machines

MDPI

Review

Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions

Jiewu Leng [1,2], Ziying Chen [1], Zhiqiang Huang [1], Xiaofeng Zhu [1], Hongye Su [1], Zisheng Lin [1] and Ding Zhang [1,*]

[1] State Key Laboratory of Precision Electronic Manufacturing Technology and Equipment, Guangdong University of Technology, Guangzhou 510006, China
[2] Shenzhen Research Institute, City University of Hong Kong, Shenzhen 518057, China
* Correspondence: zhangding@gdut.edu.cn

Abstract: Resilient manufacturing is a vision in the Industry 5.0 blueprint for satisfying sustainable development goals under pandemics or the rising individualized product needs. A resilient manufacturing strategy based on the Industrial Internet of Things (IIoT) networks plays an essential role in facilitating production and supply chain recovery. IIoT contains confidential data and private information, and many security issues arise through vulnerabilities in the infrastructure. The traditional centralized IIoT framework is not only of high cost for system configuration but also vulnerable to cyber-attacks and single-point failure, which is not suitable for achieving the resilient manufacturing vision in Industry 5.0. Recently, researchers are seeking a secure solution of middleware based on blockchain technology integration for decentralized IIoT, which can effectively protect the consistency, integrity, and availability of IIoT data by utilizing the auditing and tamper-proof features of the blockchain. This paper presented a review of secure blockchain middleware for decentralized IIoT towards Industry 5.0. Firstly, the security issues of conventional IIoT solutions and the advantages of blockchain middleware are analyzed. Secondly, an architecture of secure blockchain middleware for decentralized IIoT is proposed. Finally, enabling technologies, challenges, and future directions are reviewed. The innovation of this paper is to study and discuss the distributed blockchain middleware, investigating its ability to eliminate the risk of a single point of failure via a distributed feature in the context of resilient manufacturing in Industry 5.0 and to solve the security issues from traditional centralized IIoT. Also, the four-layer architecture of blockchain middleware presented based on the IIoT application framework is a novel aspect of this review. It is expected that the paper lays a solid foundation for making IIoT blockchain middleware a new venue for Industry 5.0 research.

Keywords: decentralized Industrial Internet of Things; blockchain middleware; data security; Industry 5.0; resilient manufacturing

Citation: Leng, J.; Chen, Z.; Huang, Z.; Zhu, X.; Su, H.; Lin, Z.; Zhang, D. Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions. *Machines* **2022**, *10*, 858. https://doi.org/10.3390/machines10100858

Academic Editor: Panagiotis Kyratsis

Received: 31 August 2022
Accepted: 22 September 2022
Published: 26 September 2022

1. Introduction

The pandemic of COVID-19 has expedited the reshaping of supply chain management. Resilient Manufacturing (RM) is envisaged in the Industry 5.0 concept as a result of either sustainable development goals under pandemics or the rising individualized product needs [1,2]. It is described as a manufacturing system that can sustain possibly severe disturbances and recover from an undesired condition to the desired state. As well, it is considered to have the ability to mitigate the negative impacts of disruptions, such as networking faults, machinery troubleshooting, and material supply breakdowns, and swiftly recover to normal conditions.

Industry 4.0 is driven by technology. Its development has brought many cutting-edge technologies, but it lacks robustness and high resilience when exposed to unknown factors. Industry 5.0, based on the technology driven by Industry 4.0, is looking for common

interests and values of workers from different countries, so as to transform into a value-oriented era. Among them, achieving a high level of resilience is an essential capability recognized by Industry 5.0. In the field of the Internet of Things (IoT) in Industry 4.0, the technology-driven IoT has given rise to computers with powerful computing power and cutting-edge data storage and processing technologies. Hence, most IoT architectures rely on a centralized framework, which makes the IoT vulnerable to unknown disturbances in the event of a single-point failure. In contrast, in the value-driven Industry 5.0, where the ability to quickly resume manufacturing when faced with unknown disruptions is a recognized fundamental feature. As well, the decentralized architecture of IIoT plays an essential role in achieving the system resilience in the transition from Industry 4.0 to Industry 5.0. Similarly, a resilient manufacturing strategy based on the Industrial Internet of Things (IIoT) networks plays an essential role in facilitating production and supply chain recovery. IIoT networks comprise billions of devices that generate enormous amounts of data [3,4], which usually contain sensitive information about humans and machines that could pose security issues. The vast majority of modern IIoT frameworks are built on centralized architectures. Users must have faith in the security of these services to process and store their data. Data processing, security, and privacy services are now provided by existing centralized systems, which call for extremely powerful computers from other parties. Data generated from equipment is collected and sent to a central cloud computing center for intense data gathering and translation. It needs a middleware solution to provide a development and execution environment that supports interoperability, distributed decision making, and the effective integration of heterogeneous human-machine systems and devices, which can also make the digital information transparent, immutable, traceable to query, and auditability (in Figure 1). The absence of secure middleware with processing and storage capabilities results in the high complexity of industrial networks. Therefore, researchers are pursuing middleware methods to availably address the mentioned IIoT security issues including integrity, consistency, and availability. However, the information may be utilized inappropriately or disclosed to certain unauthorized parties. The use of IIoT middleware will likely be severely constrained in the future due to the inadequacy of traditional security measures (e.g., cryptographic techniques). A centralized system may also make it difficult for the IIoT to be highly scalable and robust in the event of a single-point failure, which is not suitable for achieving the resilient manufacturing vision in Industry 5.0.

Decentralized techniques may be a preferable option to increase the security and dependability of current IIoT systems [5]. In addition to preventing single points of failure, the decentralized architecture of IIoT enables the long-term expansion of networks, in which blockchain is an important enabler [6]. Blockchain is a distributed ledger [7] that cannot be tampered with or cryptographically faked because of the chain topology that joins data blocks progressively following the chronological order [8]. Blockchain has many advantages to solve the dependability, interoperability, and security concerns of IIoT [9] by supplying decentralized processes. Industrial processes and entities will be able to register and confirm their products and services via the integration of blockchain with IIoT [5]. Establishing blockchain middleware for decentralized IIoT could provide dependable and secure services for industries to store and trade data, addressing the issues mentioned above (e.g., interoperability, heterogeneity, data security) and thus building trust among the value chain's participants [10]. Blockchain middleware can offer software or interface for many platforms and applications to successfully integrate communication between devices and the blockchain network. Through blockchain middleware, programmers with insufficient knowledge of the blockchain can shield the complex and tedious blockchain underlying principle to implement the interoperability between IIoT data and blockchain network, and the deployment of smart contracts via its API interface. In this way, it can promote the implementation of scalability, reliability, real-time, availability, security, and privacy of decentralized IIoT applications towards Industry 5.0.

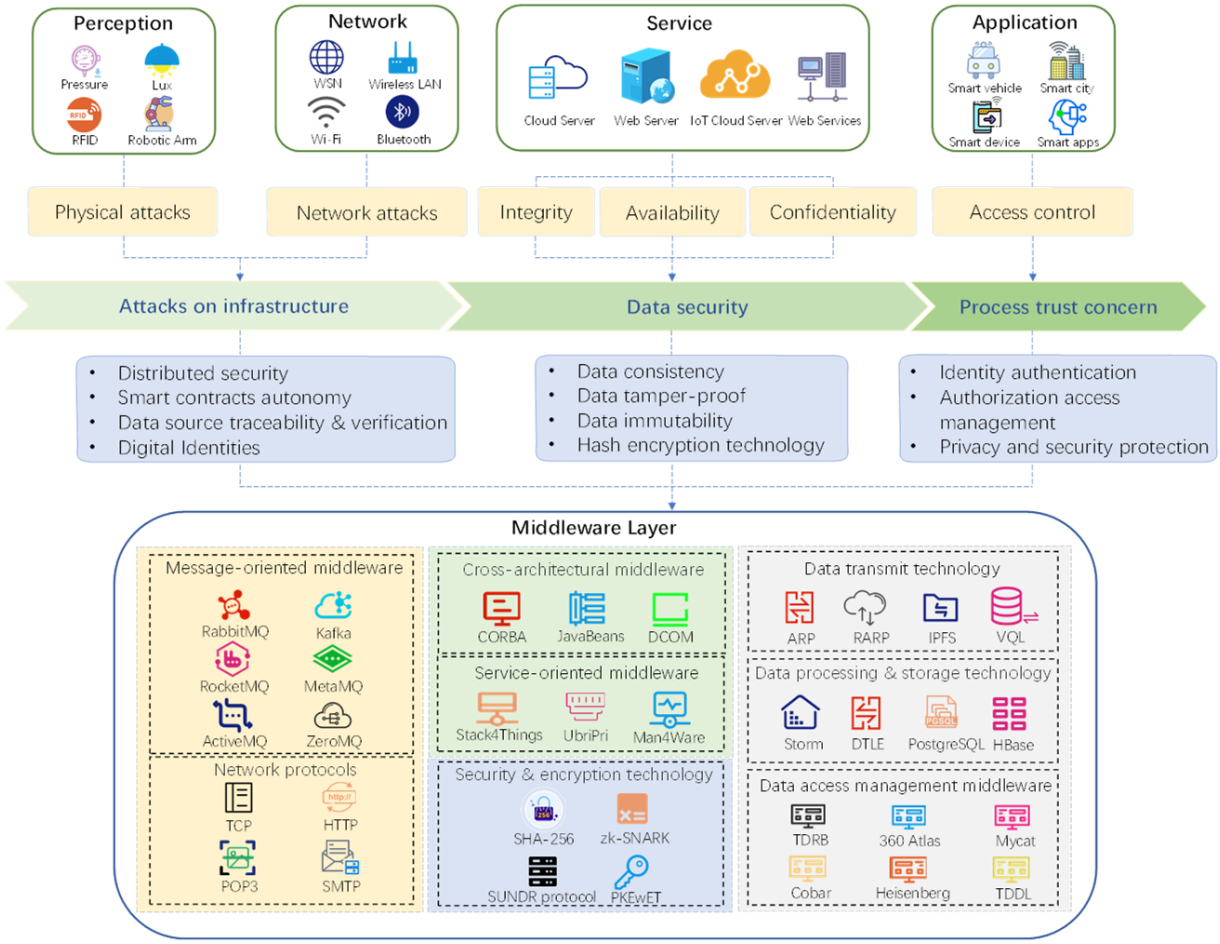

Figure 1. Conventional middleware solution and security issues for IIoT.

Recently, researchers are pursuing a blockchain middleware method to availably address the mentioned IIoT security issues. However, the current exploration of blockchain middleware is still at its initial stage. Muller and Breque [1,2] both specifically discussed the key role of resilience in industry 5.0, but they did not elaborate on the impact of blockchain technology on industry 5.0 in terms of distributed information security from the perspective of resilience. In terms of the IIoT, Xu et al. [3] summarized the application status, enabling technologies, and future directions of the IoT in the industrial field in detail, but the description of the application level of the IoT middleware and blockchain technology is not comprehensive. Wang, Lian, Leng, and Zheng et al. [6–9] summarized the application of blockchain technology in IoT and IIoT in detail. They emphasized that the characteristics of blockchain technology (tamper-proofing, immutable, and decentralized), data structure, and consensus mechanism play a key role in the security issues of IIoT. However, their discussion on the application of IoT middleware is not comprehensive enough, and the key enabling technologies and challenges of IoT middleware are not mentioned in the classification. Latif et al. [5] reviewed the development and application status of blockchain technology in IIoT. The integration of some middleware platforms and blockchain technology were also studied from the perspective of IoT middleware, but the key role of blockchain middleware in Industry 5.0 resilient manufacturing was not analyzed in the paper. Current research findings on secure blockchain middleware are relatively scarce and less systematic. A systematic introduction to blockchain middleware for decentralized IIoT towards Industry 5.0 is absent. Motivated by this observation, this paper tries to review secure blockchain middleware for decentralized IIoT towards Industry

5.0. We searched the Web of Science databases for literature. A three-step process was used to further analyze the articles that were found.

Using appropriate screening criteria, the initial step is to find high-quality articles. To produce high-quality publications, working papers and commentary are not included. Meanwhile, three keywords, namely, "Industrial Internet of Things", "blockchain middleware", and "data security and privacy", were identified for searching publications. This inclusive search yielded 271 publications for further analysis (up to 31 July 2022).

Secondly, to emphasize the architecture and the role of blockchain middleware in IIoT, articles on advanced technologies for IIoT security and blockchain middleware are also included. More specifically, the selection criteria are shown as follows.

1. These studies highlight the security issues, including infrastructure security, data security, and process trust, in IIoT, are selected. These studies highlight the concepts, technologies, architecture, and application of blockchain middleware technology in IIoT is selected.
2. Reviews/frameworks on IIoT blockchain middleware and enabling technologies were evaluated to offer a comprehensive understanding of the trends, functions, technologies, and challenges involved in Industry 5.0.
3. Studies containing concepts and issues related to digital transformation were taken into consideration, including those that did not specifically include blockchain middleware in the title, keywords, or abstract. This makes it possible to identify potential directions for future industrial innovations.

Research that is unrelated to (1) IIoT management or the blockchain domain; (2) studies that were not authored in English; (3) brief papers that are fewer than four pages are eventually excluded.

In the final step, 105 articles that fit the criteria for inclusion were included, and 21 more articles were found after the references were used as a source for literary analysis. Additionally, 21 supplementary references were added to make the review concrete. Therefore, this review consists of 126 articles in total.

Therefore, this review discusses the research status of blockchain middleware applications in decentralized IIoT. Firstly, the security issues of conventional IIoT solutions are analyzed in Section 2. Secondly, the advantages of blockchain middleware and architecture of secure blockchain middleware for decentralized IIoT are proposed in Section 3. Finally, enabling technologies, challenges, and future directions are reviewed in Sections 4 and 5, respectively. Finally, Section 6 presented the concluding remarks obtained from this review.

2. Security Issues in IIoT

2.1. The Characteristics of IIoT

Applications for the Internet of Things can influence many areas of daily life for workers. IIoT devices, networking, and communication technologies vary to fit the goals and requirements of diverse human-machine collaborative applications. Additionally, IIoT refers to the application of specific IIoT technologies and various smart objects (such as smart sensors, smart actuators, and smart manufacturing devices) in an industrial setting for the advancement of goals specific to the industry. New research trends for industrial applications are being introduced by IIoT [11,12]. It incorporates several cutting-edge technologies, including digital twins, big data analytics, robots, artificial intelligence (AI), smart sensors, actuators, and different communications protocols in traditional industrial environments [3,4]. By streamlining the production process, lowering costs, and boosting the productivity of smart businesses, IIoT aims to improve the performance of current industrial operations. It is clear that IIoT has attracted both academic and industrial interest, and as a result, it will significantly influence the design and development of next-generation (Industry 5.0) industrial infrastructures. The following list of IIoT characteristics serves as a summary.

