applied sciences

MDPI

Article

A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment

Haotian Chen [1], Sekione Reward Jeremiah [2], Changhoon Lee [1] and Jong Hyuk Park [1,*]

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Republic of Korea
[2] Department of Electrical and Information Engineering, Seoul National University of Science and Technology, Seoul 139-743, Republic of Korea
* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-10-9036-4042

Abstract: Intertwining smart manufacturing and the Internet of Things (IoT) is known as the Industrial Internet of Things (IIoT). IIoT improves product quality and reliability and requires intelligent connection, real-time data processing, collaborative monitoring, and automatic information processing. Recently, it has been increasingly deployed; however, multi-party collaborative information processing is often required in heterogeneous IIoT. The security and efficiency requirements of each party interacting with other partners have become a significant challenge in information security. This paper proposes an automated smart manufacturing framework based on Digital Twin (DT) and Blockchain. The data used in the DT are all from the cluster generated after blockchain authentication. The processed data in the DT will only be accessed and visualized in the cloud when necessary. Therefore, all the data transmitted in the process are result reports, avoiding the frequent transmission of sensitive data. Simulation results show that the proposed authentication mode takes less time than the standard protocol. In addition, our DT framework for a smart factory deploys the PDQN DRL model, proving to have higher accuracy, stability, and reliability.

Keywords: digital twins; blockchain; industrial internet of things; smart manufacturing

Citation: Chen, H.; Jeremiah, S.R.; Lee, C.; Park, J.H. A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment. *Appl. Sci.* **2023**, *13*, 1440. https://doi.org/10.3390/app13031440

Academic Editors: Andrea Prati, Antonella Petrillo and Ming Liu

Received: 21 November 2022
Revised: 9 January 2023
Accepted: 17 January 2023
Published: 21 January 2023

1. Introduction

With the continuous development of wireless communication and information processing technologies, many intelligent devices are connected to the internet to process real-time data and dynamically give feedback on the information processing results to achieve industrial intelligence [1]. The Industrial Internet of Things (IIoT) collects data through heterogeneous intelligent devices from different regions. It is utilized by Deep Learning, Natural language processing, Computer vision [2], and Robot Process automation [3] to construct systematic and intelligent industrial systems [4]. With the continuous development of the IIoT system, the number of smart devices is growing rapidly. In addition, more and more businesses need to exchange data with other organizations in the network and perform local work based on data interactions. Smart Manufacturing (SM) can use advanced information technology and manufacturing technology to optimize the production and transaction mode. It promotes the production efficiency, quality, and service level of the whole industrial production chain [5]. Intelligent devices of IIoT realize real-time collection and sharing of manufacturing resource data and achieve operational visibility and traceability of materials based on radio frequency identification (RFID) and wireless communication technology [6]. Production resources are delivered to the network through many smart devices, collaborating across different manufacturing to complete a large IIoT project. For example, heterogeneous devices have different computing and storage capabilities and security mechanisms [7], so some devices are more vulnerable than others and, in most cases, become the target of network attacks. As a mirror world very similar to C.P.S., the digital twin system can simulate all possible operations in the physical

world in this virtual world and evaluate the consequences, and further tune actual products according to the simulation results of the mirror [8]. In other words, DT allows engineers and designers to work on the details of a product before setting up the actual physical environment but also allows for cost reduction and process optimization while increasing the coordination of multi-party joint work. This is undoubtedly of great significance for SM [9].

1.1. Motivation

The headquarters has the decision-making and scheduling power in the SM system to integrate and manage each manufacturer. Since there are multiple manufacturers (sub-factories and plants), they communicate a lot to collaborate. The communication process may contain sensitive data information. Attackers can access the network and sensitive data through IIoT devices with relatively poor security performance and learn business entities' latest business policies or objectives [10]. In addition, redundant communication may cause manufacturing parts that are no longer available for service to be used by other manufacturers after one manufacturer is down for unavoidable reasons, resulting in the inability to complete the overall work [11]. Therefore, the headquarters is introduced into the SM system as the control center, which can integrate and manage the entire SM system. Each manufacturing plant only needs to obey the decision and perform the work. Even so, the amount of data in SM is not reduced. Still, some of their data flows are forwarded to headquarters, and direct communications with headquarters can be intercepted or tampered with security risks. Existing research results show that Blockchain is reliable for solving identity authentication and trust problems [12]. Blockchain can solve source reliability and result in verification problems through a non-repudiation consensus mechanism [13].

This paper proposes a Blockchain and DT-based heuristic multi-cooperation scheduling framework. While ensuring the efficiency of the whole process of smart manufacturing, it can provide privacy and security protection to the maximum extent. This paper aims to develop an SM framework that protects device privacy and provides legal identity authentication in an IIoT environment while making the operating process of this framework more efficient and accurate. Our framework divides the smart manufacturing network into three layers: the device layer, the edge layer deploying Blockchain, and the cloud layer deploying DT. This will create a virtual platform simulating all possible operations in the physical world. All data interactions between manufacturers are completed in DT, the established manufacturing status is given after data processing in DT, and the result report is sent to the headquarters. The data between headquarters and virtual manufacturing is only the interaction of results and decisions, and there is no more valuable information. Moreover, the volume of these data is much smaller than the detailed data interaction of classical conditions, thus speeding up the decision making and SM progress. The decision to deploy the headquarters in the cloud (outside of the DT) will be stored in the Blockchain, and no one can tamper with the decision content.

1.2. Contribution

Our proposed framework solves the following problems: (1) Communication volume and security risks between the headquarters and the manufacturing plant; (2) Security problems caused by frequent cross-class communication in the classical smart manufacturing process; (3) Prevents unknown and untrusted nodes from joining the smart manufacturing system. Overall, the main contributions of this paper are as follows:

- Blockchain provides authentication and identification capabilities. Only devices registered in the Blockchain can participate in SM. This can prevent illegal users from accessing the network and ensure that the data used in SM are legal and valid.
- DT implements a true copy of the physical environment. Data can be scheduled here, and after data are scheduled or when it is necessary to work with other manufacturing plants, decision requests can be sent to headquarters outside of the DT. The request

consists only of the result of processing the data. Even if an attacker eavesdrops during transmission, it is difficult to ascribe meaning to the intercepted data.

- Manufacturing in DT no longer needs to receive data from all directions; scheduling decisions from headquarters can ensure collaboration with other manufacturers even in a massive data environment. In this paper, we create clusters from which the DT schedules data flows at the discretion of headquarters. This creates a scalable SM environment capable of supporting the needs of the rapidly growing IIoT industry.
- Furthermore, DRL integration into DT and assisting it with decisions on when data should be transmitted is novel. To the best of our knowledge, our work is the first to consider such intelligent decisions based on the PDQN model. We deployed and tested classic DQN and PDQN, and our results showed PDQN model performs admirably in terms of convergence time, stability, and dependability.

1.3. Organization

The rest of the paper is organized as follows: Section 2 presents a general overview of other existing research. Section 3 proposes a blockchain and digital twin-based heuristic multi-cooperation scheduling framework. The section further presents an overview of the framework and explains its process flows. Section 4 evaluates the proposed framework with extensive system analysis and results. Finally, in Section 5, we conclude this paper.

2. Related Work

In recent years, the technical application of SM in IIoT has been widely discussed in the academic community. Research on DT and Blockchain deployment in SM is also actively carried out. In this section, we first present the critical considerations for SM. The research on security and efficiency in SM is investigated and discussed.

