because blockchain is tamper-proof, it is connected to IoT to increase security. However, the technology is still developing and faces many challenges, such as power consumption and execution time. This article discusses blockchain technology and embedded devices in distant areas where IoT devices may encounter network shortages and possible cyber threats. This study aims to examine existing research while also outlining prospective areas for future work to use blockchains in smart settings. Finally, the efficiency of the blockchain is evaluated through performance parameters, such as latency, throughput, storage, and bandwidth. The obtained results showed that blockchain technology provides security and privacy for the IoT.

**Keywords:** blockchain; embedded device; cyber security; secure system; internet of things; challenges

## 1. Introduction

The idea of the Internet of Things (IoT) was initially introduced by Kevin Ashton [1,2] during the period of wireless communications and embedded systems [3]. Things include anything that is always present, such as a tablet, smartphone, watch, etc. [4,5]. The Internet significantly impacts people's lives and communication, from professional to social relationships [6,7]. Industrial designs, UAVs, wireless communication technologies, electromechanical systems, and information and communication systems have recently made significant advancements, fostering the IoT [8–10]. Information gathering about our world and surroundings may be done at a much greater level with a network of inexpensive sensors and linked devices [11]. In fact, such in-depth knowledge will boost productivity and provide cutting-edge services in various application fields, such as ubiquitous healthcare and smart city services [12,13]. We saw IoT advancing into agriculture, the transportation system, thermal and health systems and other businesses, in addition to the phenomenal expansion in several sensing devices connected to the Internet [14,15]. Smart services and items interact on their own thanks to IoT. IoT is the connectivity of computing devices that are still integrated into common objects in order to send or receive data over the Internet.

Consequently, since IoT has lately attained enormous popularity, this promising technology presents some security issues. Additionally, a Deloitte analysis by Jain [16] indicates that security continues to be the biggest obstacle to the expansion of IoT networks [17]. In the IoT context, privacy, permission, information storage, access control, and system configuration present the most security problems [18]. Because such devices cannot afford advanced security technologies, basic security measures such as asymmetric encryption are frequently used [19]. These measures adhere to the IoT infrastructure's low-cost premise. However, their defenses are insufficient to maintain the five security objectives of data availability, integrity, authentication, confidentiality, and nonrepudiation, which poses a threat to the future adoption of IoT [20–22].

The scalability, decentralization, and trustworthiness of blockchain technology, among other attributes, make it the most suitable for use as a foundational element of IoT networks [4]. Therefore, this study suggests blockchain as a solution to alleviate such weaknesses and hasten the adoption of IoT. A framework for safeguarding IoT ecosystems is being developed using blockchain [20]. The blockchain was primarily created to record and verify cryptocurrency transactions, but it is anticipated to play a significant role in controlling, monitoring, and protecting IoT devices [17,23]. Due to its enormous potential and myriad uses, blockchain technology is currently the subject of extensive study and investment. Additionally, blockchain technology is emerging as the most significant technological advance since the creation of the Internet, and in the next years, it is anticipated to play a big role in many enterprises [24]. Many recent advancements in the IoT sector are centered on blockchain technology [25]. Numerous IoT services' susceptibility to assaults and difficulties is one explanation for this. Many problems relating to cyber-physical systems in the IoT industry can be resolved through blockchain.

Several problems need to be addressed before blockchain can successfully be implemented in the IoT area, despite the very compelling qualities of the technology

Most recently suggested techniques need large numbers of participating nodes to run blockchain-based consensus algorithms, which is beyond the capacity of IoT devices [26]. Some famous issues in this area are:

- Latency: Time and processing resources need to conduct encryption on each asset in a blockchain-based ecosystem [27]. IoT ecosystems are quite varied. IoT networks are made up of devices with highly diverse processing capabilities compared to general computer networks; thus, not all can perform the same encryption methods at the appropriate pace [28];
- Data concurrency and throughput issue: IoT networks have high concurrency because the devices stream data continually [29]. Because of its intricate cryptographic protocol and consensus procedures, the blockchain's throughput is constrained [30,31]. The main task is to increase the blockchain's throughput in order to handle the requirement for frequent transactions in IoT devices [32,33];
- Vulnerability: There are still several outstanding problems surrounding blockchain, such as generating distributed trust, while eliminating weaknesses such as DoS assaults and the famed 51% attack [34].
- This paper's contributions are as follows:
- Outlining a Systematic Literature Review (SLR) for blockchain systems, a model proposal for IoT, and significant developments in this area;
- Listing the deficiencies and difficulties with IoT security and trust evaluation and recommendation methodologies;
- Discussing key IoT security and trustworthiness considerations and identifying any lingering issues for further research.

The continuation of the article is as follows: First, the methodology is described in Section 2. Then, the results and bibliographic maps and charts are analyzed in systematic and bibliographic reviews. Section 3 indicates the results of the investigation. Section 4 deals with blockchain and its applications. In Section 5, open issues and future directions are described, and the conclusion is stated in Section 6.

Table 1 shows the phrases and their abbreviations.

**Table 1.** Abbreviations used in the paper.

| Phrase | Abbreviation |
|---|---|
| Internet of Things | IoT |
| Inter Planetary File System | IPFS |
| Software Defined Networks | SDN |
| Denial of Service | DoS |
| Peer to Peer | P2P |
| Address Resolution Protocol | ARP |
| Proof-of-Work | POW |
| Network Function Virtualization | NFV |
| Decentralized Autonomous Organization | DAO |
| Hierarchical Identity Based Encryption | HIBE |
| Industrial IoT | IIoT |

## 2. Research Design, Methodology, and Data Collection

This review is both an SLR [35,36] and a bibliometric analysis [37,38]. The goal of the bibliometric review is to offer an overview of the status of the field's knowledge at the time it was conducted, look back on earlier research, spot trends, and provide answers to the following questions:

RQ1: How does the development of the IoT affect the publication trend in the blockchain system? This statistical inquiry focuses on published articles that address IoT security, trust, and blockchain, employing datasets or benchmarks, and evaluating the case studies.

RQ2: What role do trust and security play in the IoT's expanding use of blockchain technology? The inquiry aims to assess IoT security and trust metrics over time in published research and emphasize the importance of blockchain accuracy in IoT.

RQ3: Which blockchain system flaws and solutions were found for potential IoT developments in the future? This inquiry looks at IoT suggestion weaknesses and appropriately identifies methods to boost security and trustworthiness.

RQ4: What are the key research drivers behind securing the IoT using a blockchain system? To learn more about blockchain solutions for the IoT environment and how successful they are in terms of security.

RQ5: What are the current blockchain-based solutions to security issues in the IoT environment? Recognize, evaluate, and categorize blockchain-based IoT security techniques.

The outline of the specific study framework supporting this paper is depicted in Figure 1.

This article looked for relevant published papers using the SCOPUS, WoS, and Google Scholar databases. The Scopus database's entry of the following words led to choosing papers:

"Title: Blockchain AND (IoT OR "Internet of Things" OR "Internet of Thing")"

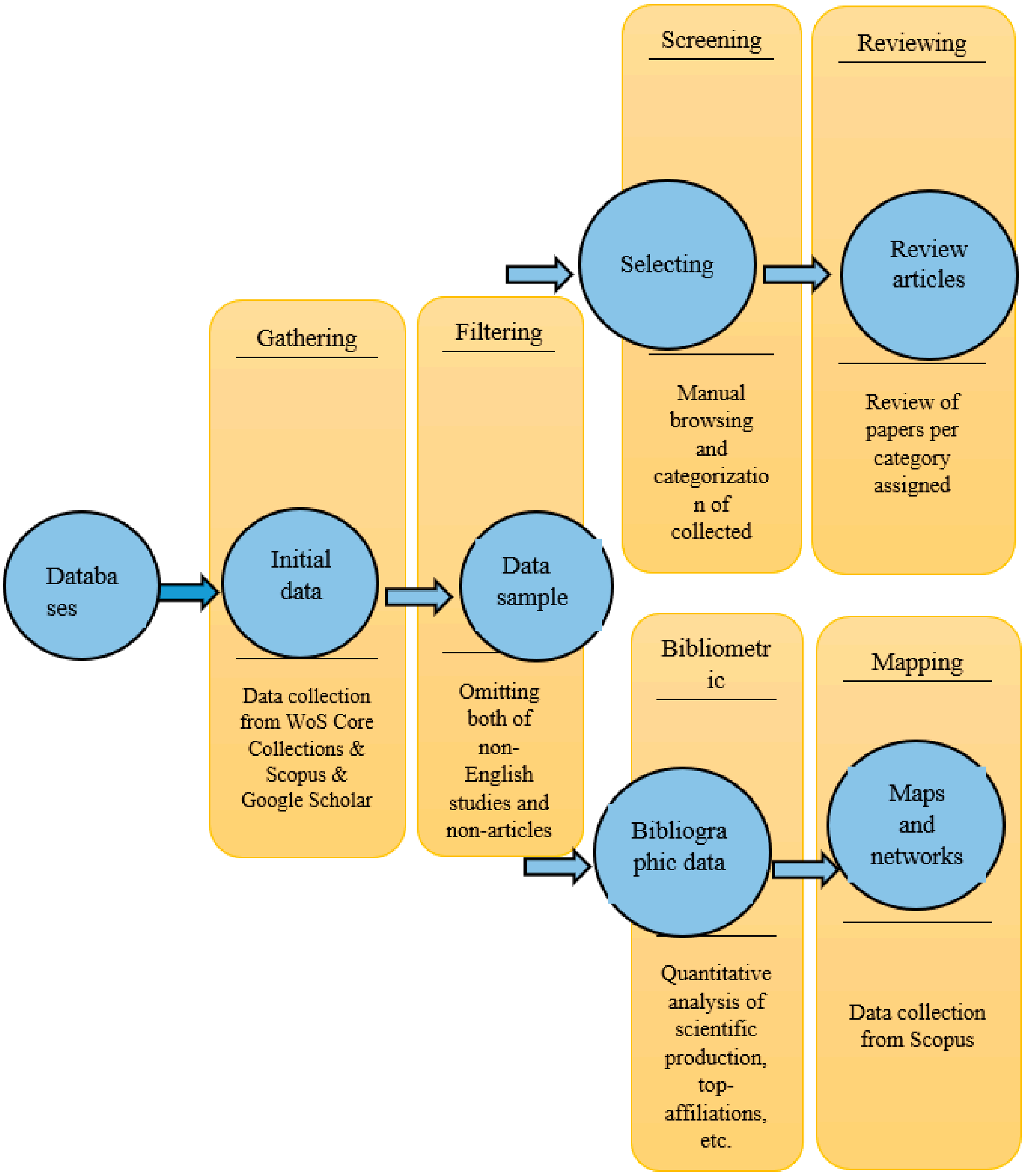
Screening
Reviewing
Selecting
Review articles
Gathering
Filtering
Manual browsing and categorizatio n of collected
Review of papers per category assigned
Databa ses
Initial data
Data sample
Bibliometr ic
Mapping
Data collection from WoS Core Collections & Scopus & Google Scholar
Omitting both of non-English studies and non-articles
Bibliogra phic data
Maps and networks
Quantitative analysis of scientific production, top-affiliations, etc.
Data collection from Scopus

**Figure 1.** Paper selection process scheme.

The queries utilized to obtain the papers and documents for this investigation from the databases are indicated in the term above. The findings containing the terms on the titles of the papers accessible were found using Boolean operators. The initial search produced a lengthy list of papers: 1566 papers from the WoS database, 4480 results from the Google Scholar database, and 2454 papers from the Scopus database were the output of this search on 5 September. After applying some filters, such as removing non-English articles and selecting only the results that include the articles, the result was obtained according to the diagram in Figure 2.