2.1.1. Mass and Jumbled Data

Big data from IIoT sensing has the following qualities: high volume, high velocity, high veracity, and high diversity. Massive volumes of data can be produced in real-time by sensor devices. In this case, the problem with manufacturing data is both inconsistent and unreliable. This difficulty results from the variety of data types used in manufacturing, each of which calls for a specific signal acquisition parameter [13].

Furthermore, results may be predicted using big data processing and machine learning approaches. Due to the fast expansion of IIoT sensing, massive data are produced and stored locally or in cloud-based data repositories. Fundamentally new approaches for large-scale IIoT data management, information processing, and industrial process control are necessary to fully realize the full potential of big data analytics for smart manufacturing. For instance, the IIoT may use a large number of sensors to continually track the state of a machine in real-time and subsequently send data to the cloud. IIoT data includes both real-time data from in-situ monitoring of machines as well as signals gathered from machining tools and units. Easy access to the data from the cloud platform allows for parallel processing on distributed computers, which may be utilized to gather important data and develop prediction-making algorithms. In the end, decision-making is encouraged (e.g., production scheduling) [14].

2.1.2. Distributed Architecture

IIoT is moving towards distributed nature. Its distributed architecture is advantageous to the deployment of edge computing. Data generated in the IIoT is growing exponentially and much faster than that in traditional centralized cloud environments, where data is stored. As well, data storage and transmission issues (such as latency and bandwidth) on cloud devices make transmission speed a core issue. Therefore, a distributed architecture facilitates the deployment of edge computing to effectively solve the problem of inefficient transmission from IIoT to cloud architecture.

Rather than processing centrally in an internally deployed data center or public cloud, the distributed edge architecture brings it closer to the humans and devices in use. Edge computing is critical for manufacturing processes that use large amounts of data and require fast response times while ensuring safety. From IIoT devices to data centers, the cloud features (e.g., data, networking, storage, and computing) are distributed at all levels of the overall edge computing node [15], transferring the storage and calculation to the most efficient location for processing data. Then the key performance of IIoT application, safety, and efficiency requirements can be realized.

2.1.3. Heterogeneity

1. Multiple devices and heterogeneous network communication

Heterogeneity is a key characteristic of the IIoT when acting as manufacturing services [16]. The heterogeneity of the IIoT ranges from machines to humans and networks. When it comes to communication between different devices encapsulated with heterogeneous networks, gateways play an indispensable role. The gateway of the IIoT is mainly used for device access, data collection, and device monitoring. The main function of the gateway is to convert the equipment with two different protocols into the corresponding protocol for two-way data transmission. It is mainly aimed at networking heterogeneous devices that cannot communicate directly. When implementing the IIoT, decisions about how to transfer data are often complex. Currently, the three most common IIoT communication protocols are MQTT, AMQP, and COAP. The standardization of IIoT data connectivity and advance in simulation tools make it easier to make more informed decisions on data connectivity and integration.

Heterogeneous network integration is a promising emerging solution. For network heterogeneity of IIoT in Industry 4.0, many researchers have presented some architectures to integrate diverse networks. However, the presented solutions lack a consistent paradigm for accessing diverse networks and are only partially employed to address the hetero-

geneity of diverse constrained wireless communication networks [17]. Therefore, unified governance of heterogeneous networks is necessary to enable communication between the various networks. The use of network middleware, which gives clients a single application call interface while hiding the heterogeneity of underlying networks, is one feasible option [17]. Additionally, it is important to standardize the middleware's interface as much as possible so that the device producers can develop adaptive device connections with heterogeneous networks.

2. Interaction of heterogeneous systems and software

With the exponentially-growing network size and heterogeneity in systems, the development of IIoT security faces huge challenges. In such an environment, it is worth considering how to integrate heterogeneous systems to achieve efficient and safe interactive operation. Currently, the middleware solution has become an effective tool for researchers to achieve interoperability between systems. It allows for the on-demand integration of systems and software components. Additionally, it aids in the abstraction of availability and heterogeneity. To add new values for various systems, several middleware platforms were created.

2.2. The Architecture of IIoT

In this section, we first examine the foundation of a fundamental IIoT architecture and how these security concerns might work there before diving into a more in-depth examination of security issues. Several ideas provide different IIoT designs. These architectures are often categorized according to layers. Notably, the IIoT architecture frequently overlaps with these layers.

Sisinni et al. [18] proposed a three-layer design for the IIoT. The layers are sensors, networks, and services. Xu et al. [19] presented another three-layer design for the IIoT. It contains physical, communication, and application layers, unlike [18]. In [20], a four-layer IIoT architecture that consists of layers for perception, network, support, and application is proposed. The support layer can be viewed as a data layer conducting data analytics functions. In [5], different from the support layer of the proposal IIoT architecture in [20], another four-layer IIoT concept that is extensively used was introduced. The four-layer in [5] contains the perception, network, middleware, and application layers. In this section, each of these layers will be briefly discussed. A five-layer reference architecture is approved by the International Telecommunication Union. It includes layers for sensing, gaining access, networking, middleware, and applications.

An IIoT architecture in [5] is introduced. Notably, we choose a four-layer architecture that may be applied to various IIoT systems. It can accommodate the fundamental components of a three-layer IIoT architecture, while also readily expanding this four-layer architecture with additional components to depict a five-layer IIoT architecture with finer granularity. In addition, considering that the discussion focuses on the application of blockchain middleware to IIoT security issues, the enterprise applications and cloud computing services will not be discussed in this paper. That said, as shown in Figure 2, the IIoT security issues we summarized fit into the discussion in a four-layer architecture.

2.2.1. Perception Layer

The perception layer, which includes a variety of sensors for collecting various kinds of human-machine collaborative production context data, is thought to be the lowest physical layer of the IIoT architecture [21]. The perception layer is made up of sensors and actuators that acquire and interpret context data to carry out tasks (e.g., retrieve location and acceleration) [22]. A variety of IIoT applications require the perception layer [23]. To connect the physical and cyber worlds, a variety of end devices can be employed at the perception layer. Near Field Communications (NFC), RFID, wireless sensors and actuators, RFID, and some smart devices are examples of typical end devices. This layer also makes use of many sensing technologies including GPS, WSN, RSN, and others. Multiple sensors built within it collect information and recognize smart items in an industrial setting. With

specific computational and energy needs, sensors, actuators, imaging devices, RFID tags, and other technologies are the main technologies of this layer. After being transformed into digital form, the data collected from the environment is sent to the network layer. For instance, an RFID tag consists of a tiny microchip linked to an antenna. In a manufacturing environment, things may be recognized, tracked, and monitored by applying RFID tags to them. Additionally, this layer can be divided into perception nodes and networks [5].

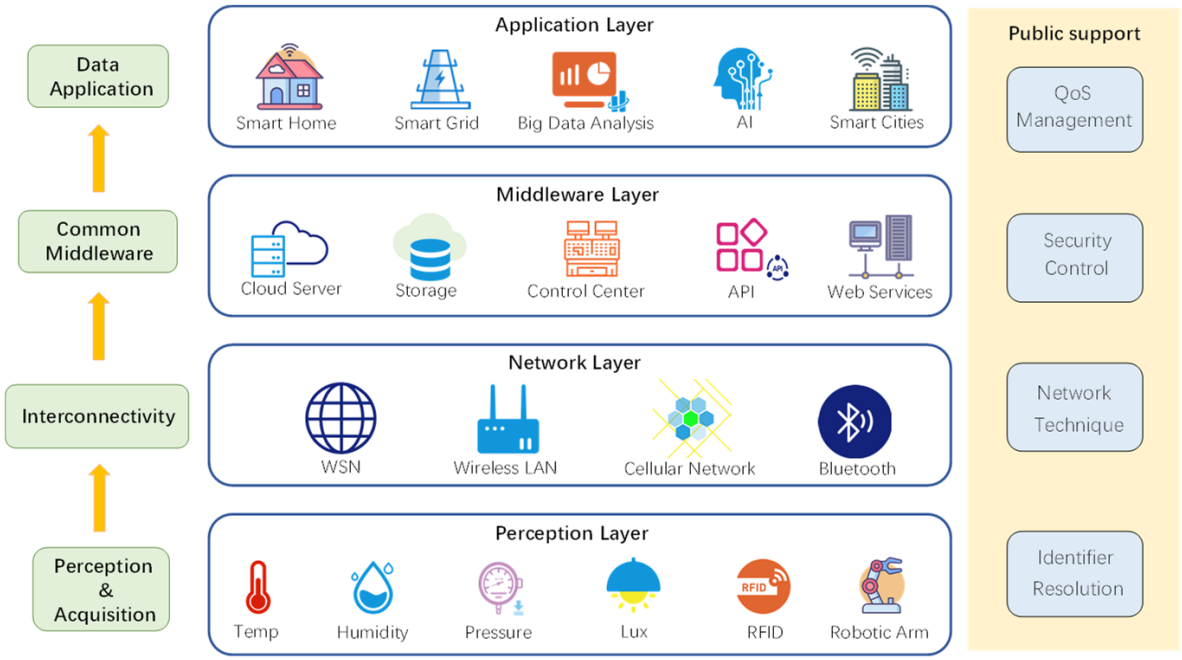

Figure 2. The four-layer architecture of IIoT.

2.2.2. Network Layer

The network layer encapsulates large amounts of protocols (e.g., MQTT, COAP, ZigBee, Ethernet). For the protocols of the IIoT, it can generally be divided into two categories, namely communication protocol (e.g., Bluetooth and ZigBee) and transmission protocol (e.g., High-Speed Ethernet (HSE), Modbus TCP/IP, and ProfiNet), performing secure information sharing [24]. Cloud computing and the Internet are the fundamental components of this layer [25]. Additionally, Internet gateway devices work in this tier by utilizing the most recent communication technologies to deliver network-connected services.

2.2.3. Middleware Layer

This third-level layer, commonly called the support layer, is presented [26]. It offers IIoT systems database and cloud services for the application layer to use further [27]. The middleware layer employs advanced computational techniques to evaluate, process, and store data. It can use cutting-edge technologies such as cloud computing and big data analytics to automatically analyze and compute the information that has been acquired. As described in the previous section. Middleware has become an effective tool for researchers to achieve interoperability between systems [28]. Some middleware models were proposed to provide added value for various industrial systems. The details will be described in later sections.

2.2.4. Application Layer

The termination layer of the IIoT is another name for the application layer. By preserving data integrity, secrecy, and authentication, this layer performs as the bridge between users and applications. This layer accesses the middleware layer's data and offers multiple services to the users. Additionally, it is integrated with commercial organizations to access

smart applications [29,30]. Using internet-capable devices such as smartphones, tablets, PCs, wearable technology, and many other smart gadgets, users can access the smart services at this layer. To develop smart applications, the application layer incorporates the IIoT network, such as smart factories, healthcare, and smart grid [31].

2.3. Security Issues in IIoT Architecture

The stable operation of IIoT brings significant improvement in automation level to industry, and at the same time makes it challenging to impose more security issues within it [32]. Several security issues must be solved to offer the client and users a flexible, scalable, and reliable IIoT environment. Attacks on IIoT raise a serious security issue for the industry. These attacks have the potential to seriously harm businesses and occasionally even put lives in danger [33]. One of the most important challenges in an IIoT system, among others, is data security. Usually, the characteristics of an IIoT system make it challenging when the standard heavy-weight security designs cannot be directly used to meet such difficulties (e.g., resource-constrained, heterogeneous, mobile). On the contrary, they need more systems and frameworks that can satisfy the unique needs of an IIoT system. Therefore, a platform for smooth data exchange between enterprises is required to transmit and analyze multiple data sources efficiently, such as in a supply chain network [34]. Consequently, organizational issues, such as cross-enterprise information sharing and cooperation (via data interchange and transparency), are especially demanding in addition to technological considerations. Due to the IIoT-linked network of heterogeneous communication protocols, and various network platforms, a possible vulnerability in one area may cause a more significant effect on the system's entire performance [35].

In general, developing a comprehensive and cohesive system is challenging due to the heterogeneity in the IIoT system. The security issues in IIoT have been compiled and categorized in several surveys. For example, four primary categories of security attacks in the IIoT were Physical Attacks, Network Attacks, Software Attacks, and Data Attacks [31]. For IIoT, [31] has examined relevant studies on IIoT security challenges from the two perspectives of defending/preventing attacks and authentication/authorization. Jayalaxmi et al. [20] presented a security taxonomy for the IIoT system based on six distinct security services: authentication, confidentiality, non-repudiation, availability, integrity, and privacy. Pal and Jadidi [33] summarized the data confidentiality, they also considered the communication, performance, and heterogeneity in users and devices. Further, dynamic infrastructure as one of the IIoT characteristics and cascading services are discussed. Leng et al. [8] considered the combination of IIoT security issues and blockchain technology. They proposed a PDI framework for surveying blockchain security.

In this paper, we considered the comprehensive survey on IIoT attacks proposed by Jayasree Sengupta et al. [31] and introduced cyber-attacks from four layers in IIoT proposed by Shahid Latif et al. [5]. Moreover, as shown in Table 1, based on the proposed attacks categorized by Shahid Latif et al. [5], we further supplement the classification of these security issues (including cyber-attacks, threats, and potential security [33]), and categorize the attributes of them corresponding to the layer they are in. Especially, based on the middleware layer mentioned by Shahid Latif et al. [5], we combined the analysis of security issues in the support layer from Shantanu Pal et al. [33] and in the processing layer from Jayasree Sengupta et al. [31] and supplement the security issues of the middleware layer. At last, we reclassified the security issues into three categories (i.e., attacks on infrastructure, data security, and process trust concern) based on the related works [31,33,36]. The details are described as followed in Figure 3 and Table 1.

Table 1. The overview of IIoT security issues.