2.1. Existing Research

IIoT is a globally distributed system consisting of smart objects, CPS, wireless communication technology, and auxiliary computing platforms, such as cloud or edge computing. SM is a representative system in the IIoT, and its completeness needs to be evaluated from multiple perspectives. We find that the concepts of Intelligent Manufacturing (IM) and SM are so similar that many scholars confuse them. Wang et al. [14] systematically compared IM and SM and proposed that SM is the conclusion of IM evolution. SM applies more emerging technologies in industry 4.0 and has advantages over I.M. Cheng [15] summarized the technical trends suitable for SM, including big data analysis, cloud computing and edge computing, virtual reality and augmented reality, and digital twin. He also summarizes communication technology features suitable for IIoT, such as high data rate, high reliability, high coverage, and low latency. He defined the 5G-IIoT system for SM and described the realization methods of different advanced manufacturing scenarios and manufacturing technologies under the three classic applications modes of 5G. Through their research, we extract the requirements of IIoT for SM systems, such as security, scalability, confidentiality, integrity, and availability. We summarize SM-related research on Blockchain and DT based on those SM requirements and present them in Table 1.

Table 1. Summary of existing research.

Author	Year	Technique/ Environments	Key Contributions	Limitation
Zhang et al. [16]	2019	Digital Twin, Machine Learning; Smart Manufacturing	A DT-based SM method is proposed. This approach is efficient and fits the green IoT theme.	No simulation to prove the result.

Table 1. *Cont.*

Author	Year	Technique/ Environments	Key Contributions	Limitation
Zhang et al. [17]	2019	Blockchain; Smart Manufacturing	Blockchain solves the problem of multi-party trust and provides a secure transmission and storage mechanism to improve SM's transaction efficiency.	No simulation to prove the result.
Tao et al. [18]	2020	Blockchain, Digital Twin	An optimal matching system is proposed to protect transaction records in DT using Blockchain. The Blockchain in the system uses an improved consensus algorithm to ensure users' privacy and service providers' credibility.	No simulation to prove the result.
Teisserenc et al. [19]	2020	Blockchain, Digital Twin	A collaborative mechanism of SM services on an industrial Internet platform based on DT-Blockchain is proposed. This work also points out challenges in service management in SM.	No simulation to prove the result.
Leng et al. [20]	2020	Blockchain; Smart Manufacturing	This paper subdivides the possible security problems in SM and summarizes the indicators of the application of Blockchain in SM.	No proposed idea.
Fang et al. [21]	2020	Digital Twin; Smart Manufacturing	DT-based workshop scheduling is implemented with high scheduling accuracy and real-time data mapping. The validity of their system in SM is verified.	Lack of processing of real-time data.
Shahbazi et al. [22]	2021	Blockchain, Machine Learning. Smart Manufacturing	Combine Blockchain and machine learning to improve data quality and device reliability in SM.	Performance in complex network environments is not considered.
Singh et al. [23]	2021	Blockchain, Deep Learning; Smart Manufacturing	An automotive manufacturing case integrating machine learning and Blockchain is proposed to increase production and meet automation requirements, which is expected to be deployed in smart cities.	No simulation to prove the result.
Lattanzi et al. [24]	2021	Digital Twin. Smart Manufacturing	The application value and necessity of DT in SM are summarized, and the technical problems of DT in SM are put forward.	No proposed idea.
Lu et al. [25]	2021	Digital Twin; Smart Manufacturing	The DT association technology that can be applied in SM is summarized, and the model of DT development is systematically summarized based on consistency.	No proposed idea.
Liao et al. [26]	2021	Blockchain, Digital Twin	A reliable and efficient decentralized digital twin framework for industrial networks is proposed, which can be adapted to work in many industries using the physical infrastructure.	Fine-grained service details further complicate the proposal approach.
Our work	2022	Digital Twin, Blockchain.	Provides a heuristic DT data scheduling framework that considers efficiency and security.	Malicious behavior within DT may occur.

Lattanzi et al. [24] proposed that the current manufacturing process has an increasingly strong demand for the rapid allocation of production resources and adaptation to the environment. To adapt to this demand, the deployment of DT is imminent. They also summarize the technical challenges to be overcome in DT deployment, including integration of different domains, generation of fidelity models, and communication of heterogeneous data. It emphasizes that DT and IoT, cloud computing, and AI have an excellent expected integration effect, laying a foundation for our research. Lu et al. [25] summarized the definition of DT in SM, sorted out the standardized DT modeling process in detail, and summarized the SM scenarios in which DT can be deployed. The author shows that DT can simulate and imitate physical resources on the software level and can deal with them instantly through code debugging and product testing, thus increasing production efficiency and manufacturing accuracy and reducing costs.

Fang et al. [21] deployed DT for manufacturing scheduling in SM. They deployed the CPS unit as a virtual and physical twin communication medium. Virtual space deployment in physical space monitoring resources is used to collect data and establish the model, through the model, to obtain the corresponding scheduling plan and carry out the simulation, the final feedback to the physical space. This method is much more accurate than the traditional method because the data obtained based on statistics are constant, which cannot fully reflect the changing environment and the influence on parameters in the production process. Zhang et al. [16] proposed a DT-based low-carbon SM workshop. The model proposed by the author can train and filter historical data and then predict and evaluate carbon emissions based on DT. Sensor-based network configuration can select appropriate sensors to construct sub-networks for a specific production planning and scheduling task, and the expected efficiency will also be improved.

SM is a typical multi-party collaborative system where each component in the production chain has trust issues. Although DT supports SM running more efficiently by simulating the changes in the physical world, if the data of every sensor are copied back to DT, it is bound to have some worthless data that will interfere with the simulation and prediction. There is a probability of malicious data entering DT to mislead SM in the correct flow of events. Therefore, the data source needs to be authenticated and identified, and Blockchain is an excellent solution to this problem [20]. Zhang et al. [17] show that Blockchain can solve this problem and realize more transparent and secure transmission and storage. Blockchain can search the source of materials in SM, which improve transaction efficiency by eliminating wrong products. Shahbazi et al. [22] deployed Blockchain and smart contracts based on real-time data collection of IoT sensors to ensure device legitimacy and data security while reducing decision delay. Using big data technology to manage large-scale datasets, SM fault diagnosis is predicted and analyzed. Singh et al. [23] divided SM into five bottom-up layers, and layers 1–3 use blockchain to implement authentication and validity identification of data sources. The collected data are analyzed based on deep learning at the fourth layer, and the analysis results are applied to SM at the fifth layer to meet the requirements of automation and scalability.

The methods combining DT and Blockchain have been relatively well explored, and our study can benefit from these prior studies and proposed methods. For example, Teisserenc et al. [19] proposed a DT-BC-based SM service collaboration mechanism for an industrial Internet platform. The proposed mechanism uses DT to enhance the service performance and solve the trust problem between parties and participants in manufacturing services. The author pointed out that there are many challenges in managing SM services in the industrial Internet platform, such as the integration technology of physical and network information, the value-added technology based on manufacturing collaboration, and the trust of stakeholders.

Liao et al. [26] proposed a decentralized data twin framework to solve industrial networks' lack of trust and low-efficiency issues. Liao's work deploys Blockchain to solve data sharing, network security, integrity, invariability, and traceability challenges. This framework also protects information transparency and enhances privacy. The model fits

many industries and has high practical value in engineering and construction. In the study of [18], Blockchain is used to protect transaction records in DT and matches DT service providers and ITS subsystems through optimal matching and processed corresponding service transactions. Then, the auction process authenticates the matching process between buyers and sellers to ensure the auction's credibility and users' privacy security. The author proposes an improved DT-DPOS consensus mechanism for ITS.