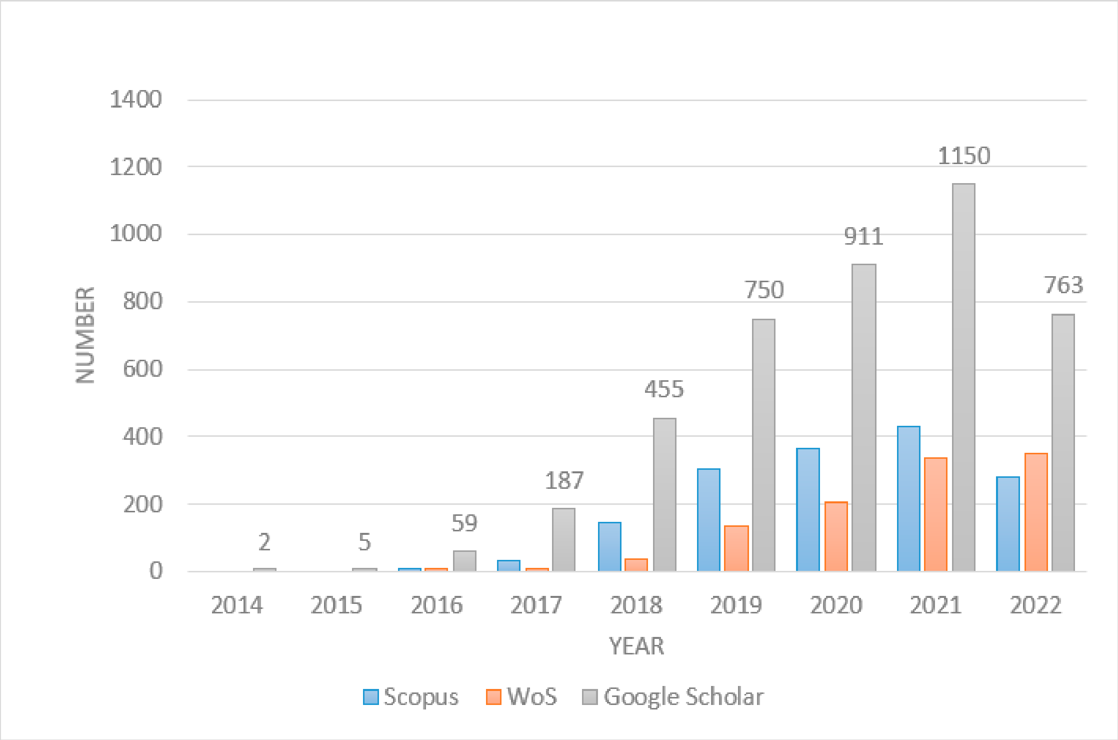

**Figure 2.** Growth of research articles.

The following were not included: non-research papers, conference proceedings, discussions, reports, case studies, editorials, comments, and letters to the editor. The search was limited to peer-reviewed literature to guarantee that only research publications were included for analysis.

The following graph resulting from the filter includes 933 articles from WoS, 1072 articles from the Scopus database, and 4180 articles from the Google Scholar database.

The results of the examination of the diagram in Figure 2 illustrate that the topic under investigation and the relation of IoT with the blockchain are up-to-date and have appeared in the last several years. Accordingly, the importance and value of the subject are revealed. Generally, the number of publications has increased over time, especially in 2021.

### 2.1. *Systematic Literature Review*

Identification, synthesis, and evaluation of all quantitative and/or qualitative data are required for SLR in order to produce a robust, experimentally derived response to a specific research topic [39–42]. The EndNote reference management program was used to organize the retrieved articles into libraries and check them for duplications. Only one of the duplicate articles was saved for analysis. To limit the scope of the study in this section, it was necessary to select a specific field. By reviewing the titles of the articles, proposed architectures for the IoT on the blockchain platform were selected. Data have been selected from publications of the last two or three years to provide a state-of-art review. To properly determine the significance of the data in the contribution of this study and apply the exclusion and inclusion criteria, it was essential in certain cases to read the whole publications (Table 2).

**Table 2.** Inclusion and exclusion criteria.

| ■ **Inclusion Criteria** | ■ **Exclusion Criteria** |
|---|---|
| ■ Papers published from the year 2018 to 2022 were included. | ■ Missing record papers were also excluded. |
| ■ Papers' titles related to blockchain architectures and IoT were selected. | ■ Duplicate articles are not considered. |
| ■ Papers from WoS and Scholar and Scopus digital sources were included. | ■ Articles whose titles did not match the expected content were excluded. |

Subsequently, each paper in a set was thoroughly reviewed, examined, and summarized during the reviewing step. Table 3 lists the submitted papers that satisfy all inclusion requirements. Table 3 lists some characteristics of the chosen papers, including the authors and the name of the publication.

**Table 3.** Selected Articles.

| Title | Type | Authors | Journal | Classification | Keywords | Ref No. |
|---|---|---|---|---|---|---|
| ■ An IoT-applicable access control model under a double-layer blockchain | ■ Official publication | ■ Li Ziyuan<br>■ Jialu Hao<br>■ Jian Liu<br>■ Huimei Wang<br>■ Ming Xian | ■ IEEE Transactions on Circuits and Systems | ■ Double-Blockchain Architecture | ■ Blockchain<br>■ Access control<br>■ Smart contracts<br>■ Servers<br>■ Cryptography<br>■ Loans and mortgages<br>■ Data models | [43] |
| ■ A double-blockchain architecture for secure storage and transaction on the IoT networks. | ■ Journal | ■ Aldriwish Khalid | ■ International Journal of Computer Science & Network Security | ■ Double-Blockchain Architecture | ■ IoT<br>■ Blockchain<br>■ Information security<br>■ Encryption | [44] |
| ■ A double-blockchain solution for agricultural sampled data security in IoT network. | ■ Journal | ■ Ren Wei<br>■ Xutao Wan<br>■ Pengcheng Gan | ■ Future Generation Computer Systems | ■ Double-Blockchain Architecture | ■ Agricultural<br>■ Blockchain<br>■ Cross-chain<br>■ Data security<br>■ Merkle Patricia Trie | [45] |

**Table 3.** *Cont.*

| Title | Type | Authors | Journal | Classification | Keywords | Ref No. |
|---|---|---|---|---|---|---|
| ■ Stochastic Analysis of Double Blockchain Architecture in IoT Communication Networks | ■ Official publication | ■ Hao, Xin Phee<br>■ Lep Yeoh<br>■ Zijie Ji<br>■ Yao Yu<br>■ Branka Vucetic<br>■ Yonghui Li | ■ IEEE Internet of Things Journal | ■ Double-Blockchain Architecture | ■ Blockchains<br>■ IoT Interference<br>■ Stochastic processes<br>■ Smart contracts<br>■ Scalability<br>■ Security | [46] |
| ■ An energy-efficient SDN controller architecture for IoT networks with the blockchain-based security | ■ Official publication | ■ Yazdinejad, Abbas<br>■ Reza M. Parizi<br>■ Ali Dehghantanha<br>■ Qi Zhang<br>■ Kim-Kwang Raymond Choo | ■ IEEE Transactions on Services Computing | ■ SDN-based architecture | ■ Blockchain<br>■ Computer architecture<br>■ Energy consumption<br>■ Routing protocols<br>■ IoT Authentication | [47] |
| ■ Bloc-Sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT | ■ Conference | ■ Abdulqadder Ihsan H.<br>■ Shijie Zhou<br>■ Deqing Zou<br>■ Israa T. Aziz<br>■ Syed Muhammad Abrar Akber | ■ In 2020 IEEE 20th International Conference on Communication Technology (ICCT) | ■ SDN-based architecture | ■ Security<br>■ Blockchain<br>■ Authentication<br>■ Denial-of-service attack<br>■ Monitoring<br>■ Intrusion detection<br>■ Inspection | [48] |
| ■ A Blockchain architecture for SDN-enabled tamper-resistant IoT networks | ■ Journal | ■ Hakiri Akram<br>■ Bassem Sellami<br>■ Sadok Ben Yahia<br>■ Pascal Berthou | ■ In the 2020 Global Information Infrastructure and Networking Symposium (GIIS) | ■ SDN-based architecture | ■ Scalability<br>■ Smart contracts<br>■ Computer architecture<br>■ Blockchain<br>■ Network function virtualization,<br>■ Security<br>■ Software-defined networking | [49] |

**Table 3.** *Cont.*

| Title | Type | Authors | Journal | Classification | Keywords | Ref No. |
|---|---|---|---|---|---|---|
| ▪ Towards a Blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks | ▪ Conference | ▪ Hakiri, Akram<br>▪ Behnam Dezfouli | ▪ In Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security | ▪ SDN-based architecture | ▪ SDN<br>▪ NFV<br>▪ IoT<br>▪ Blockchain<br>▪ Security<br>▪ Trust and Confidence | [50] |
| ▪ BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain | ▪ Journal | ▪ ABBASSI Younes<br>▪ Habib Benlahmer | ▪ International journal of electrical and computer engineering systems | ▪ SDN-based architecture | ▪ IoT Software-Defined Networking<br>▪ OpenFlow<br>▪ Blockchain<br>▪ BCSDN-IoT Architecture | [51] |
| ▪ Intelligent charging path planning for IoT network over Blockchain-based edge architecture | ▪ Official publication | ▪ Cho Hsin-Hung<br>▪ Hsin-Te Wu<br>▪ Chin-Feng Lai<br>▪ Timothy K. Shih<br>▪ Fan-Hsun Tseng | ▪ IEEE Internet of Things Journal | ▪ Edge/fog-based Architecture | ▪ Edge computing<br>▪ Cloud computing<br>▪ IoT Wireless sensor networks<br>▪ Magnetic resonance<br>▪ Vehicle dynamics | [52] |
| ▪ BlockEdge: Blockchain-edge framework for Industrial IoT (IioT) networks | ▪ Official publication | ▪ Kumar Tanesh<br>▪ Erkki Harjula<br>▪ Muneeb Ejaz<br>▪ Ahsan Manzoor<br>▪ Pawani Porambage<br>▪ Ijaz Ahmad<br>▪ Madhusanka Liyanage<br>▪ An Braeken<br>▪ Mika Ylianttila | ▪ IEEE Access | ▪ Edge/fog-based Architecture | ▪ Blockchain<br>▪ Edge computing<br>▪ Fog computing<br>▪ Cloud computing<br>▪ Industrial IoT<br>▪ Industry 4.0<br>▪ Performance evaluation | [53] |

**Table 3.** *Cont.*

| Title | Type | Authors | Journal | Classification | Keywords | Ref No. |
|---|---|---|---|---|---|---|
| Fog chain: a fog computing architecture integrating blockchain and the IoT for personal health records | Official publication | Mayer André Henrique<br>Vinicius Facco Rodrigues<br>Cristiano André da Costa<br>Rodrigo da Rosa Righi<br>Alex Roehrs<br>Rodolfo Stoffel Antunes | IEEE Access | Edge/fog-based Architecture | Blockchains,<br>Cloud computing<br>Medical services<br>Edge computing<br>IoT Computer architecture<br>P2P computing | [54] |
| Edge-based blockchain architecture for event-driven IoT using hierarchical identity-based encryption | Official publication | Pavithran Deepa<br>Jamal N. Al-Karaki<br>Khaled Shaalan | Information Processing & Management | Edge/fog-based Architecture | Blockchain<br>IoT<br>Cloudlet<br>Mobile edge computing<br>Identity-Based Encryption | [55] |
| Towards a smart healthcare system: an architecture based on IoT, Blockchain, and fog computing | Journal | Fetjah, Laila<br>Kebira Azbeg<br>Ouail Ouchetto<br>Said Jai Andaloussi | International Journal of Healthcare Information Systems and Informatics (IJHISI) | Edge/fog-based Architecture | Artificial Intelligence (AI)<br>Blockchain<br>Fog Computing<br>Healthcare<br>IoT<br>Remote Patient Monitoring<br>Smart Contracts | [56] |
| A lightweight hash-based blockchain architecture for industrial IoT | Official publication | Seok Byoungjin<br>Jinseong Park<br>Jong Hyuk Park | Applied Sciences | Lightweight Architecture | Industrial IoT<br>Blockchain<br>Lightweight hash<br>Security<br>Resource-constrained devices | [57] |

**Table 3.** *Cont.*

| Title | Type | Authors | Journal | Classification | Keywords | Ref No. |
|---|---|---|---|---|---|---|
| ■ Fogbus: A blockchain-based lightweight framework for edge and fog computing | ■ Journal | ■ Shreshth Tuli<br>■ Redowan Mahmud<br>■ Shikhar Tuli<br>■ Rajkumar Buyya | ■ Journal of Systems and Software | ■ Lightweight Architecture | ■ Fog Computing<br>■ Edge Computing<br>■ Cloud Computing<br>■ IoT Blockchain | [58] |
| ■ A decentralized lightweight blockchain-based authentication mechanism for IoT systems | ■ Journal | ■ Khalid Umair<br>■ Muhammad Asim<br>■ Thar Baker<br>■ Patrick CK Hung<br>■ Muhammad Adnan Tariq<br>■ Laura Rafferty | ■ Cluster Computing | ■ Lightweight Architecture | ■ IoT Blockchain<br>■ Fog computing<br>■ Authentication<br>■ Smart city | [59] |
| ■ Comparative study on hash functions for lightweight blockchain in the IoT | ■ Journal | ■ Alfrhan Aishah<br>■ Tarek Moulahi<br>■ Abdulatif Alabdulatif | ■ Blockchain: Research and Applications | ■ Lightweight Architecture | ■ Lightweight blockchain<br>■ IoT Hash<br>■ Cybersecurity | [60] |
| ■ Tikiri—Towards a lightweight blockchain for IoT | ■ Journal | ■ Bandara Eranga<br>■ Deepak Tosh<br>■ Peter Foytik<br>■ Sachin Shetty<br>■ Nalin Ranasinghe<br>■ Kasun De Zoysa | ■ Future Generation Computer Systems | ■ Lightweight Architecture | ■ Blockchain<br>■ Smart contact<br>■ Edge computing<br>■ IoT<br>■ Big data | [61] |
| ■ A lightweight blockchain-based IoT identity management approach | ■ Official publication | ■ Bouras Mohammed Amine<br>■ Qinghua Lu<br>■ Sahraoui Dhelim<br>■ Huansheng Ning | ■ Future Internet | ■ Lightweight Architecture | ■ Identity management<br>■ Blockchain<br>■ IoT Distributed ledger technology<br>■ Sensor<br>■ Access control | [62] |

## *2.2. Reviews and Surveys Category*

Four sets of reviews were found in this category.