Security Type		Attack Name	Description
Attacks on infrastructure	Physical attacks	Tampering [37]	The act of physically modifying a device (e.g., RFID) or communication link. Such a type of attack will lead to the consequence of access to sensitive information and gain access.
		Attack device performance [38,39]	The target of these attacks is mainly to affect or interrupt system operation by affecting device performance, for instance, a heatstroke attack, DoS/DDoS, and replay attacks.
		Side channel attack [37]	Attackers collect the encryption keys by adopting timing, power, and fault attack on devices to encrypt/decrypt confidential data.
		Permanent Denial of Service (PDoS, phlashing) [31]	Attacks are launched by destroying firmware or uploading a corrupted BIOS using malware.
		RF interference/jamming [40]	Attackers create and send noise signals over the Radio Frequency (RF)/WSN signals to initiate DoS attacks on the tags/sensor nodes thereby jamming communications.
	Network attacks	Injection attacks [40]	Include malicious code injection and fake node injection.
		Traffic analysis attacks [37]	Confidential data flowing to and from the devices are sniffed by the attackers.
		DoS/DDoS [31]	Attackers make the network traffic unavailable to the users, or multiple compromised nodes attack a specific target by flooding messages to crash the server/resources.
		Control over communication attacks [41,42]	Attackers target routing protocols and redirect the routing path from the original receiver to an insecure one by misconfiguring routers, gateways, and DNS servers. Include blackhole, wormholes, Sybil, and pharming attacks.
Data security	Integrity	Dynamic Infrastructure [43–45]	The interactions in IIoT are dynamic. It requires better security protections that could securely integrate a real-time IIoT state in cyberspace into the physical space.
		Data (resource) security [43,46,47]	Attackers manipulate sensitive information and perform unauthorized data access, breaching the trust relationships between users.
	Confidentiality	MITM attack [48]	Attackers join the network as legitimate users and gain control over the nodes via the active attack path to sniff information.
		Data breach [31]	The disclosure of personal, sensitive, or confidential information in an unauthorized manner.
		Phishing site [49]	Attackers obtain a user's private information by sending emails that contain a malicious link (e.g., malware or spyware).
		Sniffing attacks [48]	Attackers take control over a device through device tracking or tag tracking and then attack devices that are connected to them.
	Availability	Data Inconsistency [31]	Attack on data integrity results in the inconsistency of data in transit or data stored in a central database.
		Malware [50]	An adversary infects the system via malicious software to achieve tamper with data or steal information, or launch DoS.

Table 1. *Cont.*

Security Type	Attack Name	Description
Process trust concern	RFID Unauthorized Access [37]	An attacker can read, modify or delete data presented on RFID nodes because of the lack of proper authentication mechanisms.
	Unauthorized Access [31]	Access control gives access to authorized users and denies access to unauthorized users. With unauthorized access, malicious users can gain data ownership or access sensitive data.
	Device impersonation [51–53]	Using identity fabrication to disrupt the integrity of a database by data forgery.
	Service interruption [54,55]	The failure of cascading services and misuse of the services by malicious actors lead to the failure of interconnected services.

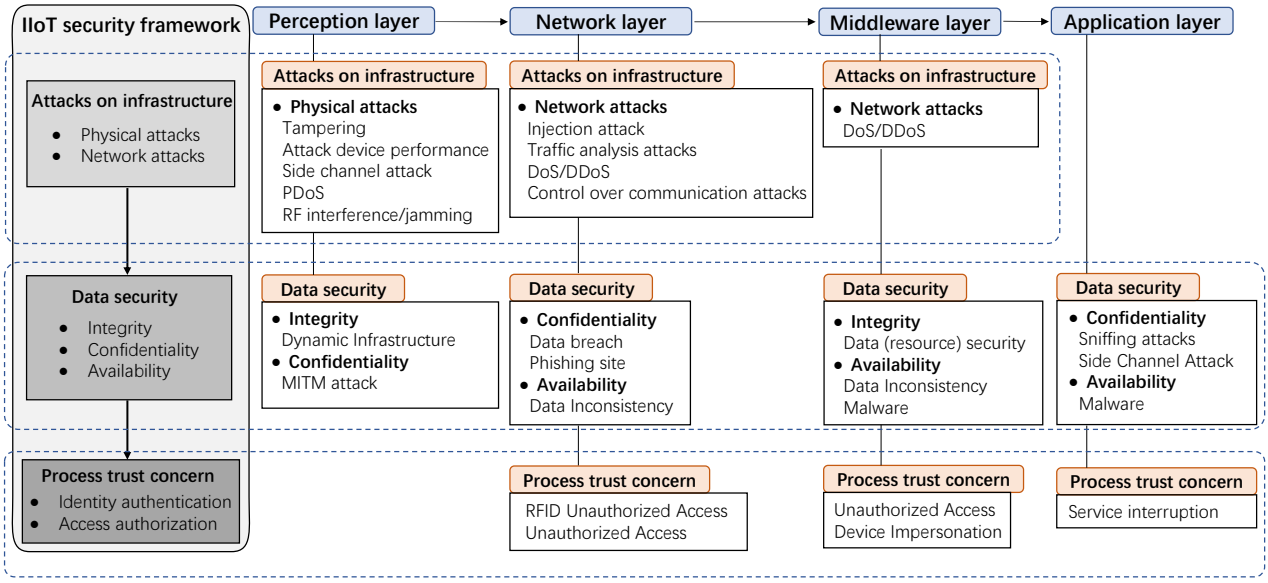

Figure 3. The framework of IIoT security issues.

3. Blockchain Middleware for Decentralized IIoT

This section discusses how blockchain is integrated into a middleware framework for many IIoT security issues. Typically, distributed resources and services from many technologies are used in smart manufacturing applications [56,57]. These resources and services could come from a single huge manufacturing company or a group of linked companies that work to support a targeted value chain. In this way, the distributed ledger services can then be connected to the blockchain-based middleware to create verifiable and immutable transaction logs. These transactions on the blockchain network can also be authenticated. Reliable, traceable records and resources to ensure that these transactions are accurate. The whole process will be supported by the blockchain services, which will also replicate and distribute the finished transaction across the involved entities as well as encrypt and append it to the chain. Finally, blockchain middleware for decentralized IIoT provides the ability to mitigate the negative impacts of disruptions, such as networking faults, machinery troubleshooting, and material supply breakdowns, and swiftly recover to normal conditions.

3.1. Advantages of Blockchain Middleware in IIoT

The resilient manufacturing vision in Industry 5.0 blueprint implies the ability to mitigate the negative impacts of disruptions, such as networking faults, machinery troubleshooting, and material supply breakdowns, and swiftly recover to normal conditions. A resilient manufacturing strategy based on the IIoT networks plays an essential role in facilitating production and supply chain recovery.

The advance of heterogeneous devices/technologies/applications of IIoT brings new challenges to developing applications in the industrial environment [58]. In this case, a middleware solution can integrate heterogeneous computing and communications devices, facilitate interoperability between applications and services, and provide common services for applications while simplifying application development [59,60]. As one of the application branches of the IIoT, the development of the IIoT is closely related to the development of Industry 5.0 [56]. Multiple functional types of devices or applications should be coordinated to achieve a shared goal.

However, there are pressing issues (e.g., interoperability, heterogeneity, and data security) that currently impede its effective development. Additionally, conventional security measures such as cryptographic methods [61] alone are unable to maintain data integrity on this massive scale. Furthermore, it is unrealistic to simply extend costly Internet security methods into the IIoT [62–65]. On the one hand, IIoT services such as centralized cloud storage could inherent insecurity from cyber-attacks, malicious code injection, and tampering that have a great influence on data security issues [31,33]. In addition, the cloud services storage is vulnerable to single-node failure [65–67]. On the other hand, in the context of IIoT, things and resources are heterogeneous and require specific programming [68]. Furthermore, the deployed protocols, together with conversion mechanisms, need to interoperate at different layers of the IIoT network safely [8]. In general, traditional IIoT services cloud cannot ensure data security such as integrity, consistency, and availability. It needs a middleware solution to provide a development and execution environment that supports interoperability, decentralized decision-making, and the effective integration of heterogeneous systems and devices, which can also make digital information transparent, immutable, traceable to query, and auditability. Therefore, researchers are pursuing a middleware method to availably address the mentioned IIoT security issues.

This distributed ledger cannot be tampered with or cryptographically faked because of the chain structure that links data blocks sequentially following the chronological order [8]. Blockchain enables distributed (peer-to-peer) and trusted (software application) transmission and recording of transactions and events. By incorporating blockchain technology into a middleware that combines various manufacturing processes with other value chain elements, it is possible to protect applications and build trust amongst the participants in the value chain [56,69]. This blockchain middleware approach enables addressing the issues mentioned above (e.g., interoperability, heterogeneity, and data security) and promotes the benefits of IIoT for achieving system resilience towards Industry 5.0.

As shown in Table 2, the metrics of blockchain middleware can be categorized in several aspects as follows:

Table 2. Metrics for application of blockchain middleware in IIoT.

Type	Metrics	Instance
Digital identities	Access permissions management	Develop distributed access control policies for the Internet [70]
		Data Authentication and privacy protection [71]
	Identities verification	No need to buy cryptocurrency or protect private keys [72]
		Digital asset management [73]

Table 2. *Cont.*

Type	Metrics	Instance
Distributed security	Privacy preservation	Point-to-point encrypted transmission and digital signature [74]
		Authorization, communication, and subject matching encryption [65]
	Data security	Data tamper-resisting [7,75]
Smart contracts	Autonomous application	Without the requirement for significant paperwork or third-party registration [56]
		Delegation of access permissions [76]
	Trust support	No need to verify whether participating on both sides is trustworthy [71]
Micro-controls	Data transmission	Enhance the data synchronization [77]
	Data storage	Reorganize the data from the database [78]
	Data tracking	Enrich the data query function based on the blockchain data provenance [79,80]

3.1.1. Digital Identities

Blockchain provides a digital analog that can be utilized to identify various entities, including corporations, in addition to machines [81]. Such characteristic makes it possible to verify the identity of individuals and organizations taking part in industrial operations through a public network. Hence, every entity participating in the manufacturing process, including machines can be given a digital identity.

Blockchain middleware can utilize a digital Identity authentication mechanism to realize. In the way of integrating a Networked smart object (NOS) (i.e., a flexible and cross-domain middleware) with the blockchain network, Rizzardi et al. [70] presented a secure and reliable distributed cross-domain access control. Genes-Duran et al. [72] proposed a blockchain middleware, which allows users to purchase services. Tapas et al. [76] proposed a model, which supports distributed resource access authorization and delegating responsibilities through the combination of the Ethereum blockchain network, smart contracts, and Stack4Things. Park et al. [71] proposed a framework. Based on digital identity authentication, it supports automatic off-chain operation verification, data authentication, and privacy protection. Hasan et al. [73] introduced a blockchain-based distributed digital manufacturing asset platform.

3.1.2. Distributed Security

The capability of blockchain to use a distributed approach to preserve the data is one of its fundamental success factors. Integrating IIoT middleware with blockchain networks allows for the protection of individual transactions. For instance, Lian et al. [7] proposed tamper-proof detection middleware. It ensured the integrity and consistency of data and the security of confidential data recorded in the blockchain and relational database. Tapas et al. [76] proposed a model. By integrating the middleware Stack4Things with the Ethereum blockchain network, the model realizes a distributed resource access authorization. Ochoa et al. [74] proposed a blockchain middleware called PriChain, which leverages the Ethereum blockchain to achieve the decentralization of the UbiPri middleware. Lv et al. [65] implemented distributed privacy protection for the publish/subscribe model, this approach effectively avoids a centralized single point of failure. Additionally, it becomes impossible for any of these organizations to subsequently dispute being engaged or in agreement because each transaction is documented with complete consent from all parties involved and relies on confirmed digital identities [75]. The method employed enables greater trust in the accuracy of the recorded transactions as well as improved transaction protection, and reduced exposure risks in the event of security breaches.

3.1.3. Smart Contracts

The use of blockchained smart contracts can effectively empower manufacturing industries and it might potentially boost several industrial sectors in diverse manners. Automation of agreement procedures between businesses and their partners and consumers is one of these improvements in the framework of Industry 4.0 [56]. Eliminating the need for third-party registrations or extensive documentation, would greatly cut administrative expenses and offer a more effective model for initiating, negotiating, and finalizing contracts. Smart contracts can be used to undertake several agreements along the value chain for smart manufacturing. Smart contracts can be completed more quickly and inexpensively while maintaining the legitimacy and validity of standard contracts.

In the application of IIoT, many researchers have proposed blockchain middleware driven by smart contracts. Tapas et al. [76] combined the functions of smart contracts to enable resource access authorization and delegation responsibilities. Park et al. [71] enable smart contracts to make the middleware support automate off-chain operation verification. Ochoa et al. [74] integrated a smart contract with a distributed storage service IPFS, which effectively ensured users' privacy.

3.1.4. Micro-Controls

Allowing for fine-grained modifications is another way that blockchain capabilities might benefit smart manufacturing [56]. The capacity to safely record activities without external verifications and guarantees will enhance the quantity of data and activities that are recorded and enable enterprises to create comprehensive ledgers of their operations. To give quality controls at any degree of detail, they may be simply examined. Additionally, it allows the generation of precise records that are simple to use as audit trails and assessment criteria for a manufacturer's operations [82]. This will make it possible for processes and activities to be continuously recorded. For instance, blockchain enables the constant and precise collection of data on situations involving safety. By doing this, the authenticity of data, authenticity, and creation of an unchangeable record are all guaranteed. Following that, data can be mined to examine any recorded information, including occurrences, consequences, and reactions. As a result of the analysis, these accidents will be better understood, patterns and the causes of issues will be found, and information will eventually be used to improve operations and develop better safety procedures.

In recent years, researchers are also pursuing a middleware method that enhances the data transmission and storage of the ledger data recorded in blockchain to facilitate micro-control of industrial manufacturing. For instance, Wang et al. [77] use middleware as an intermediary to facilitate the synchronization of database data to the blockchain. Peng et al. [78] proposed a blockchain-based middleware layer, which can extract transactions from the blockchain and efficiently reorganize them into the database. In addition, the middleware also provides various query services for users. Zhou et al. [79] proposed a distributed ledger data query platform, it not only supports querying blocks and transactions in a variety of ways but also provides a function to track its running history, which enables users to query blockchain blocks and transactions by shielding underlying principles of the blockchain. Hasan et al. [73] proposed a blockchain-based client middleware, in which the customers can track the source of data generated based on blockchain architecture in manufacturing systems. Liu et al. [80] proposed a blockchain-based middleware to process and store heterogeneous data from multiple sources at different stages of the product lifecycle. The research effectively addressed cross-enterprise access, processing, and analysis of production information problems. In addition, the integrity and confidentiality of product data are also considered. Based on the existing data storage middleware, Lu et al. [83] realized a blockchain-based cloud data acquisition and processing system with a large flow, high concurrency, and high availability.