2.2. Key Considerations for Efficient and Secure SM in IIoT Environment

An SM system based on DT requires six key considerations as follows:

- *Scalability*: There are many heterogeneous nodes in the IIoT, and the number of nodes in the network may increase with the work progress and even exceed the network load capacity. Therefore, we need to constantly expand the data types and data processing platform, even if the increasing amount of data should not cause too much impact on the operation of the whole system. A complete network system should be resistant to this problem [27].
- *Security and Privacy*: SM aims to collect large amounts of data and interact with them in various production environments, forming a complete industrial chain. Among them are the product's private information such as ID, location, working status, performance indicators, etc. Hackers may try to obtain this information for personal benefit. Therefore, protecting these data is a crucial requirement [28].
- *Confidentiality*: Private data in the industrial chain can be directly linked to commercial interests. The loss or exposure of these sensitive data will often bring economic losses or administrative risks [29].
- *Integrity*: Any unauthorized third party's operation or data modification is a critical challenge in IIoT [30].
- *Availability*: Many IIoT devices are based on real-time communication connections and operations. In distributed networks, even if one node (server or device) fails, processes on other nodes should be able to continue [31].

2.3. Research Comparisons

IIoT is a globally distributed system consisting of smart objects, CPS, wireless communication technology, and auxiliary computing platforms such as cloud or edge computing. SM is a representative system.

We summarize the characteristics of the research efforts, as shown in Table 2. The work presented in [18] demonstrates the superior performance of the deployed models and points out open technological challenges. Their work lacks information on physical integration technologies for industrial data; subsequently, optimization problems will lead to limited compatibility and connectivity. Hence, the expansion of the whole technology is not satisfactory. Moreover, the trust problem of relevant stakeholders is not standardized, and the consensus is completed in the local decentralized network, so the availability and security are reduced.

Table 2. Key consideration comparation with other related works.

Reference	Technology	Environment	Scalability	Security and Privacy	Confidentiality	Integrity	Availability
[18]	Blockchain, DT.	Industry Network	○	◐	●	●	◐
[19]	Blockchain, DT.	Industry Network	◐	●	●	●	◐
[26]	Blockchain, DT.	Smart City	◐	●	●	●	●
Our work	Blockchain, DT, DRL	IIoT	●	●	●	●	●

●: Subject covered in-depth; ◐: Partial coverage of the subject; ○: Subject not addressed.

The work presented in [19] built a DT ecosystem based on Blockchain and considers a comprehensive range of technologies. However, since their work does not provide experimental results or simulation results to prove their technical feasibility, we are skeptical about the scalability and availability of such an extensive and comprehensive technical framework. Complex frameworks must consider many factors, such as permission, identity verification, accessible content classification, communication channel, tolerable delay, and so on when granting access to multiple entities and extending the network. Reference [26] worked on an intelligent transportation system, but fine-grained service details further complicate the proposed approach. With the continuous development of smart city-related technologies and the improvement of infrastructure, the excessive complexity of this technology may affect the transition from smart transportation to the internet of vehicles.

In this paper, the creation of the cluster on the data type of a certain screening, coupled with the DT data preprocessing, so that the data flow in the whole system is more organized. Even when more data of different types enter the network framework, the reasonable classification method based on physical distance and application can ensure the continuous operation of the framework. This provides scalability in the environment with an ever-increasing data volume. The security and privacy measures allow only pre-certified sensors to send collected data to the cluster, and SM only uses the data in the secured cluster. It is also essential that data transfer between tiers be made after encryption. We recommend using lightweight Telehash encryption for IIoT devices, rather than DES or RSA algorithms with higher performance and complex requirements.

Data security, privacy, confidentiality, and integrity are protected in the above ways. In addition, attackers may use malicious behaviors to disguise or delete data. Therefore, important data interaction is only carried out in DT and interacts with the cloud headquarters only in the form of result reports, thus preventing data from being tampered in the communication process. In this paper, DT has independent control over the data in the cluster, and the headquarters' decision independently controls each scheduling behavior. Therefore, when some nodes fail, the SM system is unaffected, thus ensuring the service availability of our proposed framework. In summary, our proposed framework fits all of the core considerations.

3. Proposed Blockchain and Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework

This section provides a layered description of the proposed architecture, explaining the different layers of data processing and their deployment implications for the overall framework. Then, the whole data processing process is introduced from the global point of view. As shown in Figure 1, the heuristic multi-cooperation scheduling framework proposed in this paper is mainly divided into three layers: (1) the IIoT device layer, (2) the edge layer, and (3) the cloud layer.

- *Device layer*: At this layer, sensors collect industrial data and then forward the data to the upper layer, the edge layer. Many types of data in IIoT come from different industrial plants. SM requires manufacturers to collaborate to complete an industrial task. The interaction between various manufacturing in SM can be risky because the data provided by each plant does not guarantee validity. Therefore, the interaction between them cannot be carried out without any security guarantee, and the interaction between them can only be made after the confirmation of the legitimacy of their identity and data validity. To schedule the collaboration between manufacturers more efficiently, their scheduling decisions should be made after investigating the global status and identifying the validity of the collaboration object.

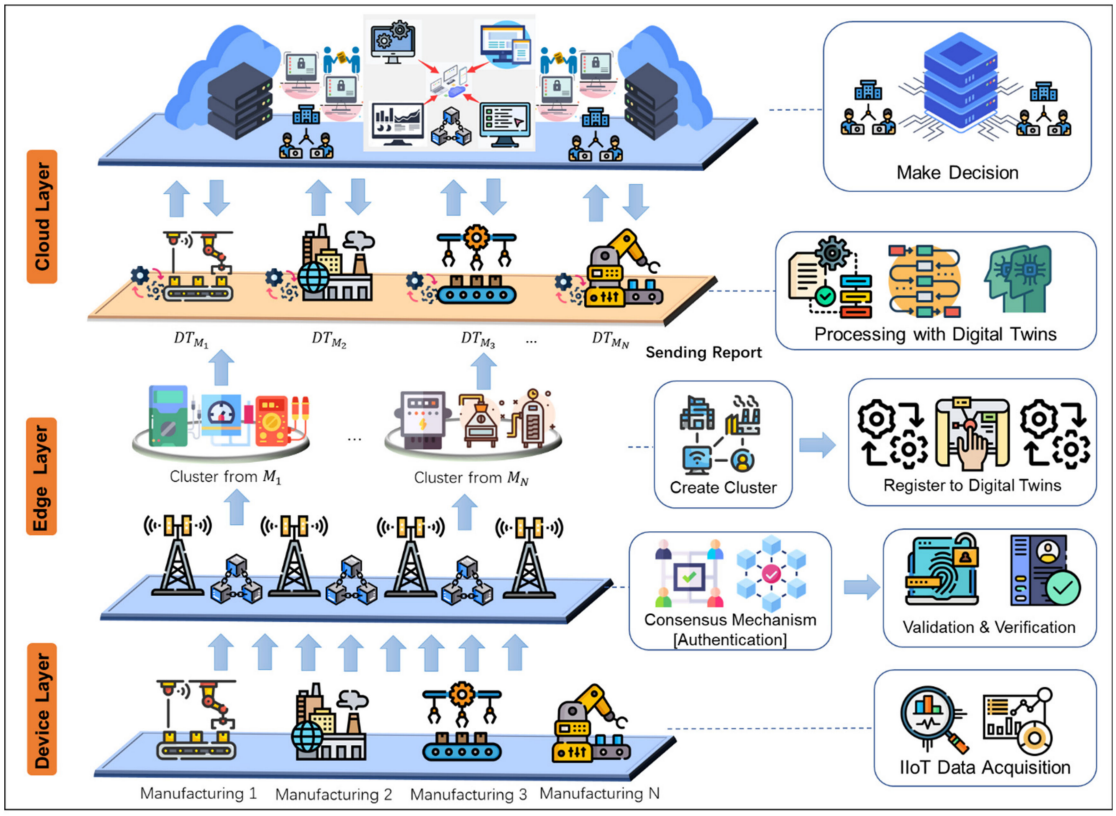

Figure 1. Proposed blockchain and digital twin-based heuristic multi-cooperation scheduling framework.