### 2.2.1. Double-Blockchain Architecture

Blockchain technologies provide significant assistance for IoT development. The blockchain offers a secure way to communicate across IoT devices. Nevertheless, malicious intrusions and cyber assaults pose a hazard to IoT systems. Three obstacles must be overcome for IoT application security: detecting intrusions and assaults, a secure connection, and compressed information storage [44]. The double blockchain is particularly a private blockchain that has been set up over a cloud-fog communication network. It is made up of a reputation blockchain that stores information about IoT device reputation in the near-terminal fog layer and an information blockchain that stores vast volumes of IoT data in the cloud layer [46].

Li, Hao [43] suggested an innovative double-layer blockchain structure with an IoT-applicable access control mechanism that separates the mortgage/registration and control operations. With the help of this design, IoT devices' communication costs were lowered, and quick responses were made possible. Attribute-based access policies for resource objects were built using a linear secret-sharing mechanism to guarantee fine-grained access control. They also put an intelligent contract prototype on Ethereum and Fisco Bcos. Numerous tests and numerical analyses proved the viability of the suggested concept.

Aldriwish [44] suggested a double-blockchain-based system to increase the security of communication transactions and the effectiveness of the data compression technique used to store data. Employing ellipse curve cryptography in a double-blockchain instance improved information security. The compressed sensing technique made sure that the data was compressed. The results of the experiments showed that the suggested technique was superior to earlier comparable studies in terms of accuracy, security, and storage performance.

Ren, Wan [45] suggested an IoT and IPFS (Interplanetary File System) storage-based double-blockchain solution for the safety of agricultural sampling data. They stored the content of the sampled data using the IPFS network, and the suggested system may retrieve the entire data segment using an Oracle method. Subsequently, they developed a consortium blockchain, depending on Ethereum technology, for the agricultural sample data chain and improved Merkle Patricia Trie-based accounts for each type of sampled data. In order to retain a public record in case malicious assaults occur, a block hash was produced and uploaded to Ethereum's main chain once the data had been recorded in blocks in the agricultural sample data chain. According to simulation findings, the suggested solution had a shorter time requirement than cloud storage and blockchain-only storage, and its system was more reliable than the other two systems.

To securely manage sensitive information and reputational data in massive wireless IoT networks, Hao, Yeoh [46] provided real-world stochastic modeling and a thorough performance analysis of double blockchain. The transmission delay, storage space, and tampering time of the IoT fog nodes in the double blockchain structure were determined using unique closed-form expressions depending on these models. The double blockchain architecture's low latency, great storage scalability, and better security were emphasized by numerical simulations, which also shed light on the performance advantages of various densities of fog nodes and IoT devices.

According to the proposed models, the two-layer blockchain architecture improves IoT communication, including reducing overhead and improving transaction safety and data protection. A summary of the features of these architectures is provided in Table 4.

**Table 4.** A summary of double-blockchain architecture case studies.

| Ref No. | Case Study | Technique | Achievement | Tools |
|---|---|---|---|---|
| [43] | ▪ Lack of access control in IoT<br>▪ Lack of rapid response in IioT scenarios | ▪ Double-layer blockchain architecture | ▪ Reducing the communication overhead<br>▪ Achieving rapid response | ▪ Implemented |
| [44] | ▪ Lack of communication transactions' safety<br>▪ Lack of the information compression method for the stored data. | ▪ Ellipse Curve Cryptography<br>▪ Double-blockchain | ▪ Improving security<br>▪ Improving accuracy<br>▪ Improving storage performance | ▪ Simulation |
| [45] | ▪ Long and difficult the identity-based searching | ▪ IPFS storage-based double-blockchain solution | ▪ Smaller time consumption | ▪ Simulation |
| [46] | ▪ Lack of secure information<br>▪ Lack of reputation data management | ▪ Double blockchain | ▪ High scalability<br>▪ Low latency<br>▪ High security | ▪ Simulation |

### 2.2.2. SDN-Based Architecture

Infrastructures should be able to attain high degrees of security and confidentiality, while being sustainable, open, and adaptable to adapt to the various needs of applications considering the diversity of applications and their quick evolution. New paradigms are developing to satisfy these demands. One of them is the Software Defined Networks (SDN) paradigm, which enables the dynamic programming of various programs and gadgets to give end-to-end service chains [63]. Parallel to this, the IoT is using the blockchain paradigm more often, enabling distributed transactions between linked things, such as financial transactions or "smart contracts" [51].

Yazdinejad, Parizi [47] investigated the possibilities of combining SDN and blockchain to address some of the issues. They specifically suggested a cluster-based, blockchain-enabled SDN controller structure for IoT networks that used a novel routing protocol, which was safe and resource-efficient. By eliminating Proof-of-Work (POW) and utilizing an effective authentication technique with distributed trust, the structure employed public and private blockchains for P2P communication across IoT devices and SDN controllers. It made the blockchain appropriate for resource-constrained IoT devices. According to the empirical findings, the cluster structure-based routing protocol had a greater throughput, lower latency, and less energy than SMSN, EESCFD, AOMDV, AODV, and DSDV routing protocols. In other words, it has been shown that the suggested design performed better than traditional blockchain.

Hakiri, Sellami [49] introduced a brand-new IoT network structure depending on blockchain that made use of SDN and NFV to secure IoT transactions. They created an intrusion detection system that enhanced IoT networks' scalability and performance through virtualized network functions. They demonstrated how DAO (Decentralized Autonomous Organization) induction assaults might be stopped in dispersed IoT networks using the architecture of the IoT-focused smart contract. They presented a revolutionary POW consensus mechanism to identify and report problematic IoT nodes and reduce malicious traffic. The method enforced trust in the IoT-on-the-blockchain network and improved flexibility, scalability, robustness, agility, and dynamic resource management. Furthermore, minimizing deep packet inspection of SDN-enabled IoT traffic increased openness and performance and allowed new kinds of trust-less interactions to enhance IoT communications.

Abdulqadder, Zhou [48] introduced a blockchain-based attack detection and mitigation model in 5G-IoT networks with SDN/network function virtualization enabled. The five planes that made up this model are the control plane, the application plane, the data plane, the blockchain plane, and the 5G infrastructure plane. The 5G user had to first authenticate with the blockchain server. Following authentication, the user's flow was processed by choosing the best virtual network function. The flow rules were installed by the controller in the virtual network functions and were then hashed and saved in blocks using Blake 256. Attacks, including port scanning and overloading of flow tables, were successfully identified and neutralized in this way. False flow rules were also dropped upon arrival. The Bloc-Sec model was evaluated and contrasted with earlier research, specifically "VARMAN," to provide superior performance metrics. Compared to VARMAN, the Bloc-Sec method secures a reduced packet loss rate. The packet loss rate decreased as the number of switches increased.

Hakiri and Dezfouli [50] presented a cutting-edge blockchain-based framework that used NFV and SDN to secure IoT transactions. To increase the performance and scalability of IoT networks, a revolutionary security appliance was designed in the form of virtualized network services. Next, in order to identify and report problematic IoT nodes and reduce malicious traffic, they created a unique consensus mechanism. Three well-known consensus techniques, namely proof of elapsed time, proof of work, and proof of stake, were analyzed and compared to the suggested approach. They revealed that the suggested method offered much faster throughput, lower latency, and reliable IoT connection.

ABBASSI and Benlahmer [51] suggested blockchain SDN-IoT, a new distributed secure IoT network layout founded on an SDN backbone, employing blockchain technology to handle present and future issues and meet new service needs. This design was developed in response to an investigation of the difficulties large-scale IoT networks encountered as a result of new communication paradigms. A system's capacity and performance were enhanced through blockchain SDN-IoT. The blockchain SDN-IoT model's major function was to produce and implement defenses, such as data protection, threat prevention, and access control and to mitigate network assaults such as Denial of Service (DoS) attacks, cache poisoning/ARP spoofing, and identify security threats. By enabling IoT forwarding devices to verify and download the most recent flow rule table as required, the blockchain SDN-IoT strategy also aimed to reduce the amount of time an attack window may be open. The suggested model's scalability, defensive effects, accuracy rates, and performance overhead were used to evaluate its performance.

The integration of SDN and blockchain improves the performance of blockchain in IoT and solves some of the challenges. Reducing the delay and security of transactions and reducing attacks are among them. Table 5 reveals the results clearly.

**Table 5.** A summary of SDN-based architecture case studies.

| Ref No. | Case Study | Technique | Achievement | Tools |
|---|---|---|---|---|
| [47] | ▪ Lack of security<br>▪ Lack of energy | ▪ Cluster structure with a new routing protocol | ▪ High throughput<br>▪ Low delay<br>▪ Low energy consumption | ▪ Simulation |
| [49] | ▪ Lack of security | ▪ Blockchain SDN-NFV architecture | ▪ Mitigating malicious traffic<br>▪ High scalability<br>▪ High flexibility<br>▪ High agility<br>▪ High resiliency<br>▪ Improving dynamic resource management | ▪ Implemented |
| [48] | ▪ Lack of security | ▪ Blockchain SDN-NFV architecture | ▪ Low the packet loss rate<br>▪ Mitigating port scanning attacks | ▪ Simulation |
| [50] | ▪ Lack of security<br>▪ Lack of privacy | ▪ Blockchain SDN-IoT architecture | ▪ Low latency<br>▪ High throughput<br>▪ High trust | ▪ Implemented |
| [51] | ▪ Lack of IoT security | ▪ Blockchain SDN-IoT architecture | ▪ Improving scalability<br>▪ Improving defense effects<br>▪ Improving accuracy rates<br>▪ Improving performance overhead | ▪ Simulation |

### 2.2.3. Edge/Fog-Based Architecture

The present technological breakthrough trend across a wide range of potential fields provides a strong basis for accomplishing the industry's objective [64–66]. Blockchain and IoT systems can manage major data security, integrity, and privacy problems. For added data, blockchain offers a crucial degree of protection [67]. In order to facilitate the implementation of different latency-sensitive and computationally intensive IoT applications, great emphasis has recently been placed on combining Fog, Edge, and Cloud infrastructures. Although some real-world frameworks make an effort to facilitate such integration, they have limits in terms of platform independence, security, resource management, and execution of multiple applications [58]. These studies covered possible privacy and security issues with fog-enabled IoT systems.

Cho, Wu [52] suggested a wireless rechargeable sensor network to improve the network's lifespan. A self-propelled vehicle was paired with a charger to provide a more adaptable charger deployment. The traveling salesman issue was defined and translated into the dynamic charger path selection issue. It was possible to get a greater fitness value across the charging path and the number of dead devices by designing four metaheuristic algorithms for IoT applications. Nevertheless, metaheuristic techniques may spend more time looking for answers, causing several IoT devices to use excessive amounts of their allotted power and go for extended periods without being recharged, which causes power fatigue. The edge computing method was also used to quicken the acquisition of charging pathways with the well-specified edge/centralized unit switching. Additionally, blockchain technology was used to ensure the estimated path is reliable and cannot be altered. The suggested design transmits data about charging pathways in the cloud and edge while maintaining high-level information believability. The simulation findings demonstrated that the suggested strategy might lead to both lower deployment costs and greater charging efficiency.

Kumar, Harjula [53] combined two of these cutting-edge technologies—Blockchain and Edge—to meet the prerequisites for IIoT applications. Low latency services, distributed trust, security, and process tracking and monitoring are a few of these IIoT requirements. Moreover, they put up a blockchain- and edge-based framework and extended it with a pertinent IIoT use case. They ran simulations using iFogSim to evaluate the performance of the suggested framework, and they compared the outcomes to the IIoT framework without blockchain capabilities. The findings show that BlockEdge has proven that decentralized trust and security management is feasible in an IIoT setting without sacrificing system performance or resource efficiency.