3.2. Architecture of Secure Blockchain Middleware for Decentralized IIoT

This paper proposed the architecture of the blockchain middleware for decentralized IIoT towards Industry 5.0 as shown in Figure 4. In general, the IIoT middleware integrated with the blockchain network is connected to the application layer. In Figure 4, there is an interaction of four processes. In the process I, it shows the data transmission between the database and the middleware layer. The middleware layer acts as an intermediary between the blockchain network and the database. In the process II, for the connection between the middleware layer and the blockchain network, the middleware layer can utilize the service of blockchain, realizing data consistency, integrity, traceability, and auditing in IIoT. In the process III, data for object identification, tracking, and monitoring in a manufacturing environment can interact at the network layer through transport protocols between different devices. The design, the manufacturing, the manufacturing schedule, and other information of products can be packaged as a transaction recorded in the blockchain layer. In the process IV, for the connection between the application layer and the middleware layer. IIoT applications enable invoking related services of the middleware layer, such as query service, message pub/sub, and authentication and authorization. At the same time, the application layer in the upper can provide technical support for the middleware layer. For example, deep learning can be used to select the storage strategy of the middleware, and big data extraction and analysis technology is used to promote the middleware to make the data reorganized and to be on-chain. Table 3 is the related work on four processes in the architecture of blockchain middleware.

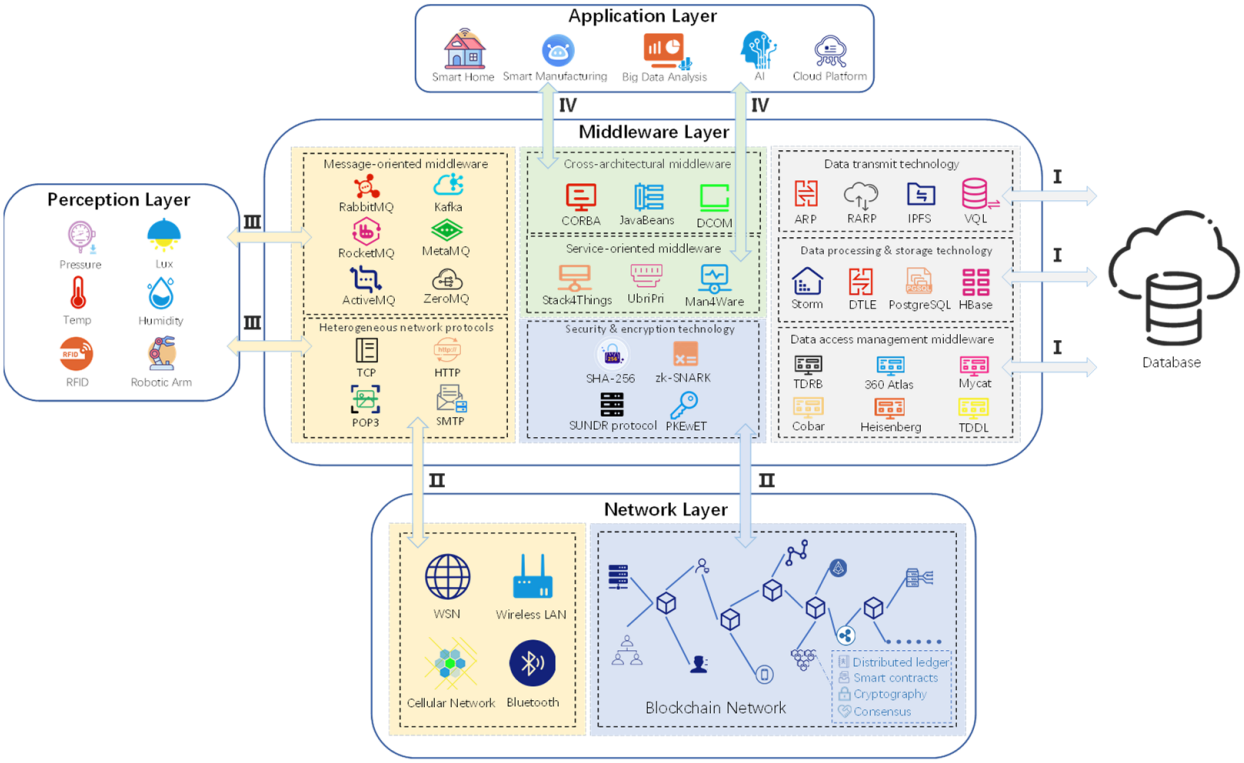

Figure 4. The architecture of the blockchain middleware for decentralized IIoT.

3.3. The Review of Blockchain Middleware

Based on the description of blockchain middleware in the previous section and the contribution of blockchain middleware mentioned in 23 references, we summarize the mentioned blockchain middleware in Table 4. By combining the architecture of blockchain middleware proposed in the last section, we divide them into five categories according to their functional type, including distributed data storage, data synchronism, security and

privacy, function integration, and blockchain IIoT cloud platform. The details of the review are described below.

Table 3. Related work on four processes in the architecture of blockchain middleware.

Process	Related work	References
Process I	Create a verifiable query layer to make transactions in the underlying blockchain system efficient to extract and reorganize.	[78]
	Combining distributed storage services with IPFS data transfer technology for data storage security and IIoT performance.	[74]
	Using the four-module model to facilitate the synchronization between database and blockchain system.	[77]
	Using TDRB middleware to achieve the tamper-proof monitoring of data transmission between blockchain and relational database.	[7]
Process II	Combining middleware with the blockchain Hyperledger Fabric to achieve data traceability and queryable.	[79]
	Using blockchain cryptography to protect pub/sub-system from centralized single points of failure.	[65]
	Leveraging blockchain transaction validation technology to achieve efficient and secure heterogeneous networks.	[84]
	Using cloud storage combined with blockchain technology to ensure security and prevent forking attacks.	[85]
Process III	Information (e.g., product design, manufacturing progress, and data for tracking and monitoring) in the manufacturing system is packaged into transaction records via middleware between the perception layer and the blockchain system.	[73]
	The multi-source heterogeneous manufacturing data of the product life cycle is packed on-chain through the perception layer, and the manufacturing process autonomy is completed by leveraging smart contracts.	[80]
Process IV	Using machine learning algorithms to implement on-chain storage strategy selection.	[64]
	Leverage big data collection and storage technology to achieve high throughput and concurrency of the system.	[83]
	Using a combination of service-oriented middleware Stack4Things for distributed resource access authorization and responsibilities delegation.	[76]
	Using Byzantine consensus algorithm to achieve distributed fault tolerance of pub/sub system application.	[66]

Table 4. Review of blockchain middleware in recent years.

Type	Authors	Functional Features	Advantages
Distributed data storage	Danish et al. [64]	Make auditable, traceable, and immutable cloud storage decisions	Data traceability, auditability, accountability, integrity
	Ochoa et al. [74]	Decentralized implementation of UbiPri middleware using the Ethereum blockchain	Data integrity and privacy
	Lu et al. [83]	Integrates with data processing technology and distributed message queue technology to implement data collection and storage of the HBase system based on IIoT big data architecture.	Data availability, integrity, and stability
Data Synchronism	Zhou et al. [79]	Allows users to mask the underlying principles of blockchain to query blocks and transactions	Queryable and traceability
	Peng et al. [78]	Extract transactions stored in the underlying blockchain system and efficiently reorganize them into a database	Provide efficient query services for blockchain data and make query data results authentical
	Wang et al. [77]	As an intermediary to facilitate the synchronization of database data to the blockchain	Improves throughput and speed of transaction synchronization and ensures consistency between database and blockchain
	Lian et al. [7]	Provide efficient tamper-proof detection for relational database	Tamper-proof and ensures the integrity, confidentiality, and consistency of data
Function integration	Zupan et al. [86]	Decentralized pub/sub messaging for a multi-federated, licensed environment	Security, validating, and privacy-preserving messaging
	Tapas et al. [76]	Distributed resource access authorization and delegating responsibilities through the Ethereum blockchain network, smart contracts, and Stack4Things	Make the data trusted and auditing
	Ramachandran et al. [66]	A distributed fault-tolerant pub/sub broker with blockchain-based immutability	Avoiding a single point of failure
	Lv et al. [65]	A distributed publish/subscribe model for privacy protection based on blockchain technology to avoid a centralized single point of failure	Confidentiality, privacy preservation, and resistance to DDOS attacks
	Rizzardi et al. [70]	NOS integrated with blockchain to achieve secure and reliable distributed access control for IIoT resource	Integrity and Confidentiality Resist DOS/DDOS attacks Tamper-proof
Security and privacy	Zou et al. [85]	The lowest trust blockchain is used to ensure the security of cloud storage services	Prevent forking attacks and MITM attacks
	Samaniego et al. [87]	Mining is distributed to edge components and is divided into levels	Eliminates the limitation of low computing power
	Sanwar et al. [84]	Provides a delay-sensitive, time-sensitive transaction authentication technology and security and privacy solutions	Minimizing the delay of the transaction, ensuring security and privacy
	Genes et al. [72]	Users can access to easily create blockchain transactions, securing the management of their identity in IIoT	avoiding user impersonation
	Park et al. [71]	Enable smart contracts to automatically validate off-chain operations while supporting data authentication and privacy protection	Provides authentication and privacy preservation

Table 4. *Cont.*

Type	Authors	Functional Features	Advantages
Blockchain IIoT cloud platform	Hasan et al. [73]	The resource of data generated based on blockchain architecture in manufacturing systems can be traced	Data privacy and security
	Liu et al. [80]	Process multi-source heterogeneous data at different stages of the product life cycle and broadcast the processed data to the blockchain network	Data integrity. Supports cross-enterprise access, processing, and analysis of production information

3.3.1. Distributed Data Storage

To achieve high traffic and high concurrency, Lu et al. [83] proposed a middleware framework, namely Hadoop. The middleware layer integrates with a data processing technology (Storm) and a distributed message queue technology (Kafka) to implement data collection and storage of the HBase system. Concerning distributed data storage, Danish et al. [64] proposed a blockchain-based adaptive middleware for IIoT data storage decision selection. In Danish architecture [64], the storage decision and cryptographic hash of the IIoT data are stored on the blockchain network and allow the IIoT application owners in the application layer to audit the decision and data integrity through the adaptive middleware. At the same time, Machine Learning (ML) is applied to make decisions on the storage methods. However, there was no emphasis on users' security and privacy in [64].

3.3.2. Data Synchronism

The synchronization of information between the database and the blockchain is critical. To solve this problem, Zhou et al. [79] proposed a data analysis middleware framework called Ledgerdata Refiner to extract and synchronize transaction data from the blockchain network directly and then parses data relationships to provide unified interfaces for users in the application layer. This middleware, allows users to mask the underlying principles of blockchain to query blocks and transactions. Based on the research of the data on-chain process, Wang et al. [77] proposed a blockchain middleware model, which achieves the efficiency of the IIoT transaction data synchronization. The four-phase model [77] ensures synchronization consistency when the system fails. Peng et al. [78] proposed a Verifiable Query Layer architecture that can effectively reorganize transactions that are recorded in the underlying blockchain system to give application users a variety of query services.

3.3.3. Security and Privacy

A blockchain-based middleware named Amatista was presented by Samaniego et al. [87] for managing the IIoT in a zero-trust mode. Amatista has no trust in the transactions or the infrastructure. It validates both participant resources and the transactions they generate. As a result, the data flow is not only a data-centric reading but also a resource-centric communication that enables access to controlled resources without the usual requirement for a central authority. Furthermore, the hierarchical mining method is also given a context parameter by Amatista. As well, the mining process in [87] is designed on two different levels. For the research on data storage security, Zou et al. [85] proposed a blockchain middleware system to enhance the security of cloud storage, called ChainFS. But there is no mention of heterogeneous device gateways security and low latency validation. While researching identity authentication and access authorization, Genes et al. [72] proposed the Key Management System (KMS) and combined it with Man4Ware [56] to address the identity management problem. In [72], the middleware layer encapsulates APIs, communication protocols, and key management technologies. The application layer can send requests to the middleware through the APIs, and the middleware connects with the blockchain network to complete the creation of a blockchain transaction. Park et al. [71] proposed a blockchain middleware framework called Ziraffe, which can support authentication of origin for external data and

protection of user privacy. The Ziraffe framework consists of four parts: users, Ziraffe in the middleware layer, the blockchain network, and the data resource server. In Ziraffe, programmers can utilize the framework to distribute smart contracts, users can acquire privacy protection according to their credentials through the framework, and the server of the data source supports a middleware-based signature. Users have access to external data sources and are enabled to import values into the blockchain. Finally, when a user downloads data from a data source, the server can confirm the external origin by signing the issue.

3.3.4. Function Integration

Many researchers integrate blockchain technology and create the capabilities to enable advanced services for the application layer of IIoT. Zupan et al. [86] implemented decentralized message publishing/subscription in a multi-federal and permissioned environment. In [86], the application layer communicates to Kafka (a distributed messaging model) of the middleware layer via proxies. The operation performed by publishers and subscribers in the application layer is received by a proxy. Moreover, to validate the operations sent from Kafka, Zupan has modeled the pub/sub semantics using smart contracts in the blockchain network. Lv et al. [65] proposed a blockchain-based privacy-preserving publish/subscribe model. To protect the subscribers' privacy, they used lightweight public key encryption to encrypt topics.