- *Edge Layer*: At this layer, we deploy a public Blockchain network where devices authenticate. Before devices at the device layer send data, they need to go through the consensus mechanism of the Blockchain system to authenticate their identity and data validity. After that, the base station makes a cluster according to the geographical distribution of data sources. Each manufacturer has a unique identification symbol so that each cluster can accommodate a specific range of complex manufacturing. Because the cluster's data can be used to identify its source, the headquarters can locate the corresponding manufacturing state more accurately and quickly when making decisions. In addition, all the devices that join the cluster must be approved by other nodes in the network through the consensus mechanism. Since only certified data can be added to the cluster, any necessary data for SM after that will be provided by the manufacturer in the cluster.
- *Cloud Layer*: DT is deployed in this layer, and a device layer mirror environment is made, where data will be scheduled for SM. The identifier judges the data used in digital manufacturing and only received from the corresponding cluster, thus ensuring the accuracy of data sources. When an SM manufacturer needs to interact with other SM manufacturers, the decision is made through the headquarters outside the DT when interacting with the headquarters. The local data processing results are encrypted and sent to the headquarters. The security of sensitive data is guaranteed because the calculation of sensitive data is realized in DT, and processing results only carry out the interaction with the headquarters.

In our proposed framework, the blockchain network provides authentication for manufacturing. It creates clusters that are easy to locate and trace. DT ensures that sensitive data are not transferred to the public network, thus ensuring the efficiency and security of SM operations. Data are transferred bottom-up from the device layer to the cloud. In the following three sections, we provide a detailed workflow of blockchain deployment in the edge layer and DT deployment in the cloud.

3.1. Blockchain-Based Data Validation

There are so many devices and sensors in the real world that there will inevitably be invalid data. If these data are added to the SM, it will increase the risks that may occur in the SM process and the difficulty of data scheduling. Deploying Blockchain at the edge layer provides an orderly interface for many devices. It connects to the cluster corresponding to manufacturing, which can screen out valid data and classify data sources. Moreover, Blockchain ensures the security of the edge layer by providing non-repudiation and traceability of data sources. Figure 2 shows the flowchart for the framework's device layer and edge layer, showing a more precise data flow and network structure.

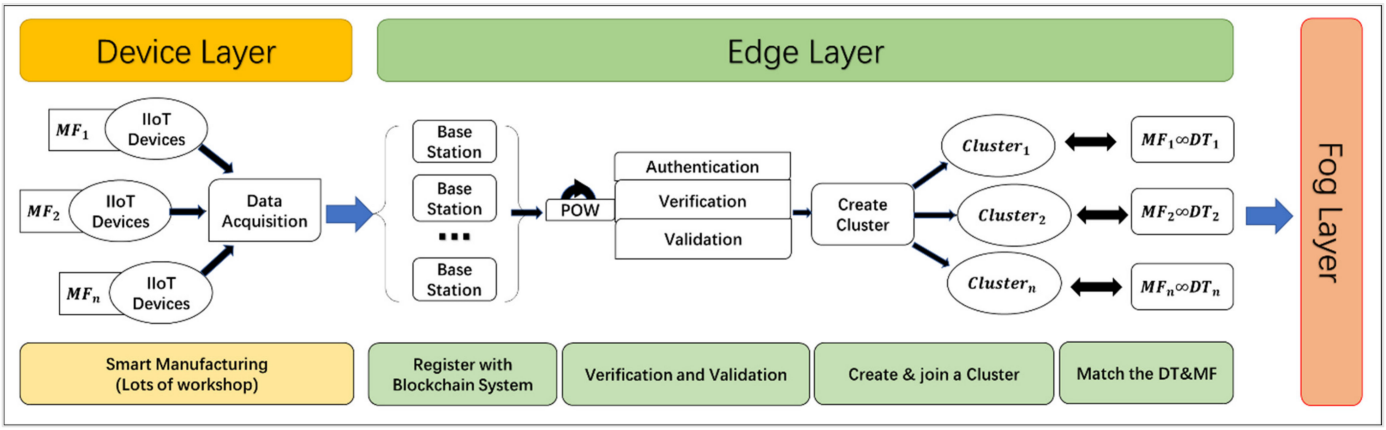

Figure 2. Flowchart of the proposed framework in device and edge layer.

We use a public blockchain here and allow all SM business-related nodes to join the blockchain network and verify validity using proof of work (PoW). Sensors collect data and upload them to the edge layer, which must authenticate and validate it before sending it. At the edge layer, all edge nodes that want to join a valid cluster must register with the Blockchain system through the consensus mechanism. After that, they can transfer data to the upper layer. As shown in Algorithm 1, they will compute a hash whose first N terms are 0, where N is the number of bits of 0 to be computed. Since the computation problem is a random one that competes with arithmetic power, fairness is guaranteed. All nodes in the network must participate in the calculation of this cryptographic puzzle if they want to join the cluster. The first edge node to calculate the result will announce the calculation process to the network. Other nodes in the network will use this method to calculate based on the local initial state in the local ledger. The data are valid when the calculation result is the same as the announcement result. A consensus is reached when the number of nodes with valid data authentication exceeds 51% of all nodes in the whole network. After the consensus mechanism is passed, the data validity is verified, and the corresponding device node will join the SM cluster and generate a block. The public key information of the edge node on the chain is also stored in the Blockchain, and other nodes can ask the node to confirm its identity through the data signature, which has the feature of non-repudiation. After the verification and validation, the device passes the authentication extremum, and its collected data are ready to be extracted at any time by the DT of the upper layer.

After all nodes' registration, each device is called an Authenticator in the Blockchain network. Once a transaction is triggered, no one can modify it, and each node in the Blockchain network jointly authenticates the transaction. After the authentication, the edge node is added to the cluster. To save energy, the data collected by the corresponding device node do not need to be authenticated again. Since the Blockchain authenticates the devices in the cluster, all the data are currently valid. This step, on the one hand, provides trust in data sources and reduces security risks; on the other hand, it reduces the total amount of data added to SM and reduces the data processing load by filtering data clusters. In addition, from the Device layer to the edge layer, lightweight encryption mechanisms, such

as regular TeleHash can improve communication efficiency and protect data security, which is an efficient and secure deployment strategy. Since TeleHash mentioned in this article is a standard unoptimized algorithm, we will not discuss Telehash in more detail here.