Mayer, Rodrigues [54] put out the FogChain architectural model for the healthcare industry, which blends blockchain, IoT, and fog computing technologies. Their primary contribution was the FogChain model, which used a different method to overcome IoT limitations by adding an intermediary fog layer close to the edge to increase their resources and capabilities. According to tests, FogChain could respond 62.6% quicker than blockchain systems that resembled the cloud. The evaluation's findings support the model's ability to accomplish its objectives, while maintaining application performance.

Pavithran, Al-Karaki [55] suggested a blockchain framework for IoT that protects privacy by leveraging hierarchical identity-based encryption (HIBE). The suggested design utilized the edge and cloudlet computing paradigms along with HIBE to maintain privacy and works well with event-driven IoT devices. Additionally, a real-world example, traffic speed radars, was used to show the effectiveness of the suggested design. A theoretical study that considered the possibility of a malevolent adversary was used to examine and verify the security of the suggested architecture. The Contiki OS was used to carry out comprehensive tests that produced data on the system and network performance of the suggested design, which allowed for an evaluation of its performance.

Fetjah, Azbeg [56] discussed the design of a smart healthcare system allowing remote patient monitoring. Blockchain technology was used in the design to guarantee security and anonymity. AI and smart contracts were utilized for the data analysis. Three layers made up the architecture: a layer for smart medical devices, a layer for fog, and a layer for clouds. A detailed scenario based on a diabetic management system validated the suggested technique. The design was utilized to offer remote patient monitoring for diabetics. The system might provide recommendations for therapies, produce proactive forecasts, anticipate potential difficulties, and inform doctors in an emergency.

In this section, we considered the blockchain as an emerging security solution in the fog/edge-enabled IoT domain by analyzing some blockchain solutions in IoT systems. A summary of the reviewed architectures is given in Table 6. Table 6 summarizes the general points of fog/edge-based structures. As can be seen, these architectures have tried to improve latency, security, privacy, and response time.

**Table 6.** A summary of edge/fog-based architecture case studies.

| Ref No. | Case Study | Technique | Achievement | Tools |
|---|---|---|---|---|
| [52] | ▪ Low lifetime of the wireless sensor network | ▪ Blockchain-based edge architecture | ▪ Better charging efficiency<br>▪ Less deployment cost | ▪ Simulation |
| [53] | ▪ Lack of security<br>▪ Lack of trust | ▪ BlockEdge' framework | ▪ Low latency<br>▪ Improving power consumption<br>▪ Improving network usage | ▪ Simulation |
| [54] | ▪ Lack of security<br>▪ Lack of privacy | ▪ FogChain model | ▪ Improving response time | ▪ Implemented |
| [55] | ▪ Lack of privacy<br>▪ Lack of security | ▪ Blockchain architecture for IoT using HIBE | ▪ High privacy<br>▪ High security | ▪ Implemented |
| [56] | ▪ Lack of remote patient monitoring | ▪ An architecture based on IoT, Blockchain, and fog computing | ▪ Suggesting treatments<br>▪ Generating proactive predictions and predicting future complications<br>▪ Alerting physicians in case of emergency | ▪ Implemented |

### 2.2.4. Lightweight Architecture

Real-time applications will succeed due to a large part of the latency needs in blockchain-enabled smart cities. It will be necessary to develop lightweight blockchain techniques that can satisfy these varied latency needs when new heterogeneous latency-constrained applications proliferate on the future network. Hence, new mechanisms are needed in blockchain technology to satisfy the stated demand given by these smart city applications, establish quick consensus, and manage a large number of transactions [68].

Seok, Park [57] suggested a blockchain design that could dynamically adapt the blockchain's hash function in response to the volume of transactions, enhancing the network's availability. They chose three lightweight hash algorithms for this design that performed better in terms of implementation space, power consumption, and throughput. These hash algorithms could guarantee cryptographic security and took up little space on devices with limited resources to execute them. Using these hash algorithms, they then created a flexible hash chain connecting each data block. The computational load and delay could be decreased with this strategy. Additionally, they divided the field into some cells and assembled cell nodes to regulate each cell. This strategy could make the network more scalable. The simulation results showed that the suggested design was appropriate for an environment where data needed to be processed quickly, particularly in the realm of monitoring and supervision for IIoT applications. In addition, they claimed that the suggested structure could be used for a wider range of IIoT applications that demand latency under 1 s if the hash functions were executed in parallel or more lightweight hash functions were devised. Nevertheless, several IIoT applications, including closed-loop control fields, interlocking, and control fields, needed constrained latency (less than 500 ms).

Tuli, Mahmud [58] offered the FogBus framework, which enables complete IoT-Fog (Edge)-Cloud interaction. For the implementation and interaction of IoT applications and compute instances, FogBus provided platform-neutral interfaces. It helped programmers to create applications, consumers to run several programs simultaneously, and service suppliers to manage their resources. FogBus used blockchain, authentication, and encryption to further safeguard activities on sensitive data. It was simple to implement, scalable, and reasonably priced because of its cross-platform software platforms. They created a computer environment using FogBus that links finger pulse oximeters as IoT devices with a smartphone-based gateway and Raspberry Pi, demonstrating its usefulness. They used the deployment of an actual IoT application to assess the features of FogBus in comparison to other architectures already in use and the effects of different FogBus settings on system parameters. The trial outcomes demonstrated that FogBus was rather quick and responsive, and various FogBus settings might modify the computing environment depending on the needs of the circumstance.

Khalid, Asim [59] suggested a decentralized authentication and access control system that works in a variety of circumstances and is suitable for small IoT devices. The technique was built on the public blockchain concept and fog computing technologies. The trial findings showed that the suggested mechanism performed better when compared to a cutting-edge blockchain-based authentication system.

Alfrhan, Moulahi [60] looked at the deployment of portable blockchain technology, primarily to protect IoT networks. They chose various hashing methods to be used on a Raspberry Pi device since hashing was crucial to building a strong blockchain structure. Overall, the work offered a numerical analysis to assess the effectiveness of well-known hash algorithms that could be utilized in a low-power blockchain-based IoT. The experiment's findings complemented earlier research that had been emphasized in their work, showing that SHA-2 functions beat sponge-based hash functions in terms of hashing performance, followed by lightweight versions of Keccak with a high bitrate value. The results also supported the necessity of creating lighter, more efficient hash routines.

Bandara, Tosh [61] suggested "Tikiri," a minimal blockchain platform for IoT devices with few resources. Tikiri presented a novel blockchain architecture to support real-time transaction processing on the blockchain and utilized Apache Kafka for the consensus. Tikiri is known for its actor-based smart contract platform and functional programming, which enables parallel execution of blockchain transactions. Tikiri developed a scalable, lightweight blockchain that could operate well on IoT devices with limited resources.

Bouras, Lu [62] suggested a lightweight architecture and the accompanying protocols for consortium blockchain-based identity management to tackle security, privacy, and scalability concerns in a central system for IoT. Additionally, they tested the strategy and developed a proof-of-concept prototype. They assessed their work by testing the transactional latency and throughput, while employing various query actions and payload sizes and compared it to other similar studies. The outcomes demonstrated that the strategy was appropriate for commercial implementation.

As it is clear from the results, lightweight architectures reduce latency and improve performance. The detailed results of this section are given in Table 7. This table includes the features of the reviewed architectures.

**Table 7.** A summary of lightweight architecture case studies.

| Ref No. | Case Study | Technique | Achievement | Tools |
|---|---|---|---|---|
| [57] | ▪ Lack of cryptographic performance | ▪ Lightweight hash-based blockchain architecture | ▪ High security<br>▪ Low power consumption<br>▪ Low computational burden<br>▪ Low latency | ▪ Simulation |
| [58] | ▪ High latency | ▪ FogBus framework | ▪ High scalable<br>▪ Cost efficient | ▪ Implemented |
| [59] | ▪ Lack of security | ▪ Lightweight blockchain technology | ▪ Low latency<br>▪ High trust | ▪ Implemented |
| [60] | ▪ Lack of security | ▪ Lightweight blockchain technology | ▪ High speed | ▪ Implemented |
| [61] | ▪ Lack of security<br>▪ Lack of privacy | ▪ Lightweight blockchain platform | ▪ High Lightweight<br>▪ High scalable<br>▪ High transaction throughput | ▪ Implemented |
| [62] | ▪ Lack of security<br>▪ Lack of privacy | ▪ Lightweight architecture<br>▪ Associated protocols | ▪ High scalability<br>▪ High security | ▪ Implemented |

Before being put into use, suggested Blockchain-based IoT systems need to be protected from several privacy risks.

### 2.3. Bibliometric Maps

A total of 1072 papers from the Scopus database were eventually retrieved and cleaned for bibliometric analysis based on the search technique and the mentioned criteria. In order to conduct the bibliometric analysis, publications discovered in the databases used for this research were also examined—this analysis allowed for creating a profile of scientific products and examining trends and theme areas.

#### 2.3.1. Distribution Based on Journal

Figure 3 includes journals, such as IEEE Internet of Things Journal, IEEE Access, IEEE Transactions on Industrial Informatics, etc., and the number of printed articles. Most of the journals were related to computer engineering and communication technology. Meanwhile, the contribution of each of the magazines from the total results is given in Table 8.

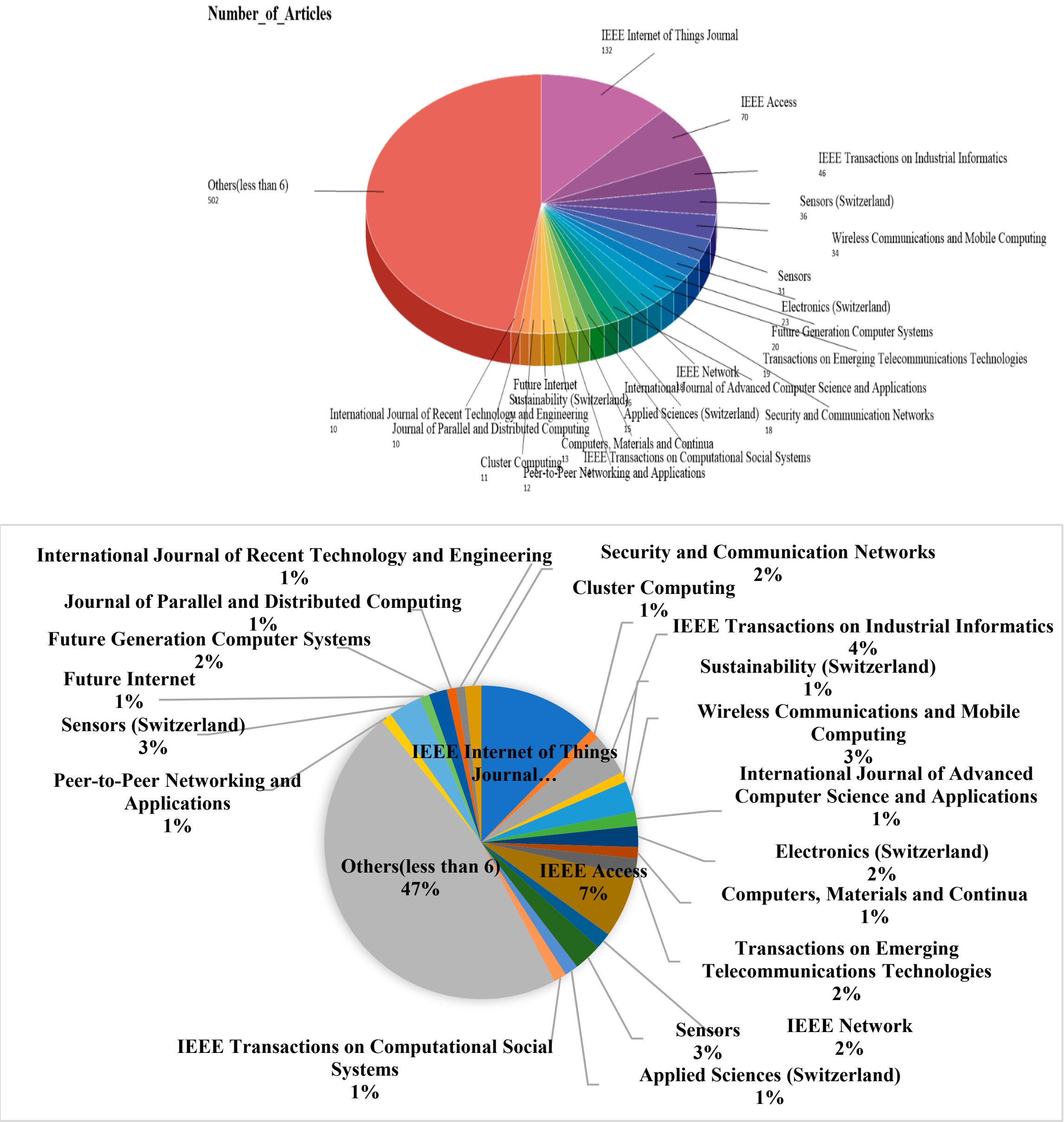

**Figure 3.** Distribution based on the type of source.

The IEEE Internet of Things Journal has the largest share (12.3%). Other magazines have contributed less than 7% of these participants. IEEE Access accounted for 6.5% of the total. It is interesting to know that the total contribution of journals that had less than 9 articles is a total of 502 articles. The results of citations and the contribution of journals are provided in Table 8. In this figure, the names of magazines that had 10 documents or above are mentioned.