In distributed authorization and business delegation. Tapas et al. [76] proposed a blockchain middleware model that integrates a blockchain-based authorization and delegation mechanism with a middleware, Stack4Things (S4T). In [76], the application layer connects to the middleware layer that contains S4T middleware and its built-in database, and the middleware layer interacts with the blockchain network that encapsulates smart contracts with different functions. Eventually, access to the user is granted or not depending on the result. The user's request is sent to the middleware layer and waits for validation. Then smart contracts on the blockchain network record the resulting data on the chain. As well, the results are returned to the middleware layer and the user's access is confirmed. But in the face of the single point of collapse problem, Tapas does not take it into account. Ramachandran et al. [66] implemented Byzantine fault tolerance on distributed authorization and authentication. On cross-domain problems, integration of the existing Network Smart Objects (NOS) platform with a blockchain network is proposed by Rizzardi et al. [70] to allow decentralized or peer-to-peer operations. In [70], the application layer sends a subscription request to the corresponding NOS unit via the broker. After the processing of resource data and application layer data, the data of different NOSs units are packaged as transactions into a blockchain network through a consensus mechanism. In this way, NOSs can be deployed in an environment where members do not trust each other.

3.3.5. Blockchain IIoT Cloud Platform

Hasan et al. [73] introduced a client middleware of the CMaaS platform that enables the client-side program to submit HTTP requests including model parameter modification, and toolpath regeneration requests, directly to the CMaaS platform. Having considered processing heterogeneous production information across different enterprises, Liu et al. [80] proposed an IIoT blockchain middleware for PLM. The presented framework divides the information flow into three stages, each of which includes different product-related activities such as product design, product production, and warehousing management, among others. Users can conduct a search using the industrial blockchain-based middleware before they need to access the appropriate design files. Then, using the specified application programming interface, users can access additional huge design files. This can boost group decision-making to complete collaborative design activities promptly and accurately. Additionally, it promotes the traceability of particular documentation across several companies.

4. Enablers in Blockchain Middleware

This section focuses on some important enabling technologies for the integration of IIoT middleware with the blockchain network. It is divided into four levels from the scope of blockchain to industrial applications for discussion. According to the architecture of the blockchain middleware mentioned in the previous sections, we put forward the level enabling technical framework of the blockchain middleware, as shown in Figure 5.

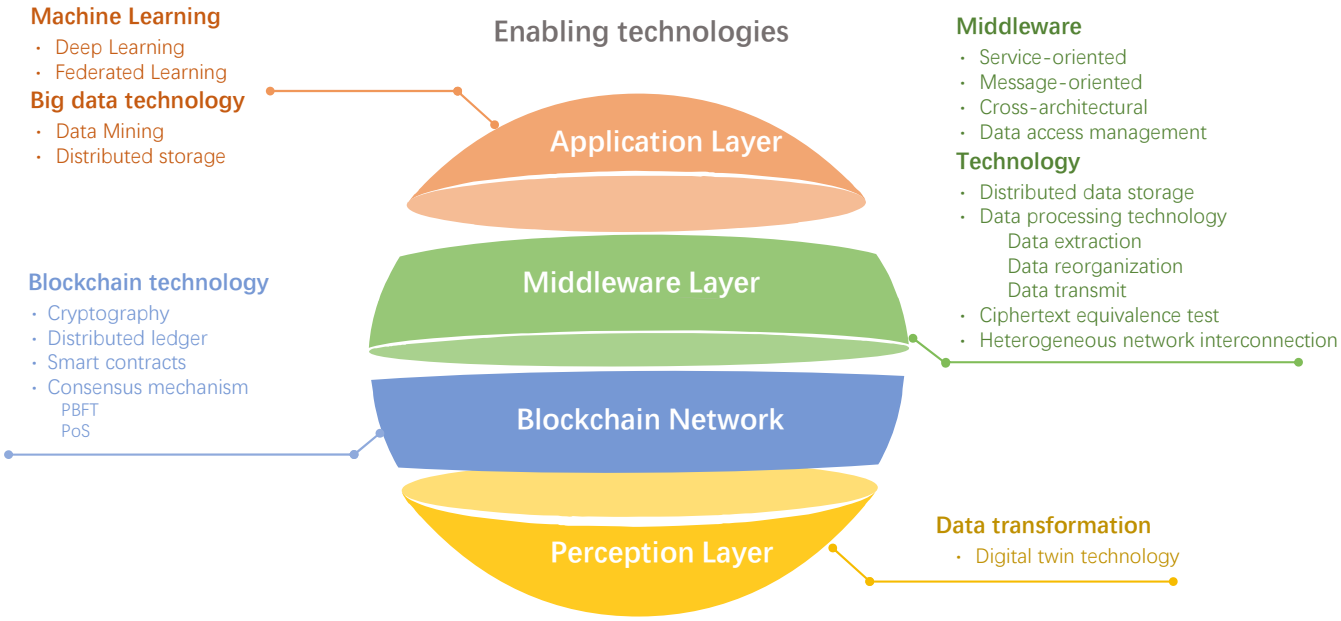

Figure 5. Key enabling technologies in blockchain middleware for IIoT.

4.1. Enablers for the Application Layer

4.1.1. Distributed Machine Learning

The management and processing of increasing data are generating new challenges in the industrial environment [88]. ML as the core of artificial intelligence (AI) technology, can protect data security and data privacy in edge services of IIoT through the integration with blockchain smart contracts [89]. The blockchain network is directly connected to edge nodes as well as IIoT middleware and communicates through the smart contract, which acts as a linkage between ML and blockchain network data interaction. Machine learning algorithms classify off-chain data resources and then store them in the blockchain network through blockchain middleware. In this way, it makes the middleware decision efficiently by classifying raw data as important through a machine learning algorithm [64]. In addition, the efficiency of data processing is improved and the overhead is reduced.

In IIoT, the constant growth of smart devices leads to privacy leakage and insufficient model accuracy of edge services. Another important factor that can have an impact on latency and reliability in industries is quick and efficient computing. To compute and evaluate the massive amounts of data acquired from the different network platforms the IIoT needs strong tools, as mentioned in [90]. Deep Learning (DL), however, is a recent study area in the field of ML. It is included in ML to go towards the original objective (i.e., AI). At the moment, DL-Enabled cloud/edge computing provides intelligent computing infrastructure for IIoT platforms while performing quick and efficient calculations. The utilization of edge-based computing infrastructure is acceptable due to the low power and limited storage of the devices [90].

However, due to insecure access to insufficient or low-quality data, the DL algorithm cannot fully meet the needs of IIoT. Thereby, Google proposed a decentralized DL model named Federated Learning (FL) for secure computing on end-user devices in wireless networks. FL in IIoT networks achieves a collaborative artificial intelligence training model

based on the distributed devices' massive data without moving them into the host server. FL can coordinate distributed computational devices to train collaboratively on a shared prediction/classification task. For instance, Hiessl et al. [91] proposed an FL model for updating knowledge. Similarly, the case study in [92] uses FL to detect anomalies in IIoT. Lu et al. [93] presented a secure data-sharing architecture, which can be combined with FL. This distributed blockchain secure data sharing architecture can model the data sharing into an ML problem. It enables the integration of FL into the permissioned blockchain during the sharing process, which solves the security and privacy issues (e.g., data leakage) in wireless networks and achieves a balance of accuracy, efficiency, and security of data management.

4.1.2. Secure Big Data Analytics

With the advent of 5G, the IIoT has developed rapidly [94]. The massive data generated in smart industrial manufacturing needs to be mined and selected to enable producers to check the process quality of products and workpiece or equipment defects earlier. However, traditional data mining methods are inefficient and the validity of the data is insufficient. From the perspective of ML, Mathias et al. [95] proposed a data mining method to analyze limited samples of electrical signals. They developed an Open Platform Communication (OPC UA)-based simulation IIoT application to monitor the data mining mechanism for welding processes. Wang et al. [94] presented an online support vector machine-based data cleaning approach in the data collection from mobile edge nodes, to maintain information reliability/integrity while reducing the networking bandwidth and energy consumption of industrial sensing data acquisition. In [83], streaming big data processing technology (such as Storm) and big data storage technology (such as HBase) are used to make up the distributed processing blockchain-based middleware.

Based on the existing middleware, integrating with big data processing and storage technology can simplify the processing of off-chain data and reduce the cost of data system maintenance.

4.2. Enablers for the Middleware Layer

Many of the blockchain middleware mentioned in previous sections are integrated with the blockchain network by the IIoT middleware (e.g., Service-oriented middleware, Message-oriented middleware, and Cross-domain middleware), which acts as the underlying technical support of the blockchain middleware. In previous sections, for example, Kafka, a distributed message queue middleware, is integrated with a blockchain network with smart contracts to allow users to audit and validate the consumed data in the pub/sub-system, achieving distributed security. Network Smart Objects (NOS), a kind of cross-domain middleware, integrates with blockchain networks to achieve point-to-point operations across domains for applications in an environment where members do not trust each other [70]. In [56], based on Man4Ware, a blockchain-enabled service-oriented middleware is designed for protecting intelligent manufacturing applications and building trust between the parties involved in the value chain.

In addition to the integration of IIoT middleware, some underlying technologies can also support the integration of blockchain networks with IIoT middleware. They are as shown in Table 5. For instance, some data storage and transmission technology promote middleware to extract and process blockchain network data [74]. Some encryption technology [7,65,71] ensures application data security and privacy and can also reduce system maintenance costs. As well, there are also APIs open for middleware and blockchain network interaction. All these underlying technologies can act as key technologies to support efficient operation and functional integration of blockchain middleware.

Table 5. Enabling technologies for the middleware layer.

Type		Techniques	Functional Features of Integration
Middleware	Service-oriented	Stack4Things [76]	Focus on authentication, authorization, and delegation mechanisms
		Man4Ware [72]	Distributed ledgers created and maintained through the Man4Ware service can be used as a trusted, traceable record and source to verify the correctness of transactions
		UbiPri [74]	User privacy centralized management middleware
	Message-oriented	Kafka [83,86]	Efficiently process data streams in real-time and store them persistently in distributed replication clusters while maintaining high throughput
Security and encryption		SHA-256 [7]	Protect the private data in blockchain middleware and facilitate the retrieval of the data from the blockchain network
		zk-SNARK [71]	A zero-knowledge proof that can perform computations after a validator with weak computations outsources the computation to an unreliable validator and feedback results with evidence that results are correct in off-chain computations.
		PKEwET (Public Key Encryption with Equality Test) primitive [65]	A ciphertext equivalence test to determine whether two ciphertexts encrypted by different public keys are equal without decrypting the ciphertext, effectively reducing user storage costs
		SUNDR protocol [85]	A remote file system to ensure fork consistency to the client and prevent forking attacks
Data processing, storage, and management		Networked smart object (NOS) [70]	Enabled to manage the data provided by heterogeneous sources in a distributed manner and evaluate, utilizing proper algorithms
		Strom [96]	An open-source distributed, scalable, and fault-tolerant real-time computing system to simplify parallel real-time data processing
		HBase [97]	A distributed database has good compatibility with distributed storage, aggregated computing, and random access to massive semi-structured or unstructured data in real-time.
		PostgreSQL [79]	A database can parse out information and reorganize it as a third-party database to provide multiple query functions
Data transmit technology		IPFS [74]	A files system for distributed storage and P2P shared files to implement other middleware modules
		TiDB [77]	Convert database data to key-value pairs for easy storage in the blockchain
Others		SDN-Gateway [84]	Act as a linkage between LLN and blockchain, provide networking control operations, and execute different actions against vulnerabilities and cyberattacks.
		Trinity APIs [66]	Through the APIs, data can be sent to the blockchain to initiate the consensus and block creation process to complete the interaction with the middleware and blockchain network

4.3. Enablers for the Blockchain Network

4.3.1. Consensus Mechanism

Generally, blockchain is a distributed ledger system, and its key issue is consistency. The consensus mechanism is widely used in the distributed system, which allows all the nodes in the blockchain with an accounting problem to agree on an accounting. Unlike the consensus mechanism form of the traditional blockchain (e.g., Bitcoin), in the IIoT blockchain network, blocks are validated by decentralized nodes [98]. IIoT infrastructure that is transformed into virtual digital assets by digital-twin technology can be recorded on the blockchain network in the form of the cryptographic hash value. All manufacturing processed events are registered by the machine tools onto the blockchain as transactions [99]. In this way, users can take the initiative in the blockchain through the token they hold. This is different from the traditional consensus algorithm, like PoW. By contrast, it can reduce the power cost of industrial computing equipment to a certain extent.

Furthermore, some IIoT middleware can also integrate certain consensus algorithms like PBFT to achieve distributed fault tolerance, and realize distributed message distribution broker, avoiding a single point of collapse. Ramachandran et al. [66] implemented Byzantine fault tolerance on distributed authorization and authentication to avoid central points of failure. For the integration of the PBFT consensus algorithm, the distributed middleware can expose a set of APIs to interact with a blockchain following the interface architecture. As well, they can utilize the consensus mechanism of a blockchain network to realize distributed fault-tolerances.

4.3.2. Smart Contracts

Smart contract in the blockchain is trackable, secure, and unalterable. It can be built based on a distributed ledger to achieve authentication and access control without the third party and be scripts stored in the blockchain [100]. The off-chain resource can interact with blockchain network data through smart contracts [101]. Unlike the Bitcoin finance system, smart contracts in IIoT deal with transactions of virtual digital assets converted by industrial infrastructure entities. Once manufacturers deploy a smart contract, they are permitted to store the hash of the latest industrial entity updating on the blockchain. Then they can retrieve the industrial entity, and request interesting production information. In addition, the blockchain network where cryptographic token for pay-as-you work paves the way for a community of manufacturing and product services among IIoT devices. Furthermore, in the onchain-off-chain interaction process, the authentication of the data feed is necessary. For instance, Town Crier was one of the first works to look at authenticated linking smart contracts to external off-chain HTTPS-enabled data resources [102].

4.3.3. Cryptography and Distributed Ledger

As the core technology of blockchain, cryptography and distributed ledger support the data entry and storage of blockchain. The underlying data architecture is determined by blockchain cryptography. The packaged data blocks are processed into a chain structure using cryptography's hash functions. Because the hash algorithm is unidirectional and tamper-resistant, the data can not be tampered with and can be traced only in the blockchain network. In addition, accounts in the blockchain network will be encrypted by asymmetric encryption, thus ensuring the security of data. Distributed ledger builds the framework of blockchain. It is essentially a distributed database. When a piece of data is generated, it will be stored in this database after everyone processes it, so distributed ledger plays the role of data storage in the blockchain.