Algorithm 1 Blockchain Authentication & Verification

```
Input: Device ID, Manufacturing ID, and the request message to join DT.
Output: Decision and final consensus result (If the device can join
                and participate in the DT or not)
Process:
   CI_k.Send(<C_id, Msg, t>, request, BS);
                        //with C_id: client identify, t: timestamp, BS: Base station
B.S.Verify (<C_id, Msg, t>, C);
C_0.Prepare(<C_id, Msg, t>, nonce);          //nonce: authentication for PoW
      C_i.nonce= HashComputation();
      while(!isValidHashDifficulty(C_i.nonce)) {
          if (!OthersDoneReceviced(C_x.S) //Other miners solve the cryptographic puzzle
                      break;
          else:
                nonce = nonce + 1;
                input = previousHash + timestamp + data + nonce.
                hash = CryptoJS.SHA256(input)        }
C_0.Broadcast(<C_id, Msg, t>,pk_i, hash, S);
        // pk_i: a public key for verification, S: the digest signature of pk_i
C_0.WaitForHashCheck();
if (C}_0.Recevice(Response) > n/2 )
      add C_0ToBlockhain (BC, C_id, 0, pk_i );
      if Cluster_n exist
          joinToCluster(Cluster_n,C_id,M_id)
      else
          createThenjoin(Cluster_n,C_id,M_id)
else
      redo.
```

3.2. DT-Based Multi-Cooperation Scheduling

DT is deployed in the cloud layer. DT is the mirror image of each physical manufacturing in the device layer, and the data in DT are all from the cluster created in the edge layer. The primary purpose of DT deployment is to simulate and predict industry works in the physical world before specific scheduling takes place, thereby reducing possible risks and industry work losses. Only when the simulation scheduling in the virtual world shows good stability will DT schedule the physical world. At the same time, data collected by sensors in the physical world will be updated in real-time and added to the DT when headquarter deems it necessary; headquarters use this real-time data to change decisions and optimize scheduling instructions. The virtual world and the real world of DT run simultaneously, so there are two types of data running in DT. One type is data from simulation experiments that are used to process data for predicting the future but have not yet been used in the physical world. The other type is more sensitive and precise data fed back from real-time data in the real world, which is being applied to a job in the physical world. Therefore, the data processing flow in DT is divided into two categories: virtual simulation and physical simulation.

Figure 3 illustrates the proposed framework's cloud layer (inside of DT) flowchart. The detailed process of scheduling mechanisms based on headquarters decisions is then

discussed in two categories. The P&V identifier represents virtual or physical simulation data, respectively.

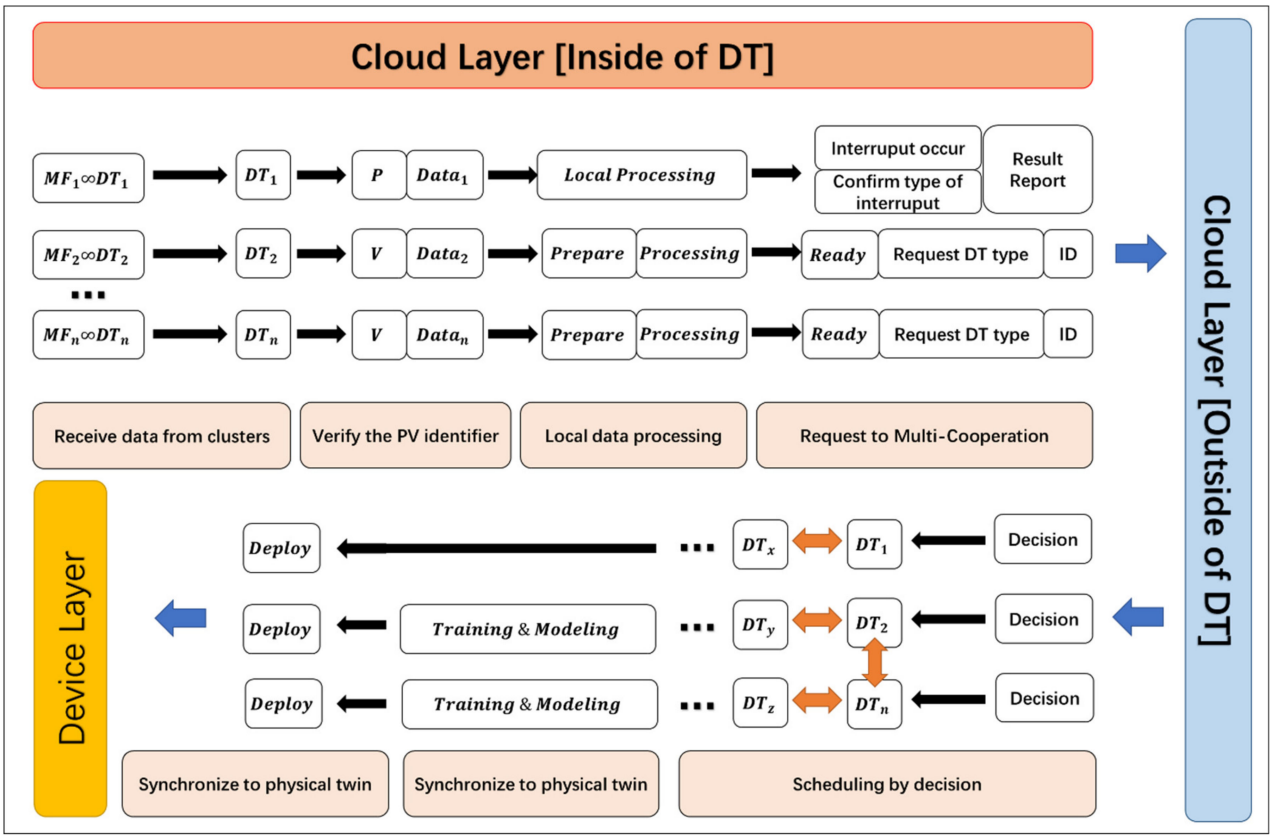

Figure 3. Flowchart of the proposed framework in the cloud layer (inside of DT).

- *Virtual Simulation*: In this process, the data used are non-real-time data. The DT uses the historical data collected by the sensors for modeling and result prediction, and performance analysis of the entire SM. Each digital manufacturer verifies the status of another digital manufacturer through its headquarters in the cloud (outside of the DT) before interacting with it. Before digital manufacturing sends data, it confirms that the partner is also ready before transmitting it. When confirming the other party's status, it is necessary to send data to the headquarters outside of the DT, including the ready identifier of the local digital manufacturing and the identifier of the target digital manufacturing it wants to interact with. These identifiers are only the result composed of strings and have no special meaning. These data are encrypted and transmitted to the cloud. Since it is only the result information, even if it is cracked, it is difficult for an attacker to sift out the helpful information from it. Headquarters processing the request also returns an encrypted result report telling the request originator which candidates are ready, and these ready digital manufacturing can then interact. Ready can be received ready, sent readily, or completely prepared. The corresponding ready state only allows the connected data transmission mode. A sending-ready digital manufacturer can only send its local data to other shops, and a receiving-ready digital manufacturer is only authorized to receive data from other digital manufacturers. Therefore, the virtual simulation data within the DT is already allowed to be sent. When any digital manufacturing receives data with the virtual simulation identification, it can be used directly without checking because the data is under the direction of the headquarters. One digital manufacturing interacts with other digital manufacturing in this method and performs data processing locally. After the prediction effect of data processing reaches the satisfactory value of digital

manufacturing, it starts to feed back to the physical world. The satisfactory standard is determined according to different SM standards.

- *Physical Simulation*: In this process, as the real-time data from the real world are processed, the state of the data source may change, and it is more sensitive to the data sent and received from other digital manufacturing. The most significant difference is that real-time data may cause other collaborative manufacturing to interrupt their work due to a failure in physical manufacturing due to uncontrollable accidents. When a scheduled work cannot continue to be executed, there are two situations: the active report of the point of failure and the report of the cooperative manufacturing because the data of the failed manufacturing cannot be accepted for a long time. Their reports are sent to headquarters outside of the DT. The transmitted data packet contains the fault point identifier and the interrupted work identifier and is encrypted. The two identifiers are also simple strings. Because the identifiers only carries and report simple information, the attacker cannot know the representative meaning of the information even if it is stolen and decrypted during transmission.