**Table 8.** Analysis of articles published by the journal.

| Journal Name | Number of Articles | Percentage | Citation (Total Cited) |
|---|---|---|---|
| IEEE Internet of Things Journal | 132 | 12.3% | 3968 |
| IEEE Access | 70 | 6.5% | 2833 |
| IEEE Transactions on Industrial Informatics | 46 | 4.2% | 2807 |
| Sensors Switzerland | 36 | 3.3% | 1603 |
| Wireless Communications and Mobile Computing | 34 | 3.1% | 210 |
| Sensors | 31 | 2.8% | 166 |
| Electronics Switzerland | 23 | 2.1% | 232 |
| Future Generation Computer Systems | 20 | 1.8% | 2779 |
| Transactions on Emerging Telecommunications Technologies | 19 | 1.7% | 221 |
| Security and Communication Networks | 18 | 1.6% | 633 |
| IEEE Network | 18 | 1.6% | 759 |
| International Journal of Advanced Computer Science and Applications | 16 | 1.4% | 96 |
| Applied Sciences Switzerland | 15 | 1.3% | 212 |
| IEEE Transactions on Computational Social Systems | 14 | 1.3% | 497 |
| Computers Materials and Continua | 13 | 1.2% | 91 |
| P2P Networking and Applications | 12 | 1.1% | 144 |
| Sustainability Switzerland | 11 | 1.0% | 144 |
| Future Internet | 11 | 1.0% | 183 |
| Cluster Computing | 11 | 1.0% | 232 |
| Journal of Parallel and Distributed Computing | 10 | 0.9% | 269 |
| International Journal of Recent Technology and Engineering | 10 | 0.9% | 44 |

### 2.3.2. Distribution Based on the Country

Figure 4 demonstrates the countries with the most articles. China ranks first with a total of 400 publications, more than 37% of the total documents. It is followed by India (17.7%) and the US (11.6%). Countries such as Slovakia, Indonesia, and Latvia are in the lowest ranks.

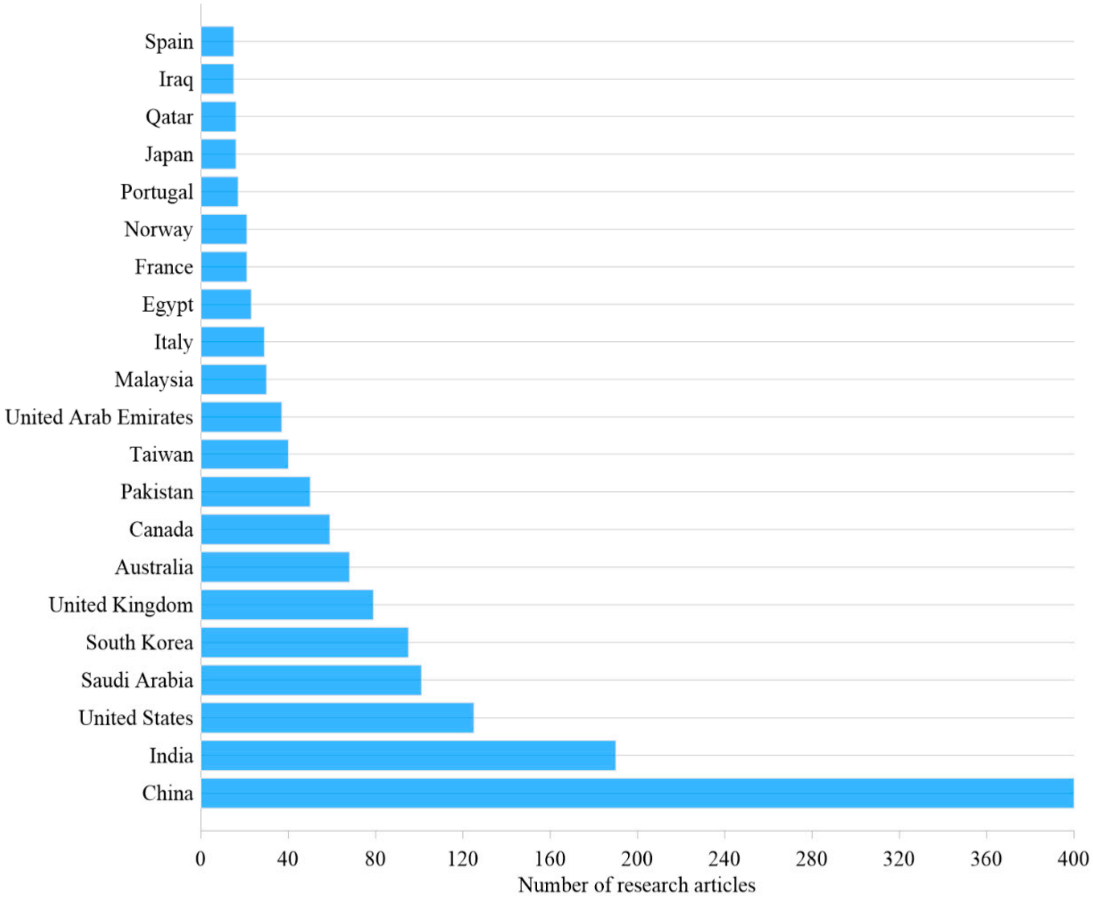

**Figure 4.** Distribution based on the country of publication.

### 2.3.3. Bibliometric Analysis of Included Studies

The gathered articles had a total of 2035 keywords, which were counted and classified based on their co-occurrences in order to authenticate the research's intended audience. The co-occurrences of each term across all publications were then set to a threshold. Let's say k is a threshold and k $\geq$ 7. Out of the 2035 keywords that satisfied the requirement, 121 were subsequently acquired. It means that every one of these 82 keywords appeared at least 7 times in all the articles gathered. The relationships across these 121 keywords are shown in Figure 5.

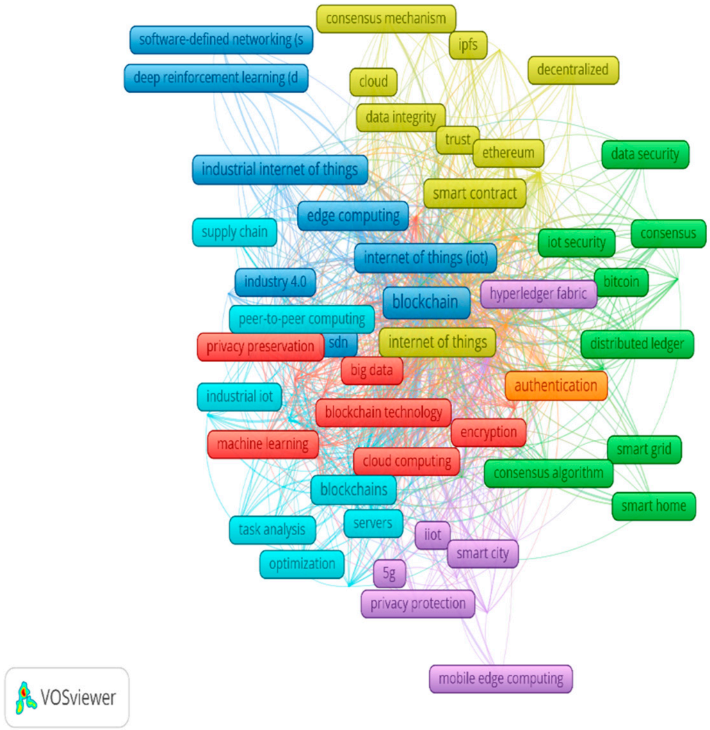

**Figure 5.** Bibliometric map created based on author keywords co-occurrence using network visualization of VOSviewer.

Using cluster analysis, high-frequency keywords that are closely connected may be linked to create different classes and reveal the organization of pertinent study area themes. At the threshold of 7, all high-frequency keywords could be separated into 7 clusters, and it also became able to make an initial assumption about the degree of link across the high-frequency terms.

The 1st cluster was designated 'Linking blockchain-IoT with AI' as it included the following keywords: 'Big data', 'Deep learning' and 'Machine learning (ML)'.

The 2nd cluster was named 'Scalability in blockchain' as it contained three keywords: 'Scalability', 'Decentralization' and 'Smart cities.

The 3rd cluster was entitled 'Linking blockchain with software-defined IoT since it contained the following keywords: 'SDN', 'Fog computing' and 'Software-defined'.

The 4th cluster became 'Trust in blockchain'; it included as keywords: 'Access control', 'Smart contract' and 'Trust'.

The 5th cluster received the denomination 'Reliable data sharing in blockchain' as it included the two keywords 'Data sharing' and 'Hyperledger fabric' and 'Smart city'.

The 6th cluster received the name 'Blockchain for the IIoT' because it included two keywords 'Servers' 'Industrial internet of things' and 'Supply chain'.

The 7th cluster was named 'Blockchain authentication' because it included the words 'Security', 'Authentication', and 'Privacy'.

The frequency and link quality of the 82 total keywords that fulfill the criterion are presented in Table 9. The most frequent term is "Security," which appears 185 times in gathered papers and 57 times with other keywords, followed by "Blockchain" and "IoT." In addition to other terms, "Security" appeared 69 times, while "Privacy" appeared 56 times. Therefore, the keywords with the highest scores experimentally support the accuracy of the search terms used to gather literature papers. Additionally, the fact that IoT and Blockchain have the largest circle sizes and the densest connections among them shows that the study focuses on those topics.

**Table 9.** Keywords occurrence.

| Keywords | Occurrences | Total Link Strength | Keywords | Occurrences | Total Link Strength | Keywords | Occurrences | Total Link Strength |
|---|---|---|---|---|---|---|---|---|
| AI | 15 | 58 | Deep reinforcement learning (DRL) | 7 | 16 | IIoT | 10 | 29 |
| Big data | 15 | 64 | Edge computing | 55 | 194 | IoT | 220 | 572 |
| Blockchain technology | 36 | 77 | Energy efficiency | 8 | 21 | Mobile edge computing | 8 | 18 |
| Cloud computing | 31 | 144 | Fog computing | 40 | 162 | Permissioned blockchain | 8 | 21 |
| Cryptography | 16 | 75 | Industrial IoT | 41 | 91 | Privacy protection | 9 | 31 |
| Data models | 9 | 62 | Industry 4.0 | 18 | 63 | Smart city | 17 | 52 |
| Data privacy | 12 | 55 | IoT | 152 | 355 | Blockchains | 72 | 379 |
| Deep learning | 10 | 33 | Performance evaluation | 7 | 24 | Computational modeling | 7 | 48 |
| Encryption | 9 | 45 | SDN | 8 | 35 | Computer architecture | 8 | 37 |
| Federated learning | 15 | 71 | Security and privacy | 12 | 31 | Industrial IoT | 27 | 101 |
| Healthcare | 21 | 97 | Software-defined-networking (SDN) | 7 | 15 | Industrial IoT | 12 | 39 |
| IoT | 11 | 45 | Access control | 57 | 182 | Optimization | 8 | 32 |
| ML | 17 | 61 | Cloud | 10 | 35 | P2P computing | 10 | 56 |
| Privacy preservation | 10 | 30 | Consensus mechanism | 11 | 29 | Resource management | 7 | 36 |
| Privacy-preserving | 13 | 54 | Consortium blockchain | 10 | 14 | Sensors | 10 | 39 |
| Bitcoin | 12 | 46 | Data integrity | 9 | 29 | Servers | 22 | 140 |
| Consensus | 24 | 59 | Decentralized | 7 | 24 | Supply chain | 17 | 44 |
| Consensus algorithm | 11 | 35 | Ethereum | 22 | 75 | Task analysis | 8 | 41 |

**Table 9.** *Cont.*

| Keywords | Occurrences | Total Link Strength | Keywords | Occurrences | Total Link Strength | Keywords | Occurrences | Total Link Strength |
|---|---|---|---|---|---|---|---|---|
| Data security | 7 | 17 | Identity management | 7 | 26 | Authentication | 54 | 183 |
| Decentralization | 14 | 46 | IoT | 325 | 926 | Authorization | 8 | 34 |
| Distributed ledger | 13 | 42 | IPFS | 7 | 32 | Privacy | 71 | 293 |
| Distributed systems | 7 | 28 | Smart contract | 81 | 244 | Security | 185 | 678 |
| IoT security | 16 | 35 | Trust | 22 | 77 | Smart contracts | 41 | 159 |
| Scalability | 26 | 95 | 5G | 8 | 32 | Trust management | 13 | 57 |
| Smart cities | 15 | 55 | COVID-19 | 8 | 30 | | | |
| Smart grid | 7 | 17 | Cybersecurity | 11 | 34 | | | |
| Smart home | 8 | 24 | Data sharing | 22 | 69 | | | |
| Throughput | 7 | 39 | Deep information learning | 7 | 16 | | | |
| Blockchain | 753 | 1842 | Hyperledger fabric | 23 | 75 | | | |

## 3. Results and Analysis

The key constraints, difficulties, possibilities, and prospects mentioned in the literature were discussed using theme maps produced by bibliometric analysis, which were developed to serve as a conversation guide.