Blockchain middleware can utilize cryptography and distributed ledger to achieve traceability of historical data, auditing, and data security (in Figure 6). Commonly, in the applications of the manufacturing sector, the distributed ledger includes a series of transactions capturing manufacturing event data associated with machine tools. As well, the set of all transactions can represent a chain of manufacturing events for a product. The blockchain middleware utilizes encapsulated data extraction and data processing

techniques to interact with transaction data from a distributed ledger database. At the same time, blocks of data packaged using cryptography are recorded into the blockchain network as key-value pairs, increasing the capacity of data storage and ensuring the security of IIoT middleware.

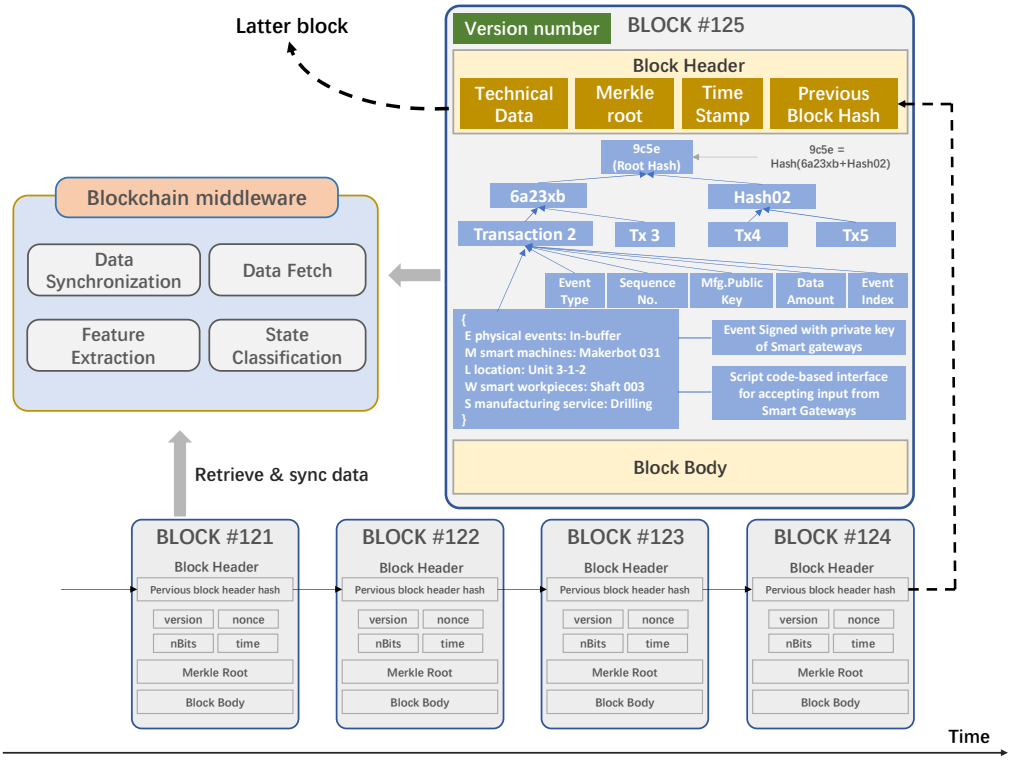

Figure 6. Illustration of Blockchain data structure storage.

4.4. Digital Transformation for the Perception Layer

In IIoT, as for the record and synchronization of manufacturing data, the original raw data are usually not stored directly in the blockchain, in which a digital twin system is built to realize the transformation of industrial infrastructure from physical/digital data into blockchained assets [103–105].

On the simplification of manufacturing information into data-tag of limited spaces, Leng et al. adopted an abbreviation schema to accommodate this limitation [106]. Through a mapping algorithm, the digital twin identification of the data tag on each IIoT entity is linked to the corresponding blockchain transaction on the blockchain network, and it is the anchor for obtaining the entity's lifecycle activities [107]. In the interaction (synchronization) process between the cyber and physical space of the IIoT, it illustrates a lifecycle digital twin model of individualized products [108]. The data tag is a mapping to its associated digital twin [109]. By collecting the transactions of workpieces/products' related events, the digital twin of products is therefore securitized for lifecycle tracking. Thus, users can interact with a digital twin model on their demands via the middleware layer. When the users invoke the blockchain middleware interface to send off manufacturing data, transactions reveal a continuous trail of the products being fabricated.

5. Research Directions

Based on the discussion of enabling technologies in the previous section, we offer some suggestions for research directions according to the four-layer architecture (in Figure 7). It is expected that it lays a foundation for making IIoT blockchain middleware a new venue for Industry 5.0 research innovation.

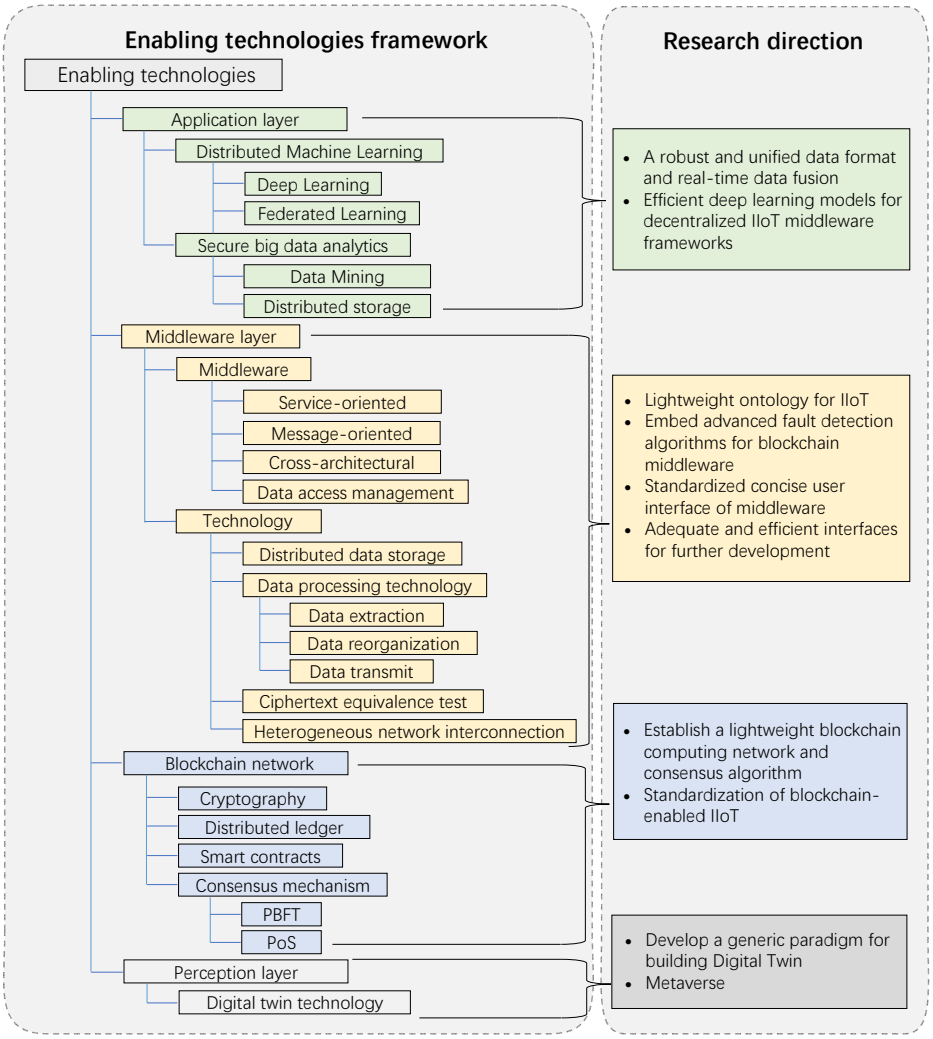

Figure 7. Research direction framework of blockchain middleware for IIoT.

5.1. Directions for the Application Layer

5.1.1. A robust and Unified Data Format and Real-Time Data Fusion

Information is distributed among multiple devices and is difficult to aggregate due to geographical or mapping barriers. A robust and cost-effective data format, as well as an integration method, is desirable [110] for managing data to achieve resilient manufacturing for Industry 5.0. The integration of Information Communication Technologies (ICT) into the industrial Internet of Things framework is also a favorable development direction for real-time data fusion [111], such as data preparation, crawl scheduling, multi-level indexing, and human and machine query.

5.1.2. Efficient Deep Learning Models for Decentralized IIoT Middleware Frameworks

Concerning the overall complexity of management issues and the finite storage and computation capabilities of the IIoT devices, existing implementations of distributed machine learning based on edge design uses additional optimization information to obtain higher productivity, self-organization capabilities, lower running times, and energy consumption [112,113]. For instance, federated learning (FL, also termed federated machine learning) has been proposed to coordinate distributed computational devices to train collaboratively on a shared prediction/classification task. However, the implementation of the FL in the smart industry is still not simple, and future research directions need to identify a better way to manage distributed computing resources to meet the needs of complex IIoT environments in Industry 5.0.

5.2. Directions for the Middleware Layer

5.2.1. Lightweight Ontology for IIoT

In integrating a blockchain-based data sharing framework to preserve security and privacy [114], IIoT interoperability affects its scalability and performance [115]. When a large number of machines interact in industrial networks [116], provisioning interoperability in IIoT from semantic conflicts, global heterogeneity, and new/unknown devices is of significance for achieving resilience due to lacking standard architecture, in which ontology methods are useful [117]. Existing ontology-based semantic approaches are cumbersome for satisfying resource flexibility needs. Therefore, in the processing of distributed middleware sensory data, designing a lightweight ontology for decentralized IIoT so that semantic interoperability will save the processing and annotation time, which is in urgent need for achieving resilient manufacturing towards Industry 5.0.

5.2.2. Embed Advanced Fault Detection Algorithms for Blockchain Middleware

As increasingly heterogeneous devices are involved in the decentralized IIoT, the possibilities of failures and faults increase [118]. Blockchain middleware for decentralized IIoT is supposed to be robust in not only detecting and withstanding failures but also detecting faults promptly. Advanced self-configured fault detection algorithms should be embedded into the blockchain middleware for efficiently and securely coordinating different devices. Accuracy and timeliness in detecting faults will accelerate the industrial process in achieving system resilience towards Industry 5.0.

5.2.3. Standardized Concise User Interface of Middleware

The user interface of the blockchain middleware is supposed to be as concise as possible so that engineers with different implementation fields are aware of the IIoT application he/she is using [118]. In the distributed environment, engineers will be adopting or operating the industrial blockchain with limited knowledge of networking and communications. Seamless integration of the decentralized IIoT with a user-friendly interface for blockchain middleware will help its acceptance, facilitating users to do the work without the complex underlying principles.

5.2.4. Adequate and Efficient Interfaces for Further Development

Developing efficient interfaces can not only enrich the functions of middleware but also facilitate the development and deployment of middleware and reduce the coupling between codes. For example, in ledger data analysis middleware, providing a sufficient interface for further function development can promote searching blocks or transactions efficiently. Design interfaces in databases or decentralized file sharing systems can solve the low-quality data issues in smart manufacturing [119]. Design adequate API interfaces to support more complicated SQL queries and integrate more diverse databases as well as blockchain systems.

5.3. Directions for the Blockchain Network

5.3.1. Establish a Lightweight Blockchain Computing Network and Consensus Algorithm

Introducing blockchain into the decentralized IIoT suffers from two obvious disadvantages. First, time latency in industrial controls is at a microsecond level [120], while the blockchain network usually cannot satisfy microsecond resolution demands in IIoT. Second, controllers in current IIoT devices are generally of low performance and limited storage spaces. Collecting massive industrial data into blockchain nodes hosting the IIoT devices may result in the collapse of the entire network, and thereby is impossible under this circumstance. Therefore, integrating blockchain with middleware should be lightweight to solve the storage and performance issues.

Existing consensus methods usually rely on costly computing tasks and puzzles to make the participants liberally add new blocks to a blockchain [121]. However, in industrial applications, the need for crash fault tolerance is much higher than that for

Byzantine fault tolerance. Innovations in storage structure and consensus mechanism for industrial usage should be performed to improve the throughput [122,123]. Establishing an effective lightweight consensus algorithm in IIoT systems for industrial applications is a future direction for improving the efficiency of the IIoT blockchain network under disruptions or disturbances.

5.3.2. Standardization of Blockchain-Enabled IIoT

Standardizing blockchain middleware for decentralized IIoT, as well as synchronizing with existing standards, is still in its early stages. Without clear regulations, coordination between different IIoT blockchain systems is challenging [124]. Blockchain middleware standards are supposed to provide guidelines for either developers or engineering clients. Furthermore, blockchained smart contracts are supposed to be legally enforceable for eliminating conflicts between participants. Although the integration of IIoT middleware with blockchain networks has inherent security features, there are still some exploitable loopholes in smart contracts in blockchain networks.

5.4. Directions for the Perception Layer

5.4.1. Develop a Generic Paradigm for Building Digital Twin

A unified data model or a generic Digital Twin architecture is in great need for digital asset/information conversion, concerning a lack of consensus on how to build a Digital Twin system for heterogeneous systems in a distributed IIoT network [125]. Therefore, designing a new paradigm for establishing a Digital Twin is supposed to be a generic paradigm of implementing a basic Digital Twin system more compatible with IIoT blockchain middleware.

5.4.2. Metaverse

According to Dr. Yu Yuan's definition, the Metaverse may refer to a kind of experience in which the outside world is perceived by the users (human or non-human) as being a universe that is built upon digital technologies as a different universe ("Virtual Reality"), a digital extension of our current universe ("Augmented Reality" or "Mixed Reality"), or a digital counterpart of our current universe ("Digital Twin"). Named after the universe, a metaverse shall be persistent and should be massive, comprehensive, immersive, and self-consistent. Described as "meta", a metaverse should be ultra-realistic, accessible, pervasive, and may be decentralized. In a narrow sense, metaverse may be simply defined as Persistent Virtual Reality (PVR). In a broad sense, the metaverse is the advanced stage and long-term vision of Digital Transformation.

Metaverse may be a promising research direction for the development of blockchain middleware [126]. The biggest difference between Industry 4.0 and the era of steam engines, electrification, and information technology is that the concept of Industry 4.0 places more emphasis on intelligence and the use of digital technology to minimize human involvement in the entire production process (i.e., the link between automated equipment and IT systems, which originally required human involvement, can be completed automatically without the need for human participation). In fact, under the concept of the digital twin. The human is only responsible for building the virtual world and defining the way of data collection, management and optimization, and then a continuous learning, optimization, and intelligent interaction will be formed between the physical space and the virtual space, and the role of the human is to supervise this association to keep it undefined and normal. Therefore, the Metaverse may be a promising research direction for the development of blockchain middleware for enhancing system resilience.