After the headquarters receives the failure information, it will send a message to the point of failure. Failure detection identifier will be generated for the physical manufacturing entity, including network and the physical equipment configuration environment variables. If confirmed, the manufacturing cannot continue to collaborate, a mirror image of the point of failure will return a correspondence result of data packets to the headquarters. Headquarters will send a result message to other digital manufacturers in collaboration. The resulting message contains unique identifiers for the original node failure that cannot continue and provides a list of other candidate manufacturing of the same type that is ready. Other manufacturers whose services are interrupted then attempt to establish communication connections with manufacturers of the same kind. After the interrupt work or regroup operation is complete, the DT also updates its decision synchronically to the physical manufacturing in the corresponding physical world. Similarly, when a working manufacturer needs to establish a connection with a new manufacturer that has not joined the work, the headquarters shall confirm the status of the corresponding manufacturing and make the connection. When the cooperation with another manufacturer ends, the DT in the local manufacturing disconnects the communication connection by reporting to the headquarters, which notifies the target manufacturing.

The implementation of this layer is shown in Algorithm 2. When data arrive in a cluster, it is first put into the DT according to its manufacturing identifier. Then, the data type is confirmed according to the PV identifier of the data. The two types of data use slightly different processing methods, with the main difference in handling data for possible interruptions. For the physical simulation stage, the interruption to be considered includes the failure of one of the multi-party participants to continue the work and the joining and withdrawal of the partner of the work. All these behaviors require DT to report to the headquarters and apply for scheduling, and the headquarters uniformly execute the scheduling decision. How the DT communicates to the cloud headquarters is explained in detail in the next section.

Algorithm 2 Digital Twin-based Scheduling

```
1: Input: Authenticated and verified data Msg from cluster Msg(MF_i, data, Id_PV,
CoTeam[id,MsgType]);
  //MF is a manufacturing id, Id_PV denote the data is provided for virtual or physical simula-
tion, CoTeam is a data structure that includes partner id and sends or receives data
2: Output: Result of processing status and request for collaboration with other DTs,
the collaboration information consists only of identifiers
3: Process:
4: Result of processing status
5: CheckIdentifier(MF_i, Id_PV);
6: JoinDT(MF_i);
7: if Id_PV show PS            //Physical Simulation
8:     LocalProcess(data,CoTeam[id,MsgType]);            //Work Process
9:     if no interruption occurs
10:        FinishWork(MF_i, CoTeam[id,MsgType]);
           //Report to Headquarter and discontinue the data connection
11:    else
12:        if request new partner
13:            ReportHeadquarter(DT_i,DTType);
               //DTType: The DT type of collaboration requester needs
14:            Schedule(decision,DT_j[]);
               // DT_j   is a list of candidates DT from headquarters decision
15:            backtoLocalProcess();
16:        else if request to terminate cooperation with a partner
17:            ReportHeadquarter(DT_i, DT_j[] );
18:            Schedule(decision,DT_j[]);
19:            backtoLocalProcess();
20:        else if request to report partners or itself
21:            ReportHeadquarter(DT_i, DT_j[] );
               //Here, DT_j can have the same value as DT_i
22:            Schedule(decision,DT_j[]);
               //if not report itself, headquarter will return a decision to solve a problem
23:            backtoLocalProcess();
24: else                  //Virtual Simulation
25:    Prepare(data);
26:    SendRequest(DT_i, state, DT_j[]);
       //state denotes whether local processing is ready or not
27:    if DT_j[] is not a null value
28:            Schedule(decision,DT_j[]);
29:            LocalProcess(data,CoTeam[id,MsgType]);
30:            FinishWork(MF_i, CoTeam[id,MsgType]);
31:            deploytoPhysicalWorld(desicison, MF_i,MF_j[]);
32:    else
33:            wait for a while;
34:            backtoSendRequest();
```

Overall, DT directly establishes a connection with manufacturing in the physical world. Therefore, the communication from the edge layer to the fog layer can be easily encrypted because DT is directly related to the Physical Twin (PT), and the corresponding DT can easily decrypt the data from the corresponding PT when the data in DT needs to make decisions from the headquarters, it only sends the encrypted processing results to the headquarters outside of the DT and applies them to decisions. The readability and data significance of the result information is very low for external data thieves. In addition,

because the data of industrial importance is only transmitted in the fog layer composed of multiple DTs, only the internal members related to SM have access to the traffic, which is not necessary to be sent outside, so the security of the data transmission is guaranteed.

4. Evaluation and Performance

For our research, the most important thing is to evaluate the authenticate time of the Blockchain consensus algorithm and the precision and speed of decision-making at headquarters.

4.1. Experience Setup

Instead of a real blockchain, we are using a simulated blockchain with simulated data. We analyze the proposed framework using Ubuntu 18.04 and an i7 processor with 32 GB RAM. The Blockchain network on the edge layer is built utilizing the Hyperledger Fabric 1.3. Virtual Cloud and Edge nodes are generated using VMware 14.

4.2. Performance Analysis

In this section, the efficiency of the blockchain network is evaluated. We mainly focus on the authentication time, which refers to the time required to complete the consensus, and the transmission delay from the device layer to the edge layer after the consensus is achieved. Transaction throughput refers to the maximum number of transactions completed per unit of time. A transaction generator with adjustable frequency generates transactions randomly, and the number of transactions sent within the statistical time is controllable. When the transaction throughput is measured, random transactions are continuously generated at a specific rate until the number of transactions sent within the statistical time is greater than the number of transactions recorded on the block within the same time. Then, the transaction throughput is obtained by averaging.

As shown in Table 3, we created two simulated commercial blockchains, one deployed in a LAN Fabric and the other deployed in a WAN Fabric. A blockchain TPS of 365.9 for the LAN and 76.4 for the WAN are used. In a WAN environment, network nodes across physical regions, network operators, and public cloud nodes generate network delay and limited network bandwidth. As a result, the transaction throughput of a WAN Fabric decreases, which is about 20.89% of that of a LAN Fabric.

Table 3. Throughput of a distance-based different network.

Comparison Item	LAN-Fabric	WAN-Fabric
TPS	365.9	76.4

As shown in Figure 4, the experimental results prove the feasibility of using Blockchain technology in this architecture. The proposed solution has lower latency and faster authentication speed than the classical POW algorithm. The faster authentication speed is mainly due to the improvement of the proposed algorithm. All participants will send the request to participate in the consensus to the base station and log their identity information to the base station. After calculating the hash value in the consensus algorithm, the base station will prioritize verifying the nearest node according to the geographical location during the broadcast. This distance results in much lower communication latency. In addition, since the cross-tier transmission must be encrypted, the lightweight algorithm is more efficient than the benchmark algorithms, such as RSA and DES, regarding computation rate and transmission rate. Therefore, the Telehash algorithm deployed in the device and edge layer's transmission medium also provides lower transmission delay. Thus, the network expansion of the protocol is better with the continuous expansion of the network, more time can be saved, and lower authentication delay means higher SM efficiency, because more time can be used to process computation tasks. To sum up, this makes it ideal for implementation in live scenes before manufacturing adds DT to complement and protect DT-based cloud environments.