### 3.1. Blockchain as a Solution for Securing IoT Big Data Analytics Using AI

Through ML-based data analytics, big data optimizes intricate supply networks [69,70]. Nevertheless, there are drawbacks to data analytics, including a loss of privacy and control that increases the danger of data breaches. A method in the field of ML called Federated Learning (FL) offers distributed model training while protecting privacy [71,72].

Numerous AI applications can benefit from blockchain technology's capacity to ensure data accuracy when feeding data into AI systems and documenting findings from them [73]. As seen by the way that bots are quickly taking over the web, AI or ML, which have been around for a few decades, are now again fashionable. In practically every sector of the economy today, including financial and banking services, transportation, healthcare, and the military, AI is becoming increasingly relevant and inseparable from daily life activities [24].

### 3.2. Scalability Problem in IoT-Blockchain

Substantial attempts have been undertaken to address blockchain's scalability concerns in order to adapt this exciting technology for integrating diverse IoT devices. Lately, concepts and methods for linking heterogeneous IoT devices have drawn much interest from industry and academia [74].

Blockchain scalability concerns might result in centralization, which is a concern for the cryptocurrency's future. The blockchain does not scale well as the number of nodes increases. Given that numerous nodes are expected to be present in IoT networks, this is a significant issue [75].

Scalability has often been identified as a problem that requires quick, effective answers in recent works. Some literary works just made references to some already chosen miners. Nevertheless, in these instances, the architecture resembles any centralized system more. Other studies have found inefficiencies in network performance (such as fewer transactions per second when more devices are being added). Hence, further study is needed to achieve scalability with trustworthy connectivity without compromising performance.

### *3.3. Blockchain as a Solution for Securing the Software-Defined IoT*

Bringing IoT components out of the cloud and onto edge servers decreases latency by lowering overall network traffic [76]. Nevertheless, additional system maintenance and design issues arise when IoT services are provisioned on IoT edge devices. Utilizing software-defined IoT components in the form of virtual resources is one strategy that is conceivable [77]. On SDN-based IoT setups, the blockchain may be used for security provisioning. However, there were certain issues, such as sluggish processing and poor assault detection [68]. Blockchain can serve as a trusted third party and "out-of-band" party for the distributed SDIIoT to gather and synchronize network-wide views (such as network topology, network events, OpenFlow instructions, etc.) amongst many SDN controllers in a traceable, dependable, and safe manner [78,79]. The design of a software-defined and virtualized blockchain in the IoT is still unresolved [80].

### *3.4. Smart Contract IoT Blockchain to Trust*

Scripts for smart contracts are kept on the blockchain. They are adaptable, which is why they are so strong. They can securely encrypt and store data, limit access to that data to the required parties and then be programmed to use it as part of a self-executing logical workflow of actions among parties. Smart contracts convert company operations into computational operations, considerably enhancing operational efficiency [81]. The use of smart contracts in IoT will offer a method for enhancing the security and integrity of IoT data [75]. We can completely automate the procedure while building complete confidence among all of these stakeholders using smart contracts, blockchain, and IoT devices [82].

### *3.5. Secure Data Sharing through Blockchain*

In IoT, data is essential. The vast majority of IoT systems in use today rely on centralized cloud-based data exchange services. Trust from the sensor owner and the user of the sensor data is also necessary for the participation of such a third-party service supplier. Additionally, payment is required for their services [83]. Reaching shared understanding through trustworthy data sharing across trusted stakeholders is the key to extensive collaboration in IoT [84]. A possible method for enabling safe and intelligent data exchange in the IIoT is the combination of blockchain with federated learning [85].

### *3.6. Privacy and Trust Using Blockchain in IIoT*

Because of its decentralized and transparent character, the usage of blockchain technology in IIoT systems is becoming more popular [86]. For instance, IIoT sensors installed in a manufacturing facility might operate more effectively in a decentralized setting. It is due to the decentralized ledger being updated after each step and information being sent to every other IIoT blockchain node. Because of the decentralized update phenomena, every sensor will be aware of the devices around it, reducing the likelihood of failure and harm. Nevertheless, decentralization will decrease the likelihood of failure, but this development increases computational overhead for each sensor node. Therefore, for such decentralized systems, lightweight blockchain-based IIoT protocols are needed. As a result of its high processing cost, integrating encryption privacy protection with blockchain-based IIoT systems is quite difficult [87,88]. Thus, research is needed to create simple encryption methods that nevertheless protect privacy.

### *3.7. Blockchain Technology for IoT Authentication*

Device identification is one of the hardest parts of any IoT application. IoT devices can exchange and process data without requiring human interaction. These entities must successfully authenticate and identify one another due to their absolute authority. The IoT devices may become vulnerable to various attacks, including DDoS and replay attacks, if they are not properly authenticated. Due to IoT's scale and other properties, it is almost impossible to design an efficient authentication mechanism. Despite the fact that this issue has received a lot of attention, most of the solutions depend on a centralized system [89]. The goal of blockchain is to create a data format to build a distributed record of transactions that is impenetrable to outside interference [90].

## **4. Industry and Use of Blockchain Technology**

This section discusses various applications using blockchain and IoT, which have been reviewed in the literature. Blockchain helps in security and privacy in various industries such as electricity, water, gas, food, etc. Several items are mentioned below.

Leelasantitham [91] demonstrated that Thailand's single-buyer business model for electricity is improved. Thailand's electricity-producing authority is in charge of generating power and distributing it to consumers (2%), metropolitan electricity authorities (30%), and province electricity authorities (68%). Residential and industrial power consumers will get distribution and retail electricity services from the province and metropolitan electrical authorities. The free power trading market, though, is anticipated to launch soon. Through disruptive technologies, such as blockchain and cryptocurrency, it is required to plan for and support the adjustment, change, or modification. Future power business models should be in accordance with the government's objective to accelerate technological advancement and innovation in Thailand 4.0. Hence, research of the business model guidelines for blockchain-based power utility systems in Thailand revealed that the prospective business model for selling electricity will probably involve a decentralized P2P trading platform. The initial anticipated effects of the costing analysis are compared to the current power trading system and the blockchain technology system to provide a summary. The outcomes of these initially anticipated effects have demonstrated that, in the future, the costs associated with using blockchain technology for users, prosumers, and small and medium-sized businesses may be less than those associated with Thailand's provincial electricity authority, electricity generating authority, and metropolitan electricity authority [92]. Buyers may select their vendors where the data is transparent and the information is reliable. Additionally, there is cryptocurrency, a crucial tool for trades and transactions. Trading energy with cryptocurrencies is a cutting-edge method that has been utilized for a long time [93]. Blockchain-based electricity trading is projected to gain popularity, notably in the United States [94]. LO3 Energy, a provider of micro-grid networks, now oversees the Brooklyn Micro Grid [95].

To comply with the halal requirement, particularly in the food supply chain, government entities under the religious affairs ministry are entrusted with regulating and maintaining the application of sharia law in Indonesia. Any food ingested by Muslims must adhere to the rules and customs of Islamic law to be considered halal. The improvement of Indonesia's halal value chain and digital economy is one of the strategic initiatives to accomplish the aim. The halal hubs in each district or province, halal certification, and an integrated halal traceability system are among the initiatives that support it. An established program is currently a halal certification. Even small and medium-sized businesses in Indonesia now have access to halal certification, which guarantees that the items sold there are halal. Currently, the three halal agencies mandate that firms place halal emblems on their products, therefore providing a halal guarantee. Customers may also verify the status of halal products on the official MUI website. The present mechanism, however, has some shortcomings [96]. Additionally, creating a shared or distributed database that can be verified, secure, transparent, and used to hold halal supply chain information is crucial [97]. They come together with Indonesia's goal of dominating the worldwide halal market and the problem with the present framework. The need for a traceability system is urged by the necessity of preventing foodborne illness. Although the objective is to prevent the consumption of haram items, barcode technology alone cannot provide real-time assurance. Blockchain is a modern technology that can keep up with demands. Blockchain is a part of the top technology in the digital economy, especially following trends for huge personalization, along with AI [98,99].

In [100], B-Spot, a durable and secure photo transfer technique based on blockchain and steganography, is suggested. At the sender side, a secret photo is initially concealed in a cover photo using a 3-3-2 least significant bit image steganography technique. Consequently, the secret photo's existence is kept a secret. After that, blocks are created from blocks of pixels that make up the Steg picture. A blockchain is created by connecting blocks using their hash values. The fracture of the chain serves as a reflection of any block alterations, making the system tamper-evident. For the second recovery procedure, a hash table contains a duplicate of the blockchain. Any network may be used to send data between the blockchain and the hash table. Once it gets the data, the receiver initially carries out the verification procedure to ensure the blockchain's integrity. The process is made more resistant to noises by recovering the lost and altered blocks using the hash table. Ultimately, using the retrieved blockchain, the stego-image is rebuilt. The receiver can then obtain the secret photo after the extraction procedure. According to the simulation findings, the suggested mechanism has a large data capacity, improved imperceptibility, a manageable processing time, and great noise resilience. This approach strengthens the existing systems and gives an additional degree of protection.

## 5. Open Issue and Future Trends

This section presents several significant concerns that have not yet been completely and deeply investigated.

- Although they provide a strong method for IoT security, blockchain systems are still susceptible. As a result of the disappearance of the hash power-based consensus mechanism, attackers are now able to host the blockchain. Similar to attackers being able to use private keys with low randomness to breach blockchain accounts, users must create effective strategies for safeguarding transaction privacy and avoiding competitive attacks that might lead to double-dipping during transactions [101];
- Investigators have not yet addressed several problems and difficulties, such as IoT devices' limitations, massive data analysis, and other previously identified difficulties with integrating IoT blockchain;
- Some challenging research problems include deep learning, ML techniques, datasets for intrusion detection, scalability evaluations of blockchain-based solutions, how to select the best consensus algorithm, such as memetic algorithms, and the creation of practical and interoperable cryptographic protocols [102]. They need to be looked at more thoroughly soon [103,104];
- Providing a scalability study of blockchain-based solutions for IoT-based agriculture is one of the difficulties that needs more focus in the future;
- Future research will concentrate on improving IoT transactions to make them more suited for in-blockchain big data analytics, utilizing sophisticated Graph Neural Networks (GNN) [105,106]. These improvements will include making IoT transactions more organized, plentiful, and complete from beginning to end;
- Although IIoT-based blockchain and fog computing take advantage of both technologies' benefits, several issues still need to be researched further to identify new opportunities. One issue is the creation of algorithms and infrastructures appropriate for such highly innovative automatic platforms [67];
- Although several strategies exist to reduce energy usage in blockchain-based systems [107], they are still ineffective when compared to the performances offered by lower-end devices [108]. The system's overall energy utilization is directly impacted when using high-processing blockchain nodes to improve the robustness of IoT instal-

lations [109,110]. If a small number of blockchain nodes are utilized, and a mining method with a lower difficulty level is chosen, it may be kept at manageable levels. Moreover, it is necessary to minimize computational costs while utilizing various cryptosystems [111,112].