6. Concluding Remarks

This paper presented a review of secure blockchain middleware for decentralized IIoT towards Industry 5.0. The security issues of conventional IIoT solutions and the advantages of blockchain middleware are analyzed. Key enabling technologies in blockchain

middleware are categorized respectively based on the corresponding layers, namely, the perception layer, the blockchain network, the middleware layer, and the application layer. The application of digital transformation in blockchain middleware is discussed. Future research directions for blockchain middleware in IIoT are outlined. The purpose of this paper is to research and analyze the abilities of distributed blockchain middleware to minimize the threat of a single point of failure in the context of resilient manufacturing in Industry 5.0. Compared with the traditional centralized IIoT, the distributed characteristics of secure blockchain middleware are more resistant to various disturbances (e.g., security issues) or other unknown factors in the industrial manufacturing environment, and can play an essential role in Industry 5.0 resilient manufacturing. It is expected that the paper lays a solid foundation for making IIoT blockchain middleware a new venue for Industry 5.0 research.

Author Contributions: Conceptualization, J.L. and D.Z.; methodology, J.L.; formal analysis, Z.C.; investigation, Z.C. and Z.H.; writing—original draft preparation, J.L., Z.C., Z.H., X.Z., H.S. and Z.L.; writing—review and editing, J.L. and D.Z.; supervision, J.L.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant No. 52075107, U20A6004 and 72271067; Natural Science Fund of Guangdong Province under Grant No. 2022B1515020006; the State Administration of Science, Technology and Industry for National Defense, PRC under Grant No. JCKY2020209B005; and the Shenzhen Special Fund for the Development of Strategic Emerging Industries under Grant No. JCYJ20170818100156260.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

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

References

1. Müller, J. Enabling Technologies for Industry 5.0. 2020. Available online: https://www.4bt.us/wp-content/uploads/2021/04/INDUSTRY-5.0.pdf (accessed on 19 July 2022).
2. Breque, M.; De Nul, L.; Petridis, A. Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry. 2021. Available online: https://msu.euramet.org/current_calls/documents/EC_Industry5.0.pdf (accessed on 19 July 2022).
3. Da Xu, L.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
4. Li, S.; Zhao, S.; Yang, P.; Andriotis, P.; Xu, L.; Sun, Q. Distributed Consensus Algorithm for Events Detection in Cyber-Physical Systems. *IEEE Internet Things J.* **2019**, *6*, 2299–2308. [CrossRef]
5. Latif, S.; Idrees, Z.; e Huma, Z.; Ahmad, J. Blockchain Technology for the Industrial Internet of Things: A Comprehensive Survey on Security Challenges, Architectures, Applications, and Future Research Directions. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4337. [CrossRef]
6. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on Blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
7. Lian, J.; Wang, S.; Xie, Y. TDRB: An Efficient Tamper-Proof Detection Middleware for Relational Database Based on Blockchain Technology. *IEEE Access* **2021**, *9*, 66707–66722. [CrossRef]
8. Leng, J.; Zhou, M.; Zhao, J.L.; Huang, Y.; Bian, Y. Blockchain Security: A Survey of Techniques and Research Directions. *IEEE Trans. Serv. Comput.* **2022**, *15*, 2490–2510. [CrossRef]
9. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
10. Sun, Q.; Wang, N.; Li, S.; Zhou, H. Local Spatial Obesity Analysis and Estimation Using Online Social Network Sensors. *J. Biomed. Inform.* **2018**, *83*, 54–62. [CrossRef] [PubMed]
11. Yli-Ojanperä, M.; Sierla, S.; Papakonstantinou, N.; Vyatkin, V. Adapting an Agile Manufacturing Concept to the Reference Architecture Model Industry 4.0: A Survey and Case Study. *J. Ind. Inf. Integr.* **2018**, *15*, 147–160. [CrossRef]
12. Zhou, B.; Maines, C.; Tang, S.; Shi, Q.; Yang, P.; Yang, Q.; Qi, J. A 3-D Security Modeling Platform for Social IoT Environments. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 1174–1188. [CrossRef]
13. Bukkapatnam, S.T.; Lakhtakia, A.; Kumara, S.R. Analysis of Sensor Signals Shows Turning on a Lathe Exhibits Low-Dimensional Chaos. *Phys. Rev. E* **1995**, *52*, 2375–2387. [CrossRef] [PubMed]
14. Yang, H.; Kumara, S.; Bukkapatnam, S.T.; Tsung, F. The internet of Things for Smart Manufacturing: A Review. *IISE Trans.* **2019**, *51*, 1190–1216. [CrossRef]

15. Leng, J.; Chen, Z.; Sha, W.; Ye, S.; Liu, Q.; Chen, X. Cloud-Edge Orchestration-Based Bi-Level Autonomous Process Control for Mass Individualization of Rapid Printed Circuit Boards Prototyping Services. *J. Manuf. Syst.* **2022**, *63*, 143–161. [CrossRef]
16. Issarny, V.; Georgantas, N.; Hachem, S.; Zarras, A.; Vassiliadist, P.; Autili, M.; Gerosa, M.A.; Hamida, A.B. Service-Oriented Middleware for the Future Internet: State of the Art and Research Directions. *J. Internet Serv. Appl.* **2011**, *2*, 23–45. [CrossRef]
17. Zeng, J.; Yang, L.T.; Lin, M.; Ning, H.; Ma, J. A Survey: Cyber-Physical-Social Systems and Their System-Level Design Methodology. *Future Gener. Comput. Syst.* **2020**, *105*, 1028–1042. [CrossRef]
18. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
19. Xu, H.; Yu, W.; Griffith, D.; Golmie, N. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access* **2018**, *6*, 78238–78259. [CrossRef]
20. Jayalaxmi, P.; Saha, R.; Kumar, G.; Kumar, N.; Kim, T.-H. A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges. *IEEE Access* **2021**, *9*, 25344–25359. [CrossRef]
21. Jose, A.C.; Malekian, R. Improving Smart Home Security: Integrating Logical Sensing into Smart Home. *IEEE Sens. J.* **2017**, *17*, 4269–4286. [CrossRef]
22. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
23. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context Aware Computing for The Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 414–454. [CrossRef]
24. Silva, B.N.; Khan, M.; Han, K. Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges. *IETE Technol. Rev.* **2017**, *35*, 205–220. [CrossRef]
25. 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]
26. Latif, S.; Zou, Z.; Idrees, Z.; Ahmad, J. A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network. *IEEE Access* **2020**, *8*, 89337–89350. [CrossRef]
27. Muhammad, F.; Anjum, W.; Mazhar, K.S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6.
28. Mohamed, N.; Al-Jaroodi, J. A Survey on Service-Oriented Middleware for Wireless Sensor Networks. *Serv. Oriented Comput. Appl.* **2011**, *5*, 71–85. [CrossRef]
29. Mohiuddin, I.; Almogren, A. Workload Aware VM Consolidation Method in Edge/Cloud Computing for Iot Applications. *J. Parallel Distrib. Comput.* **2019**, *123*, 204–214. [CrossRef]
30. Alam, M.G.R.; Hassan, M.M.; Uddin, M.Z.; Almogren, A.; Fortino, G. Autonomic Computation Offloading in Mobile Edge for Iot Applications. *Future Gener. Comput. Syst.* **2019**, *90*, 149–157. [CrossRef]
31. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2019**, *149*, 102481. [CrossRef]
32. Attri, T.; Bhushan, B. Enabling Technologies, Attacks, and Machine Learning-Based Countermeasures for IoT and IIoT. In *Integration of WSNs into Internet of Things*; CRC Press: Boca Raton, FL, USA, 2021; pp. 249–272. [CrossRef]
33. Pal, S.; Jadidi, Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. *Appl. Sci.* **2021**, *11*, 9393. [CrossRef]
34. Ghadge, A.; Kara, M.E.; Moradlou, H.; Goswami, M. The Impact of Industry 4.0 Implementation on Supply Chains. *J. Manuf. Technol. Manag.* **2020**, *31*, 669–686. [CrossRef]
35. Müller, J.M.; Veile, J.W.; Voigt, K.-I. Prerequisites and Incentives for Digital Information Sharing in Industry 4.0—An International Comparison Across Data Types. *Comput. Ind. Eng.* **2020**, *148*, 106733. [CrossRef]
36. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of Things (Iot) Security: Current Status, Challenges and Prospective Measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
37. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.
38. Yang, J.C.; Fang, B.X. Security Model and Key Technologies for the Internet of Things. *J. China Univ. Posts Telecommun.* **2011**, *18*, 109–112. [CrossRef]
39. Xiao, B.; Chen, W.; He, Y.; Sha, E.M. An Active Detecting Method Against SYN Flooding Attack. In Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), Fukuoka, Japan, 20–22 July 2005; Volume 1, pp. 709–715.
40. Ahemd, M.M.; Shah, M.A.; Wahid, A. IoT Security: A Layered Approach for Attacks & Defenses. In Proceedings of the 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 104–110.
41. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure Routing for Internet of Things: A Survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [CrossRef]
42. Pongle, P.; Chavan, G. A Survey: Attacks on RPL and 6LoWPAN in IoT. In Proceedings of the 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 8–10 January 2015; pp. 1–6.

43. Elkhodr, M.; Shahrestani, S.; Cheung, H. The Internet of Things: Vision & Challenges. In Proceedings of the IEEE 2013 Tencon-Spring, Sydney, NSW, Australia, 17–19 April 2013; pp. 218–222.
44. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture, And Business Models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
45. Guinard, D.; Trifa, V.; Karnouskos, S.; Spiess, P.; Savio, D. Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services. *IEEE Trans. Serv. Comput.* **2010**, *3*, 223–235. [CrossRef]
46. O'Leary, D.E. 'Big Data', The 'Internet of Things' and the 'Internet of Signs. *Intell. Syst. Account. Financ. Manag.* **2013**, *20*, 53–65. [CrossRef]
47. Yan, Z.; Zhang, P.; Vasilakos, A.V. A Survey on Trust Management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
48. Li, S.; Xu, L.D.; Zhao, S. The Internet of Things: A Survey. *Inf. Syst. Front.* **2015**, *17*, 243–259. [CrossRef]
49. Gupta, B.B.; Tewari, A.; Jain, A.K.; Agrawal, D.P. Fighting Against Phishing Attacks: State of the Art and Future Challenges. *Neural Comput. Appl.* **2016**, *28*, 3629–3654. [CrossRef]
50. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security Threats and Issues in Automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.
51. Babar, S.; Mahalle, P.; Stango, A.; Prasad, N.; Prasad, R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 420–429.
52. Pal, S.; Hitchens, M.; Varadharajan, V. Modeling Identity for the Internet of Things: Survey, Classification and Trends. In Proceedings of the 2018 12th International Conference on Sensing Technology (ICST), Limerick, Ireland, 4–6 December 2018; pp. 45–51.
53. Sarma, A.C.; Girão, J. Identities in the Future Internet of Things. *Wirel. Pers. Commun.* **2009**, *49*, 353–363. [CrossRef]
54. Lhaksmana, K.M.; Murakami, Y.; Ishida, T. Analysis of Large-Scale Service Network Tolerance to Cascading Failure. *IEEE Internet Things J.* **2016**, *3*, 1159–1170. [CrossRef]
55. Lhaksmana, K.M.; Murakami, Y.; Ishida, T. Cascading Failure Tolerance in Large-Scale Service Networks. In Proceedings of the 2015 IEEE International Conference on Services Computing, New York, NY, USA, 27 June–2 July 2015; pp. 1–8.
56. Mohamed, N.; Al-Jaroodi, J. Applying Blockchain in Industry 4.0 Applications. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0852–0858.
57. Leng, J.; Ruan, G.; Jiang, P.; Xu, K.; Liu, Q.; Zhou, X.; Liu, C. Blockchain-Empowered Sustainable Manufacturing and Product Lifecycle Management in Industry 4.0: A Survey. *Renew. Sustain. Energy Rev.* **2020**, *132*, 110112. [CrossRef]
58. Razzaque, M.A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for Internet of Things: A Survey. *IEEE Internet Things J.* **2015**, *3*, 70–95. [CrossRef]
59. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT Middleware: A Survey on Issues and Enabling Technologies. *IEEE Internet Things J.* **2017**, *4*, 1–20. [CrossRef]
60. Fremantle, P.; Scott, P. A Survey of Secure Middleware for the Internet of Things. *PeerJ Comput. Sci.* **2017**, *3*, e114. [CrossRef]
61. Hassan, A. Lightweight Cryptography for the Internet of Things. In Proceedings of the Future Technologies Conference (FTC) 2020, Vancouver, BC, Canada, 5–6 November 2020; Arai, K., Kapoor, S., Bhatia, R., Eds.; Advances in Intelligent Systems and Computing. Springer: Cham, Switzerland, 2020. [CrossRef]
62. Lyu, X.; Ni, W.; Tian, H.; Liu, R.P.; Wang, X.; Giannakis, G.B.; Paulraj, A. Optimal Schedule of Mobile Edge Computing for Internet of Things Using Partial Information. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2606–2615. [CrossRef]
63. Atlam, H.F.; Alenezi, A.; Alharthi, A.; Walters, R.J.; Wills, G.B. Integration of cloud Computing with Internet of Things: Challenges and Open Issues. In Proceedings of the 2017 IEEE International Conference on Internet of Things (Ithings) and IEEE Green Computing and Communications (Greencom) and IEEE Cyber, Physical and Social Computing (Cpscom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 670–675.
64. Danish, S.M.; Assoc, C.M. A Blockchain-Based Adaptive Middleware for Large Scale Internet of Things Data Storage Selection. In Proceedings of the Middleware'19: 20th International Middleware Conference Doctoral Symposium, Davis, CA, USA, 9–13 December 2019; pp. 17–19.
65. Lv, P.; Wang, L.; Zhu, H.; Deng, W.; Gu, L. An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains. *IEEE Access* **2019**, *7*, 41309–41314. [CrossRef]
66. Ramachandran, G.S.; Wright, K.L.; Zheng, L.; Navaney, P.; Naveed, M.; Krishnamachari, B.; Dhaliwal, J. Trinity: A Byzantine Fault-Tolerant Distributed Publish-Subscribe System with Immutable Blockchain-Based Persistence. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 227–235.
67. Kshetri, N. Can Blockchain Strengthen the Internet of Things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
68. Al-Jaroodi, J.; Mohamed, N. Service-Oriented Middleware: A Survey. *J. Netw. Comput. Appl.* **2012**, *35*, 211–220. [CrossRef]
69. Leng, J.; Yan, D.; Liu, Q.; Xu, K.; Zhao, J.L.; Shi, R.; Wei, L.; Zhang, D.; Chen, X. ManuChain: Combining Permissioned Blockchain with a Holistic Optimization Model as Bi-Level Intelligence for Smart Manufacturing. *IEEE Trans. Syst. Man, Cybern. Syst.* **2019**, *50*, 182–192. [CrossRef]
70. Rizzardi, A.; Sicari, S.; Miorandi, D.; Coen-Porisini, A. Securing the Access Control Policies to the Internet of Things Resources Through Permissioned Blockchain. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6934. [CrossRef]