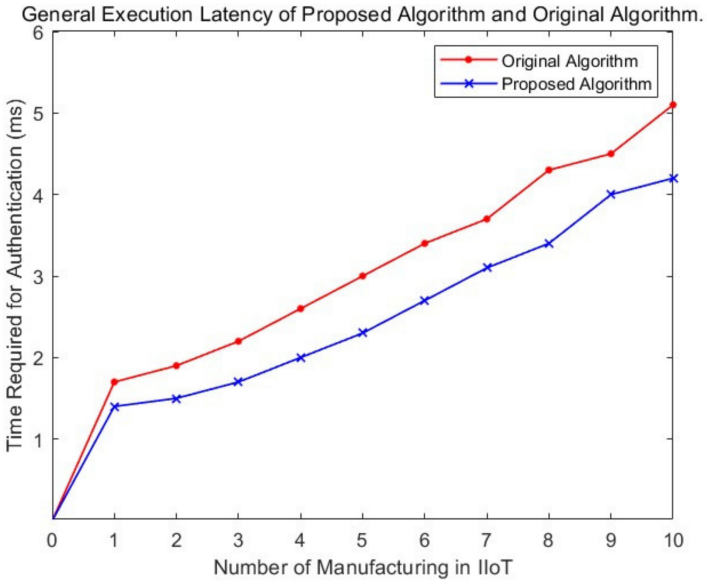

Figure 4. Authenticated time of the proposed Blockchain algorithm.

As is depicted, the proposed algorithm managed to maintain high and stable throughput for the blockchain network. As shown in Figure 5, the original algorithm recorded a decline of throughput with the increasement of peer nodes in the network; on the other hand, our proposed algorithm shows better throughput than the original algorithm. In our approach, the broadcasting is centered near the base station and starts transmitting information based on physical distance, and the cluster will be divided by the base station. The throughput results in Table 3 show that network nodes across physical regions, network operators, public cloud nodes, limited network bandwidth, and other problems will cause network delay. Data processing based on physical distance can resolve these problems to achieve a higher throughput rate. In addition, the destination of cluster-based data transmission is more apparent in the network routing process. More similar data can be packaged together, so the number of transactions completed per unit of time will increase. This improves the efficiency of our proposed heuristic multi-cooperation scheduling framework for the SM environment.

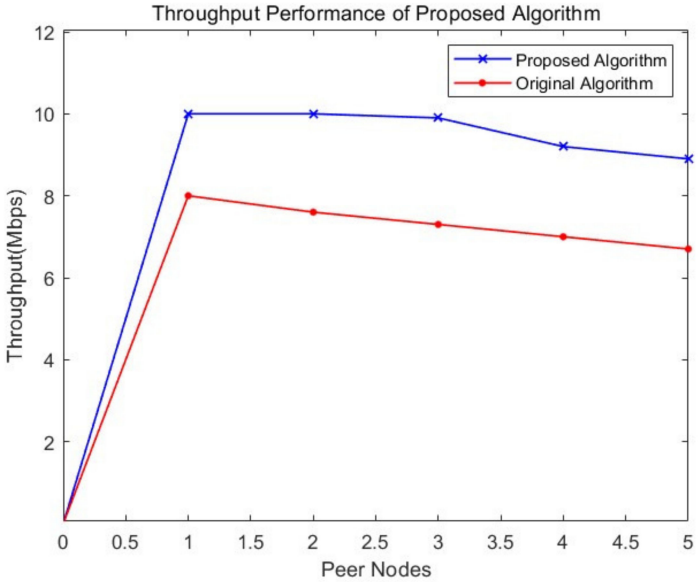

Figure 5. Authenticated time of the proposed Blockchain algorithm.

4.3. Simulation of the PDQN DRL Model in DT

DT has been employed in current production and testing systems in various sectors. It has been emphasized as a deployment approach for establishing completely automated systems and improving semantic interoperability across several domains. In a smart factory, the manager's purpose is to construct an intelligent agent, make plans, and take measures to decrease unexpected downtime and waiting time, enhancing the overall factory processing rate. A typical smart manufacturing system is optimized in this manner.

4.3.1. DT's Simulation and Modeling

For our work, we consider a factory installed with cameras in a physical location to obtain manufacturing (factory) conditions by providing footage for a specific range inside the factory. Our model considers the factory's storage house from several places with a central operator and a reserved area (reserved areas with space capacity CR) used to store unprocessed goods. The remaining space in the storage facility is recorded as Cr (we consider this the current state for our model), corresponding to the present time stamp (t). Under such settings, it is clear that for each time step, the current state of our model is set at Cr of range {0 to CR}, and therefore, CR+1 states are available.

SMDP model is used to build the discount cost function to estimate the system's processing capacity for warehouse storage. In our study, the Semi-Markov Decision Process (SMDP) model is used as the primary model for examining storage units inside a smart factory. The agent controls the range R(n) for the factory storage activity and capacity and it is required to be checked at each timestamp (t). It is also worth mentioning that the decision system's precision is entirely dependent on the precision of the dispersion of the RFID antenna and resolution of the image-based object detection cameras and system, which determines the number of possible actions. The states (Sn) will be set to {0} when the reserve area is filled, and there is no space left for additional units ready to process or store at the warehouse. Under such circumstances, it is fair for the agent (DRL-model) to select action (A(n)) = 0, thus meaning it terminates obtaining and storage of new units in the defined storage area of capacity CR.

4.3.2. Profit Sharing DRL (with DQN)

The capacities of the sensor and camera systems determine how accurately actions are taken in the smart factory storage DT. For the DRL model to function better, the footage and sensor must guarantee a certain level of precision. However, an increase in the precision of sensors and cameras means an increase in candidate actions (possible actions to be taken by the DRL model), which also significantly correlated with increased accuracy. If a traditional DRL method is used to model the system, initializing the weights will be laborious and challenging to maintain and preset manually. That will have an impact on how effectively the algorithms converge. DQN successfully uses the benefits of neural networks to supplement RL The approach uses the Q-learning target-value function to create the DL tags for creating the loss function to merge these two models efficiently.

DQN uses experience replay to address this issue of data correlation. Additionally, two main networks are constructed. To build a loss function, one network creates the current $\boldsymbol{Q}$ value ($\boldsymbol{QM}$), and the second generates the targeted $\boldsymbol{Q}$ value ($\boldsymbol{QT}$). This is very is crucial for neural network training. Consequently, the following equation shows how the DL loss function may be obtained:

$$\boldsymbol{DQN{-}Loss\ L(\theta t)} = (\boldsymbol{QT} - \boldsymbol{QM})^{\boldsymbol{2}} \tag{1}$$

Then, the Bellman equation can be used to update the target network ($\boldsymbol{QT}$) as follows:

$$\boldsymbol{QT} = \boldsymbol{r} + \boldsymbol{\gamma}\ \boldsymbol{max}(\boldsymbol{a} - \boldsymbol{r})\ \boldsymbol{Q}(\boldsymbol{sr},\ \boldsymbol{ar};\ \boldsymbol{\theta}) \tag{2}$$

where the reward amount is denoted by $(\boldsymbol{r})$ and $(\boldsymbol{\theta})$ denotes the iterative process technique, and $(\boldsymbol{\gamma})$ indicates the discount percentage. For our work, we take $(\boldsymbol{ar})$ as the presently

available actions, and we execute an action (ar) to go to the next state, which is (sr). Despite the addition of DL, which may significantly increase the effectiveness of high-dimensional feature characteristics extraction, the intrinsic flaw in RL persists, necessitating several iterations until convergence. To maximize the advantages of experience replay, a model is supposed to save as many samples as possible. However, when employing DRL to explore the environment, previous data retrieved from replay memory will impact the agent's adaptation to the new environment. On the other hand, profit sharing (PS) may minimize past knowledge's influence on RL by introducing an additional term at the end of the iterative equation.