## 6. Conclusions

IoT devices are now vulnerable and unable to defend themselves. Because IoT devices have limited resources, there are no security software and hardware design, development, or deployment practices, and standards have not been developed. The variety of IoT resources is also impeding efforts to define a strong worldwide strategy for protecting IoT layers. It is anticipated that blockchain will transform IoT. The problems outlined in this research should be taken into consideration when integrating these two technologies. IoT and blockchain integration offers several benefits that should be carefully addressed. This paper examines the key challenges that blockchain and IoT must overcome to work effectively together. In order to achieve the enormous expectations for the technology to revolutionize several facets of society and the economy, IoT security and privacy are essential success elements. Most security and privacy issues are addressed by the suggested blockchain-based IoT designs, which also consider several IoT devices' resource limitations. Blockchain technology is difficult since it also has significant drawbacks. The ledger storage facility's limitations, restricted technological advancements, a skilled labor shortage, a lack of appropriate legal rules and standards, variances in processing times and speeds, computer power limitations, and scalability constraints are a few of these difficulties. Therefore, the objective is to improve blockchain operations so that efficiency and security are properly aligned. Despite these difficulties, multi-stakeholder application settings, where privacy, security, and trust are concerned, might greatly benefit from using blockchain technologies. The study's contribution is the use of blockchain techniques to analyze and categorize works of literature about IoT. This investigation examined the structure of IoT applications and mapped the functional building blocks of blockchain technology to focus on the architectural challenges related to deploying blockchain for the IoT. According to this paper's taxonomy, most of the gathered articles concentrated more on offering security. Investigators who worked in this area acknowledged their concerns and proposed solutions to address existing and future obstacles. Besides the storage capacity and scalability that affect both technologies, investigations must be initiated to assure the security and privacy of critical technologies that the IoT and blockchain can become. The study was finished by stating and emphasizing a few difficulties and potential avenues for future research in blockchain-based IoT systems.

**Author Contributions:** Conceptualization, M.D., H.M.R.A.-K., S.H.H.N. and N.J.N.; methodology, M.D., H.M.R.A.-K., S.H.H.N., A.Q.M.A. and N.J.N.; software, M.D., H.M.R.A.-K., S.H.H.N. and N.J.N.; validation, M.D., H.M.R.A.-K., S.H.H.N., B.Z.E. and N.J.N.; formal analysis, A.Q.M.A., B.Z.E. and N.J.N.; investigation, M.D., H.M.R.A.-K., S.H.H.N. and N.J.N.; resources, M.D., H.M.R.A.-K. and S.H.H.N.; data curation, A.Q.M.A. and B.Z.E.; writing—original draft preparation, M.D., H.M.R.A.-K. and S.H.H.N.; writing—review and editing, A.Q.M.A., B.Z.E. and N.J.N.; visualization, M.D., H.M.R.A.-K., S.H.H.N. and N.J.N.; supervision, N.J.N.; project administration, M.D. and N.J.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** There is no funding.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** All data are reported in this paper.

**Conflicts of Interest:** There is no conflicts of interest.

## References

1. Peng, S.-L.; Pal, S.; Huang, L. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*; Springer: Berlin/Heidelberg, Germany, 2020.
2. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
3. Li, A.; Spano, D.; Krivochiza, J.; Domouchtsidis, S.; Tsinos, C.G.; Masouros, C.; Chatzinotas, S.; Li, Y.; Vucetic, B.; Ottersten, B. A tutorial on interference exploitation via symbol-level precoding: Overview, state-of-the-art and future directions. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 796–839. [CrossRef]
4. Tseng, L.; Yao, X.; Otoum, S.; Aloqaily, M.; Jararweh, Y. Blockchain-based database in an IoT environment: Challenges, opportunities, and analysis. *Clust. Comput.* **2020**, *23*, 2151–2165. [CrossRef]
5. Naen, M.F.; Adnan, M.H.M.; Yazi, N.A.; Nee, C.K. Development of Attendance Monitoring System with Artificial Intelligence Optimization in Cloud. *Int. J. Artif. Intell.* **2021**, *8*, 88–98. [CrossRef]
6. Zheng, W.; Yin, L.; Chen, X.; Ma, Z.; Liu, S.; Yang, B. Knowledge base graph embedding module design for Visual question answering model. *Pattern Recognit.* **2021**, *120*, 108153. [CrossRef]
7. Wu, H.; Jin, S.; Yue, W. Pricing Policy for a Dynamic Spectrum Allocation Scheme with Batch Requests and Impatient Packets in Cognitive Radio Networks. *J. Syst. Sci. Syst. Eng.* **2022**, *31*, 133–149. [CrossRef]
8. Ye, C.; Cao, W.; Chen, S. Security challenges of blockchain in Internet of things: Systematic literature review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4177. [CrossRef]
9. Ye, R.; Liu, P.; Shi, K.; Yan, B. State damping control: A novel simple method of rotor UAV with high performance. *IEEE Access* **2020**, *8*, 214346–214357. [CrossRef]
10. Mao, Y.; Zhu, Y.; Tang, Z.; Chen, Z. A Novel Airspace Planning Algorithm for Cooperative Target Localization. *Electronics* **2022**, *11*, 2950. [CrossRef]
11. Ma, K.; Hu, X.; Yue, Z.; Wang, Y.; Yang, J.; Zhao, H.; Liu, Z. Voltage Regulation With Electric Taxi Based on Dynamic Game Strategy. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2413–2426. [CrossRef]
12. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: Challenges and solutions. *arXiv* **2016**, arXiv:1608.05187.
13. Shahidi, S.; Vahdat, S.; Atapour, A.; Reisizadeh, S.; Soltaninejad, F.; Maghami-Mehr, A. The clinical course and risk factors in COVID-19 patients with acute kidney injury. *J. Fam. Med. Prim. Care* **2022**, *11*, 6183–6189.
14. Mohammadi, V.; Rahmani, A.M.; Darwesh, A.M.; Sahafi, A. Trust-based recommendation systems in Internet of Things: A systematic literature review. *Hum.-Cent. Comput. Inf. Sci.* **2019**, *9*, 1–61. [CrossRef]
15. Liu, K.; Yang, Z.; Wei, W.; Gao, B.; Xin, D.; Sun, C.; Gao, G.; Wu, G. Novel detection approach for thermal defects: Study on its feasibility and application to vehicle cables. *High Volt.* **2022**. [CrossRef]
16. Jain, S. Can Blockchain Accelerate Internet of Things (IoT) Adoption. Deloitte Switzer-Land. 2021. Available online: https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html (accessed on 20 October 2022).
17. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Barnawi, A.; Alzahrani, B.A. Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. *J. Netw. Comput. Appl.* **2020**, *157*, 102537. [CrossRef]
18. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
19. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
20. El-Masri, M.; Hussain, E.M.A. Blockchain as a mean to secure Internet of Things ecosystems—A systematic literature review. *J. Enterp. Inf. Manag.* **2021**. [CrossRef]
21. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
22. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1676–1717. [CrossRef]
23. Lee, B.; Lee, J.-H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *J. Supercomput.* **2017**, *73*, 1152–1167. [CrossRef]
24. Rabah, K. Convergence of AI, IoT, big data and blockchain: A review. *Lake Inst. J.* **2018**, *1*, 1–18.
25. Aljofey, A.; Rasool, A.; Jiang, Q.; Qu, Q. A Feature-Based Robust Method for Abnormal Contracts Detection in Ethereum Blockchain. *Electronics* **2022**, *11*, 2937. [CrossRef]
26. Fotohi, R.; Aliee, F.S. Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. *Comput. Netw.* **2021**, *197*, 108331. [CrossRef]
27. Kakarlapudi, P.V.; Mahmoud, Q.H. Design and Development of a Blockchain-Based System for Private Data Management. *Electronics* **2021**, *10*, 3131. [CrossRef]
28. Banafa, A. IoT and blockchain convergence: Benefits and challenges. *IEEE Internet Things* **2017**, *9*. Available online: https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html (accessed on 20 October 2022).

29. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain technology toward green IoT: Opportunities and challenges. *IEEE Netw.* **2020**, *34*, 263–269. [CrossRef]
30. Dwivedi, A.D.; Malina, L.; Dzurenda, P.; Srivastava, G. Optimized blockchain model for internet of things based healthcare applications. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 135–139.
31. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
32. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
33. Bhadoria, R.S.; Das, A.P.; Bashar, A.; Zikria, M. Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections. *Electronics* **2022**, *11*, 3359. [CrossRef]
34. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [CrossRef]
35. Doewes, R.I.; Gharibian, G.; zadeh, F.A.; Zaman, B.A.; vahdat, S.; Akhavan-Sigari, R. An updated systematic review on the effects of aerobic exercise on human blood lipid profile. *Curr. Probl. Cardiol.* **2022**, *in press*. [CrossRef]
36. Zadeh, F.A.; Bokov, D.O.; Yasin, G.; Vahdat, S.; Abbasalizad-Farhangi, M. Central obesity accelerates leukocyte telomere length (LTL) shortening in apparently healthy adults: A systematic review and meta-analysis. *Crit. Rev. Food Sci. Nutr.* **2021**, 1–10. [CrossRef]
37. Herrera-Franco, G.; Montalván-Burbano, N.; Carrión-Mero, P.; Jaya-Montalvo, M.; Gurumendi-Noriega, M. Worldwide research on geoparks through bibliometric analysis. *Sustainability* **2021**, *13*, 1175. [CrossRef]
38. Nobanee, H.; Al Hamadi, F.Y.; Abdulaziz, F.A.; Abukarsh, L.S.; Alqahtani, A.F.; AlSubaey, S.K.; Alqahtani, S.M.; Almansoori, H.A. A bibliometric analysis of sustainability and risk management. *Sustainability* **2021**, *13*, 3277. [CrossRef]
39. Quezada-Sarmiento, P.A.; Elorriaga, J.A.; Arruarte, A.; Washizaki, H. Open BOK on software engineering educational context: A systematic literature review. *Sustainability* **2020**, *12*, 6858. [CrossRef]
40. Esmailiyan, M.; Amerizadeh, A.; Vahdat, S.; Ghodsi, M.; Doewes, R.I.; Sundram, Y. Effect of different types of aerobic exercise on individuals with and without hypertension: An updated systematic review. *Curr. Probl. Cardiol.* **2021**, 101034. [CrossRef]
41. Vahdat, S.; Shahidi, S. D-dimer levels in chronic kidney illness: A comprehensive and systematic literature review. *Proc. Natl. Acad. Sci. India Sect. B Biol. Sci.* **2020**, *90*, 911–928. [CrossRef]
42. Vahdat, S. A review of pathophysiological mechanism, diagnosis, and treatment of thrombosis risk associated with COVID-19 infection. *IJC Heart Vasc.* **2022**, *41*, 101068. [CrossRef]
43. Li, Z.; Hao, J.; Liu, J.; Wang, H.; Xian, M. An IoT-applicable access control model under double-layer blockchain. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *68*, 2102–2106. [CrossRef]
44. Aldriwish, K. A double-blockchain architecture for secure storage and transaction on the Internet of Things networks. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 119–126.
45. Ren, W.; Wan, X.; Gan, P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. *Future Gener. Comput. Syst.* **2021**, *117*, 453–461. [CrossRef]
46. Hao, X.; Yeoh, P.L.; Ji, Z.; Yu, Y.; Vucetic, B.; Li, Y. Stochastic Analysis of Double Blockchain Architecture in IoT Communication Networks. *IEEE Internet Things J.* **2022**, 9700–9711. [CrossRef]
47. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.-K.R. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [CrossRef]
48. Abdulqadder, I.H.; Zhou, S.; Zou, D.; Aziz, I.T.; Akber, S.M.A. Bloc-sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT. In Proceedings of the 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020; pp. 499–507.
49. Hakiri, A.; Sellami, B.; Yahia, S.B.; Berthou, P. A Blockchain architecture for SDN-enabled tamper-resistant IoT networks. In Proceedings of the 2020 Global Information Infrastructure and Networking Symposium (GIIS), Tunis, Tunisia, 28–31 October 2020; pp. 1–4.
50. Hakiri, A.; Dezfouli, B. Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks. In Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security, New York, NY, USA, 28 April 2021; pp. 11–18.
51. ABBASSI, Y.; Benlahmer, H. BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain. *Int. J. Electr. Comput. Eng. Syst.* **2022**, *13*, 155–163. [CrossRef]
52. Cho, H.-H.; Wu, H.-T.; Lai, C.-F.; Shih, T.K.; Tseng, F.-H. Intelligent charging path planning for IoT network over Blockchain-based edge architecture. *IEEE Internet Things J.* **2020**, *8*, 2379–2394. [CrossRef]
53. Kumar, T.; Harjula, E.; Ejaz, M.; Manzoor, A.; Porambage, P.; Ahmad, I.; Liyanage, M.; Braeken, A.; Ylianttila, M. BlockEdge: Blockchain-edge framework for industrial IoT networks. *IEEE Access* **2020**, *8*, 154166–154185. [CrossRef]
54. Mayer, A.H.; Rodrigues, V.F.; da Costa, C.A.; da Rosa Righi, R.; Roehrs, A.; Antunes, R.S. Fogchain: A fog computing architecture integrating blockchain and Internet of things for personal health records. *IEEE Access* **2021**, *9*, 122723–122737. [CrossRef]