71. Park, J.; Kim, H.; Kim, G.; Ryou, J. Smart Contract Data Feed Framework for Privacy-Preserving Oracle System on Blockchain. *Computers* **2020**, *10*, 7. [CrossRef]
72. Duran, R.G.; Yarleque-Ruesta, D.; Belles-Munoz, M.; Jimenez-Viguer, A.; Munoz-Tapia, J.L. An Architecture for Easy Onboarding and Key Life-Cycle Management in Blockchain Applications. *IEEE Access* **2020**, *8*, 115005–115016. [CrossRef]
73. Hasan, M.; Starly, B. Decentralized Cloud Manufacturing-As-A-Service (Cmaas) Platform Architecture with Configurable Digital Assets. *J. Manuf. Syst.* **2020**, *56*, 157–174. [CrossRef]
74. Ochôa, I.S.; Silva, L.A.; de Mello, G.; da Silva, B.A.; de Paz, J.F.; González, G.V.; Garcia, N.M.; Leithardt, V.R.Q. PRICHAIN: A Partially Decentralized Implementation of UbiPri Middleware Using Blockchain. *Sensors* **2019**, *19*, 4483. [CrossRef]
75. Underwood, S. Blockchain Beyond Bitcoin. *Commun. ACM* **2016**, *59*, 15–17. [CrossRef]
76. Tapas, N.; Merlino, G.; Longo, F. Blockchain-based IoT-cloud authorization and delegation. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 411–416.
77. Wang, N.; Wang, B.; Liu, T.; Li, W.; Yang, S. A Middleware Approach to Synchronize Transaction Data to Blockchain. In Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; pp. 1–8.
78. Peng, Z.; Wu, H.; Xiao, B.; Guo, S. VQL: Providing Query Efficiency and Data Authenticity in Blockchain Systems. In Proceedings of the 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW), Macao, China, 8–12 April 2019; pp. 1–6.
79. Zhou, E.; Sun, H.; Pi, B.; Sun, J.; Yamashita, K.; Nomura, Y. Ledgerdata Refiner: A Powerful Ledger Data Query Platform for Hyperledger Fabric. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 433–440.
80. Liu, X.; Wang, W.; Guo, H.; Barenji, A.V.; Li, Z.; Huang, G.Q. Industrial Blockchain Based Framework for Product Lifecycle Management in Industry 4.0. *Robot. Comput. Manuf.* **2019**, *63*, 101897. [CrossRef]
81. Maxim, J. Onename Launches Blockchain Identity Product Passcard. *Bitcoin Mag.* **2015**. Available online: https://bitcoinmagazine.com/business/onename-launches-blockchain-identity-product-passcard-1431548450 (accessed on 19 July 2022).
82. Takahashi, R. *How Can Creative Industries Benefit from Blockchain?* McKinsey & Company: Hong Kong, China, 2017; Available online: http://bloomen.io/portfolio-item/mckinsey-can-creative-industries-benefit-blockchain/ (accessed on 19 July 2022).
83. Lu, Y.; Fu, Q.; Xi, X.; Chen, Z. Cloud Data Acquisition and Processing Model Based on Blockchain. *J. Intell. Fuzzy Syst.* **2020**, *39*, 5027–5036. [CrossRef]
84. Zupan, N.; Zhang, K.W.; Jacobsen, H.A. Demo: Hyperpubsub: A Decentralized, Permissioned, Publish/Subscribe Service Using Blockchains. In Proceedings of the Middleware '17: 18th International Middleware Conference, Las Vegas, NV, USA, 11–15 December 2017; pp. 15–16.
85. Tang, Y.; Zou, Q.; Chen, J.; Li, K.; Kamhoua, C.A.; Kwiat, K.; Njilla, L. ChainFS: Blockchain-Secured Cloud Storage. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 987–990.
86. Samaniego, M.; Deters, R. Zero-Trust Hierarchical Management in IoT. In Proceedings of the 2018 IEEE International Congress on Internet of Things (ICIOT), Bhimtal, India, 23–24 February 2018; pp. 88–95.
87. Hosen, A.S.M.S.; Singh, S.; Sharma, P.K.; Ghosh, U.; Wang, J.; Ra, I.-H.; Cho, G.H. Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network. *IEEE Access* **2020**, *8*, 117266–117277. [CrossRef]
88. Walas, F.; Redchuk, A. IIoT/IoT and Artificial Intelligence/Machine Learning as a Process Optimization Driver under Industry 4.0 Model. *J. Comput. Sci. Technol.* **2021**, *21*, e15. [CrossRef]
89. Tian, Y.; Li, T.; Xiong, J.; Bhuiyan, M.Z.A.; Ma, J.; Peng, C. A Blockchain-Based Machine Learning Framework for Edge Services in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1918–1929. [CrossRef]
90. Khalil, R.A.; Saeed, N.; Masood, M.; Fard, Y.M.; Alouini, M.-S.; Al-Naffouri, T.Y. Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications. *IEEE Internet Things J.* **2021**, *8*, 11016–11040. [CrossRef]
91. Hiessl, T.; Schall, D.; Kemnitz, J.; Schulte, S. Industrial Federated Learning—Requirements and System Design. In Proceedings of the PAAMS 2020: Highlights in Practical Applications of Agents, Multi-Agent Systems, and Trust-worthiness, the PAAMS Collection, L'Aquila, Italy, 7–9 October 2020; Communications in Computer and Information Science. Springer: Cham, Switzerland, 2020; Volume 1233. [CrossRef]
92. Liu, Y.; Garg, S.; Nie, J.; Zhang, Y.; Xiong, Z.; Kang, J.; Hossain, M.S. Deep Anomaly Detection for Time-Series Data in Industrial Iot: A Communication-Efficient on-Device Federated Learning Approach. *IEEE Internet Things J.* **2020**, *8*, 6348–6358. [CrossRef]
93. 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]
94. Wang, T.; Ke, H.; Zheng, X.; Wang, K.; Sangaiah, A.K.; Liu, A. Big Data Cleaning Based on Mobile Edge Computing in Industrial Sensor-Cloud. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1321–1329. [CrossRef]
95. Mathias, S.G.; Schmied, S.; Grossmann, D. Monitoring of Discrete Electrical Signals from Welding Processes Using Data Mining and Iiot Approaches. In Proceedings of the 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI), Baltimore, MD, USA, 9–11 November 2020; pp. 911–916.
96. Rahmstorf, S. Rising hazard of storm-surge flooding. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 11806–11808. [CrossRef]

97. Yang, F.; Milosevic, D.; Cao, J. Optimising Column Family for OLAP Queries in HBase. *Int. J. Big Data Intell.* **2017**, *4*, 23–35. [CrossRef]
98. Leng, J.; Jiang, P.; Xu, K.; Liu, Q.; Zhao, J.L.; Bian, Y.; Shi, R. Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing. *J. Clean. Prod.* **2019**, *234*, 767–778. [CrossRef]
99. *ERC-721*; Non-Fungible Token Standard. Ethereum Foundation: Zuger, Switzerland, 2018.
100. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
101. Leng, J.; Sha, W.; Lin, Z.; Jing, J.; Liu, Q.; Chen, X. Blockchained Smart Contract Pyramid-Driven Multi-Agent Autonomous Process Control for Resilient Individualised Manufacturing Towards Industry 5.0. *Int. J. Prod. Res.* **2022**, 1–20. [CrossRef]
102. Zhang, F.; Cecchetti, E.; Croman, K.; Juels, A.; Shi, E. Town Crier: An Authenticated Data Feed for Smart Contracts. In Proceedings of the CCS'16: 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 270–282.
103. Liu, Q.; Zhang, H.; Leng, J.; Chen, X. Digital Twin-Driven Rapid Individualised Designing of Automated Flow-Shop Manufacturing System. *Int. J. Prod. Res.* **2018**, *57*, 3903–3919. [CrossRef]
104. Leng, J.; Chen, Z.; Sha, W.; Lin, Z.; Lin, J.; Liu, Q. Digital Twins-Based Flexible Operating of Open Architecture Production Line for Individualized Manufacturing. *Adv. Eng. Inform.* **2022**, *53*, 101676. [CrossRef]
105. Leng, J.; Zhou, M.; Xiao, Y.; Zhang, H.; Liu, Q.; Shen, W.; Su, Q.; Li, L. Digital Twins-Based Remote Semi-Physical Commissioning of Flow-Type Smart Manufacturing Systems. *J. Clean. Prod.* **2021**, *306*, 127278. [CrossRef]
106. Leng, J.; Jiang, P.; Liu, C.; Wang, C. Contextual Self-Organizing of Mass Individualization Process Under Social Manufacturing Paradigm: A Cyber–Physical–Social System Approach. *Enterp. Inf. Syst.* **2018**, *14*, 1124–1149. [CrossRef]
107. Zhao, R.; Yan, D.; Liu, Q.; Leng, J.; Wan, J.; Chen, X.; Zhang, X. Digital Twin-Driven Cyber-Physical System for Autonomously Controlling of Micro Punching System. *IEEE Access* **2019**, *7*, 9459–9469. [CrossRef]
108. Zhang, Y.; Ren, S.; Liu, Y.; Sakao, T.; Huisingh, D. A Framework for Big Data Driven Product Lifecycle Management. *J. Clean. Prod.* **2017**, *159*, 229–240. [CrossRef]
109. Leng, J.; Ye, S.; Zhou, M.; Zhao, J.L.; Liu, Q.; Guo, W.; Cao, W.; Fu, L. Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Trans. Syst. Man, Cybern. Syst.* **2020**, *51*, 237–252. [CrossRef]
110. Rehman, M.H.U.; Ahmed, E.; Yaqoob, I.; Hashem, I.A.T.; Imran, M.; Ahmad, S. Big Data Analytics in Industrial IoT Using a Concentric Computing Model. *IEEE Commun. Mag.* **2018**, *56*, 37–43. [CrossRef]
111. Younan, M.; Houssein, E.H.; Elhoseny, M.; Ali, A.A. Challenges and Recommended Technologies for the Industrial Internet of Things: A Comprehensive Review. *Measurement* **2020**, *151*, 107198. [CrossRef]
112. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. Tackling Faults in the Industry 4.0 Era—A Survey of Machine-Learning Solutions and Key Aspects. *Sensors* **2019**, *20*, 109. [CrossRef] [PubMed]
113. Leng, J.; Ruan, G.; Song, Y.; Liu, Q.; Fu, Y.; Ding, K.; Chen, X. A Loosely Coupled Deep Reinforcement Learning Approach for Order Acceptance Decision of Mass-Individualized Printed Circuit Board Manufacturing in Industry 4.0. *J. Clean. Prod.* **2020**, *280*, 124405. [CrossRef]
114. Gao, Y.; Chen, Y.; Hu, X.; Lin, H.; Liu, Y.; Nie, L. Blockchain Based IIoT Data Sharing Framework for SDN-Enabled Pervasive Edge Computing. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5041–5049. [CrossRef]
115. Derhamy, H.; Eliasson, J.; Delsing, J. IoT Interoperability—On-Demand and Low Latency Transparent Multiprotocol Translator. *IEEE Internet Things J.* **2017**, *4*, 1754–1763. [CrossRef]
116. Shahzad, Y.; Javed, H.; Farman, H.; Ahmad, J.; Jan, B.; Zubair, M. Internet of Energy: Opportunities, applications, architectures and challenges in smart industries. *Comput. Electr. Eng.* **2020**, *86*, 106739. [CrossRef]
117. Rahman, H.; Hussain, M.I. A Comprehensive Survey on Semantic Interoperability for Internet of Things: State-of-The-Art and Research Challenges. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3902. [CrossRef]
118. Aazam, M.; Zeadally, S.; Harras, K.A. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4674–4682. [CrossRef]
119. 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]
120. Huo, R.; Zeng, S.; Wang, Z.; Shang, J.; Chen, W.; Huang, T.; Wang, S.; Yu, F.R.; Liu, Y. A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 88–122. [CrossRef]
121. Guan, Z.; Lu, X.; Wang, N.; Wu, J.; Du, X.; Guizani, M. Towards Secure and Efficient Energy Trading in Iiot-Enabled Energy Internet: A Blockchain Approach. *Future Gener. Comput. Syst.* **2020**, *110*, 686–695. [CrossRef]
122. Wang, E.K.; Liang, Z.; Chen, C.M.; Kumari, S.; Khan, M.K. PoRX: A Reputation Incentive Scheme for Blockchain Consensus of IIoT. *Future Gener. Comput. Syst.* **2020**, *102*, 140–151. [CrossRef]
123. Khan, M.Z.; Alhazmi, O.H.; Javed, M.A.; Ghandorh, H.; Aloufi, K.S. Reliable Internet of Things: Challenges and Future Trends. *Electronics* **2021**, *10*, 2377. [CrossRef]
124. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.-H. Convergence of Blockchain and Artificial Intelligence in Iot Network for the Sustainable Smart City. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]

125. Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital Twin: Enabling Technologies, Challenges and Open Research. *IEEE Access* **2020**, *8*, 108952–108971. [CrossRef]
126. Lim, W.Y.B.; Xiong, Z.; Niyato, D.; Cao, X.; Miao, C.; Sun, S.; Yang, Q. Realizing the Metaverse with Edge Intelligence: A Match Made in Heaven. *IEEE Wirel. Commun.* **2022**, 1–9. [CrossRef]