55. Pavithran, D.; Al-Karaki, J.N.; Shaalan, K. Edge-based blockchain architecture for event-driven IoT using hierarchical identity based encryption. *Inf. Process. Manag.* **2021**, *58*, 102528. [CrossRef]
56. Fetjah, L.; Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. Towards a Smart Healthcare System: An Architecture Based on IoT, Blockchain, and Fog Computing. *Int. J. Healthc. Inf. Syst. Inform.* **2021**, *16*, 1–18. [CrossRef]
57. Seok, B.; Park, J.; Park, J.H. A lightweight hash-based blockchain architecture for industrial IoT. *Appl. Sci.* **2019**, *9*, 3740. [CrossRef]
58. Tuli, S.; Mahmud, R.; Tuli, S.; Buyya, R. Fogbus: A blockchain-based lightweight framework for edge and fog computing. *J. Syst. Softw.* **2019**, *154*, 22–36. [CrossRef]
59. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.; Tariq, M.A.; Rafferty, L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust. Comput.* **2020**, *23*, 2067–2087. [CrossRef]
60. Alfrhan, A.; Moulahi, T.; Alabdulatif, A. Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT). *Blockchain Res. Appl.* **2021**, *2*, 100036. [CrossRef]
61. Bandara, E.; Tosh, D.; Foytik, P.; Shetty, S.; Ranasinghe, N.; De Zoysa, K. Tikiri—Towards a lightweight blockchain for IoT. *Future Gener. Comput. Syst.* **2021**, *119*, 154–165. [CrossRef]
62. Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A lightweight blockchain-based IoT identity management approach. *Future Internet* **2021**, *13*, 24. [CrossRef]
63. Hao, R.-B.; Lu, Z.-Q.; Ding, H.; Chen, L.-Q. A nonlinear vibration isolator supported on a flexible plate: Analysis and experiment. *Nonlinear Dyn.* **2022**, *108*, 941–958. [CrossRef]
64. Dai, B.; Zhang, B.; Niu, Z.; Feng, Y.; Liu, Y.; Fan, Y. A novel ultrawideband branch waveguide coupler with low amplitude imbalance. *IEEE Trans. Microw. Theory Tech.* **2022**, *70*, 3838–3846. [CrossRef]
65. Xi, Y.; Jiang, W.; Wei, K.; Hong, T.; Cheng, T.; Gong, S. Wideband RCS Reduction of Microstrip Antenna Array Using Coding Metasurface With Low Q Resonators and Fast Optimization Method. *IEEE Antennas Wirel. Propag. Lett.* **2021**, *21*, 656–660. [CrossRef]
66. Hong, T.; Guo, S.; Jiang, W.; Gong, S. Highly Selective Frequency Selective Surface With Ultrawideband Rejection. *IEEE Trans. Antennas Propag.* **2021**, *70*, 3459–3468. [CrossRef]
67. Bouachir, O.; Aloqaily, M.; Tseng, L.; Boukerche, A. Blockchain and fog computing for cyberphysical systems: The case of smart industry. *Computer* **2020**, *53*, 36–45. [CrossRef]
68. Pourvahab, M.; Ekbatanifard, G. An efficient forensics architecture in software-defined networking-IoT using blockchain technology. *IEEE Access* **2019**, *7*, 99573–99588. [CrossRef]
69. Feng, Y.; Zhang, B.; Liu, Y.; Niu, Z.; Fan, Y.; Chen, X. A D-band manifold triplexer with high isolation utilizing novel waveguide dual-mode filters. *IEEE Trans. Terahertz Sci. Technol.* **2022**. [CrossRef]
70. Zhang, J.; Zhu, C.; Zheng, L.; Xu, K. ROSEFusion: Random optimization for online dense reconstruction under fast camera motion. *ACM Trans. Graph.* **2021**, *40*, 1–17.
71. Unal, D.; Hammoudeh, M.; Khan, M.A.; Abuarqoub, A.; Epiphaniou, G.; Hamila, R. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. *Comput. Secur.* **2021**, *109*, 102393. [CrossRef]
72. Zhao, H.; Zhu, C.; Xu, X.; Huang, H.; Xu, K. Learning practically feasible policies for online 3D bin packing. *Sci. China Inf. Sci.* **2022**, *65*, 1–17. [CrossRef]
73. Luo, G.; Yuan, Q.; Li, J.; Wang, S.; Yang, F. Artificial intelligence powered mobile networks: From cognition to decision. *IEEE Netw.* **2022**, *36*, 136–144. [CrossRef]
74. Alrehaili, A.; Namoun, A.; Tufail, A. A Comparative Analysis of Scalability Issues within Blockchain-based Solutions in the Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 480–490. [CrossRef]
75. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G. Blockchain with internet of things: Benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [CrossRef]
76. Zheng, H.; Jin, S. A multi-source fluid queue based stochastic model of the probabilistic offloading strategy in a MEC system with multiple mobile devices and a single MEC server. *Int. J. Appl. Math. Comput. Sci.* **2022**, *32*, 125–138.
77. Samaniego, M.; Deters, R. Using blockchain to push software-defined IoT components onto edge hosts. In Proceedings of the International Conference on Big Data and Advanced Wireless Technologies, Blagoevgrad, Bulgaria, 10–11 November 2016; pp. 1–9.
78. Xu, K.-D.; Guo, Y.-J.; Liu, Y.; Deng, X.; Chen, Q.; Ma, Z. 60-GHz compact dual-mode on-chip bandpass filter using GaAs technology. *IEEE Electron Device Lett.* **2021**, *42*, 1120–1123. [CrossRef]
79. Xu, K.-D.; Weng, X.; Li, J.; Guo, Y.-J.; Wu, R.; Cui, J.; Chen, Q. 60-GHz third-order on-chip bandpass filter using GaAs pHEMT technology. *Semicond. Sci. Technol.* **2022**, *37*, 055004. [CrossRef]
80. Qiu, C.; Yu, F.R.; Yao, H.; Jiang, C.; Xu, F.; Zhao, C. Blockchain-based software-defined industrial Internet of Things: A dueling deep ${Q} $-learning approach. *IEEE Internet Things J.* **2018**, *6*, 4627–4639. [CrossRef]
81. Stanciu, A. Blockchain based distributed control system for edge computing. In Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017; pp. 667–671.
82. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.B. Blockchain and smart contract for IoT enabled smart agriculture. *PeerJ Comput. Sci.* **2021**, *7*, e407. [CrossRef] [PubMed]

83. Manzoor, A.; Liyanage, M.; Braeke, A.; Kanhere, S.S.; Ylianttila, M. Blockchain based proxy re-encryption scheme for secure IoT data sharing. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 99–103.
84. Shi, P.; Wang, H.; Yang, S.; Chen, C.; Yang, W. Blockchain-based trusted data sharing among trusted stakeholders in IoT. *Softw. Pract. Exp.* **2021**, *51*, 2051–2064. [CrossRef]
85. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
86. Miller, D. Blockchain and the internet of things in the industrial sector. *IT Prof.* **2018**, *20*, 15–18. [CrossRef]
87. Barbosa, P.; Brito, A.; Almeida, H. A technique to provide differential privacy for appliance usage in smart metering. *Inf. Sci.* **2016**, *370*, 355–367. [CrossRef]
88. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
89. Ashraf, A.; Elmedany, W. Authentication in IoT devices using blockchain technology: A review. In Proceedings of the 4th Smart Cities Symposium (SCS 2021), Zallaq, Bahrain, 21–23 November 2021; pp. 545–551.
90. Sinha, D. Authentication and Privacy Preservation in IoT Based Forest Fire Detection by Using Blockchain—A Review. In Proceedings of the 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), Jaipur, India, 9–10 May 2019; Internet of Things and Connected Technologies. p. 133.
91. Leelasantitham, A. A business model guideline of electricity utility systems based on blockchain technology in thailand: A case study of consumers, prosumers and SMEs. *Wirel. Pers. Commun.* **2020**, *115*, 3123–3136. [CrossRef]
92. Liu, Y.; Xu, K.-D.; Li, J.; Guo, Y.-J.; Zhang, A.; Chen, Q. Millimeter-wave E-plane waveguide bandpass filters based on spoof surface plasmon polaritons. *IEEE Trans. Microw. Theory Tech.* **2022**, *70*, 4399–4409. [CrossRef]
93. Lin, Y.; Song, H.; Ke, F.; Yan, W.; Liu, Z.; Cai, F. Optimal caching scheme in D2D networks with multiple robot helpers. *Comput. Commun.* **2022**, *181*, 132–142. [CrossRef]
94. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
95. Wongsamerchue, T.; Leelasantitham, A. An Electronic Double Auction of Prepaid Electricity Trading Using Blockchain Technology. *J. Mob. Multimed.* **2022**, *18*, 1829–1850. [CrossRef]
96. Novianti, D.; Arkeman, Y.; Almunawar, M.N.; Haditjaroko, L.; Ismayana, A. Designing a Transparent Distributed Systems for Halal Supply Chains Using Blockchain Technology. *J. Bus. Econ. Anal.* **2020**, *3*, 151–170. [CrossRef]
97. Abidin, N.Z.; Perdana, F.F.P. A proposed conceptual framework for blockchain technology in Halal food product verification. *J. Halal Ind. Serv.* **2020**, *3*. [CrossRef]
98. Alamsyah, A.; Hakim, N.; Hendayani, R. Blockchain-Based Traceability System to Support the Indonesian Halal Supply Chain Ecosystem. *Economies* **2022**, *10*, 134. [CrossRef]
99. Li, A.; Masouros, C.; Swindlehurst, A.L.; Yu, W. 1-bit massive MIMO transmission: Embracing interference with symbol-level precoding. *IEEE Commun. Mag.* **2021**, *59*, 121–127. [CrossRef]
100. Li, D.; Kar, P. B-Spot: Blockchain and Steganography based Robust and Secure Photo Transmission Mechanism. *J. Mob. Multimed.* **2022**, *18*, 1677–1708. [CrossRef]
101. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
102. Zheng, W.; Liu, X.; Ni, X.; Yin, L.; Yang, B. Improving visual reasoning through semantic representation. *IEEE Access* **2021**, *9*, 91476–91486. [CrossRef]
103. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
104. Cao, B.; Zhang, W.; Wang, X.; Zhao, J.; Gu, Y.; Zhang, Y. A memetic algorithm based on two_Arch2 for multi-depot heterogeneous-vehicle capacitated arc routing problem. *Swarm Evol. Comput.* **2021**, *63*, 100864. [CrossRef]
105. Zheng, W.; Liu, X.; Yin, L. Sentence representation method based on multi-layer semantic network. *Appl. Sci.* **2021**, *11*, 1316. [CrossRef]
106. Li, J.; Xu, K.; Chaudhuri, S.; Yumer, E.; Zhang, H.; Guibas, L. Grass: Generative recursive autoencoders for shape structures. *ACM Trans. Graph.* **2017**, *36*, 1–14. [CrossRef]
107. Sankaran, S.; Sanju, S.; Achuthan, K. Towards realistic energy profiling of blockchains for securing internet of things. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; pp. 1454–1459.
108. Wang, Y.; Han, X.; Jin, S. MAP based modeling method and performance study of a task offloading scheme with time-correlated traffic and VM repair in MEC systems. *Wirel. Netw.* **2022**, 1–22. [CrossRef]
109. Kouzinopoulos, C.S.; Spathoulas, G.; Giannoutakis, K.M.; Votis, K.; Pandey, P.; Tzovaras, D.; Katsikas, S.K.; Collen, A.; Nijdam, N.A. Using blockchains to strengthen the security of internet of things. In Proceedings of the International ISCIS Security Workshop, London, UK, 27–28 February 2018; pp. 90–100.

110. Ma, K.; Li, Z.; Liu, P.; Yang, J.; Geng, Y.; Yang, B.; Guan, X. Reliability-constrained throughput optimization of industrial wireless sensor networks with energy harvesting relay. *IEEE Internet Things J.* **2021**, *8*, 13343–13354. [CrossRef]
111. Roy, S.; Ashaduzzaman, M.; Hassan, M.; Chowdhury, A.R. Blockchain for IoT security and management: Current prospects, challenges and future directions. In Proceedings of the 2018 5th International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 18–20 December 2018; pp. 1–9.
112. Rahulamathavan, Y.; Phan, R.C.-W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6.