4.3.3. PDQN vs. D.Q.N. Performance Evolution

We made a comparison of various methods, including convergence time (ConvT), average convergence (AveConv), and variance convergence (VarConV), both considering a total of 1000 iterations. Our evaluation begins with varying learning rates (0.1, 0.01, and 0.001). The comparison shows that it considerably impacts convergence stability, as shown in Figure 6. It is worth noting that the simulations with varied parameters are an average of 25 simulation runs 25. The same approach was adopted for the following experiments discussed later in this section. The results demonstrate that a stable operating condition may be maintained during the iterative procedure when the learning rate is 0.01. We conducted tests with classic DQN and PDQN. PDQN requires a shorter convergence time (6.136) than classical DQN (7.528). It performs admirably in terms of stability and dependability and is more stable (10.202) and reliable (68.248) than DQN, which has values of 7.326 and 25.549 for stability and reliability, respectively. For the reliability measure, it indicates the degree of oscillation during learning of the model. The higher the score, the less severe the deviation or variance of operations during the transition between convergence states. Reliability indicates the deviation of optimal performance achieved among trials; the higher the score, the more reliable the performance of the model.

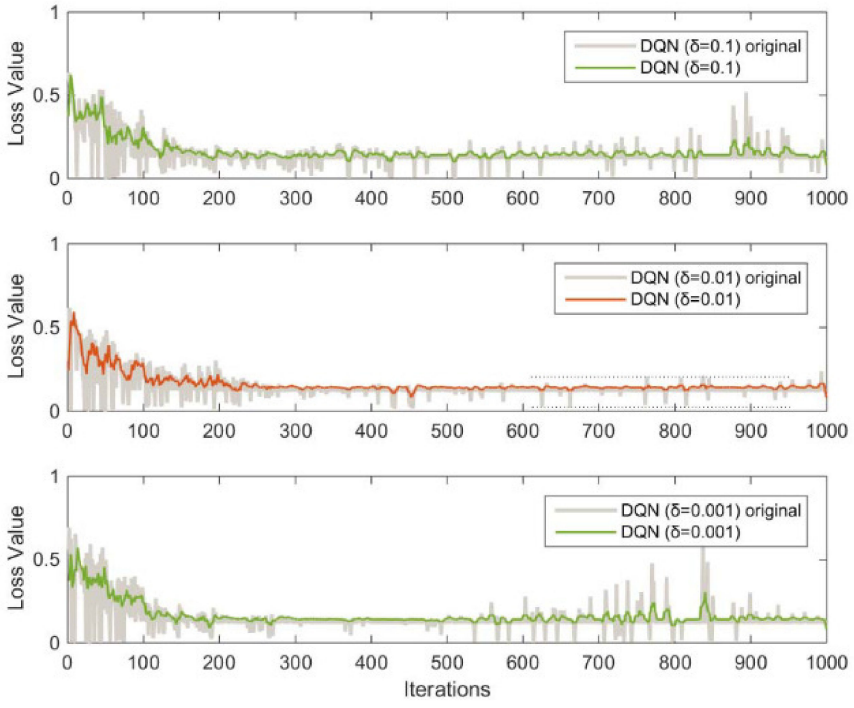

Figure 6. Performance of DQN using various Learning Rates (with and without profit sharing).

5. Conclusions

This article begins with a review of IIoT and SM concepts. Based on both characteristics, a secure SM framework based on Blockchain, and DT is proposed to provide transmission

security for IIoT. The simulation results show that the proposed blockchain authentication mechanism requires less time. Since the distance of broadcasting is based on physical distance and not node location in the Blockchain network, the authentication phase is completed in less time. The PDQN DRL model has high accuracy, stability, and reliability compared to classical DQN within the DT framework for the smart factory. Our RL DT simulation model helps resolve storage capacity control issues in smart factory warehouses. Blockchain-based authentication ensures that all data added to the cluster are valid. The DT platform with valid data processes data according to the set algorithm and requests decision-making from the headquarters in the cloud but outside of DT when other platforms are needed. The headquarters allocates scheduling strategies for each manufacturing and ensures maximum work efficiency for each multi-manufacturing cooperation. Only the processing results and some identifiers will be sent to the cloud headquarters when the request is made. As the readability and significance of these data are unknown to other organizations, sensitive information inside the manufacturing will not be disclosed. In future work, we plan to combine quantum computing technology further to improve the framework's efficiency and security.

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

Funding: This research was supported by the Energy Cloud R&D Program (2019M3F2A1073386) through the NRF (National Research Foundation of Korea), both funded by the Ministry of Science and ICT.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Park, J.S.; Park, J.H. Future trends of IoT, 5G mobile networks, and AI: Challenges, opportunities, and solutions. *J. Inf. Process. Syst.* **2020**, *16*, 743–749. [CrossRef]
2. Lee, J.; Hwang, K.I. RAVIP: Real-time AI vision platform for heterogeneous multi-channel video stream. *J. Inf. Process. Syst.* **2021**, *17*, 227–241. [CrossRef]
3. Ribeiro, J.; Lima, R.; Eckhardt, T.; Paiva, S. Robotic Process Automation and Artificial Intelligence in Industry 4.0—A Literature review. *Procedia Comput. Sci.* **2021**, *181*, 51–58. [CrossRef]
4. Noor, M.; Abbas, H.; Bin Shahid, W. Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis. *J. Netw. Comput. Appl.* **2018**, *103*, 249–261. [CrossRef]
5. Kang, H.S.; Lee, J.Y.; Choi, S.; Kim, H.; Park, J.H.; Son, J.Y.; Kim, B.H.; Noh, S.D. Smart manufacturing: Past research, present findings, and future directions. *Int. J. Precis. Eng. Manuf.-Green Technol.* **2016**, *3*, 111–128. [CrossRef]
6. Zelbst, P.J.; Green, K.W.; Sower, V.E.; Bond, P.L. The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. *J. Manuf. Technol. Manag.* **2020**, *31*, 441–457. [CrossRef]
7. Sittón-Candanedo, I.; Alonso, R.S.; García, Ó.; Muñoz, L.; Rodríguez-González, S. Edge computing, IoT and social computing in smart energy scenarios. *Sensors* **2019**, *19*, 3353. [CrossRef]
8. Kuts, V.; Modoni, G.E.; Otto, T.; Sacco, M.; Tähemaa, T.; Bondarenko, Y.; Wang, R. Synchronizing physical factory and its digital twin through an IIoT middleware: A case study. *Proc. Est. Acad. Sci.* **2019**, *68*, 364. [CrossRef]
9. Luzniak, K. Digital Twin Applications—What Challenges Do They Solve? Available online: https://neoteric.eu/blog/digital-twin-applications-what-challenges-do-they-solve/#:~{}:text=What%20are%20digital%20twin%20applications,planning%20of%20large%2C%20complex%20projects (accessed on 12 August 2022).
10. Hassan, R.J.; Zeebaree, S.R.M.; Ameen, S.Y.; Kak, S.F.; Sadeeq, M.A.M.; Ageed, Z.S.; Al-Zebari, A.; Salih, A.A. State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions. *Asian J. Res. Comput. Sci.* **2021**, *22*, 32–48. [CrossRef]

11. Mittal, S.; Khan, M.A.; Romero, D.; Wuest, T. Smart manufacturing: Characteristics, technologies and enabling factors. *Proc. Inst. Mech. Eng. Part B J. Eng. Manuf.* **2019**, *233*, 1342–1361. [CrossRef]
12. El Azzaoui, A.; Choi, M.Y.; Lee, C.H.; Park, J.H. Scalable Lightweight Blockchain-Based Authentication Mechanism for Secure VoIP Communication. *Hum.-Cent. Comput. Inf. Sci.* **2022**, *12*, 8. [CrossRef]
13. Gong, J.; Navimipour, N.J. An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. *Clust. Comput.* **2022**, *25*, 383–400. [CrossRef]
14. Wang, B.; Tao, F.; Fang, X.; Liu, C.; Liu, Y.; Freiheit, T. Smart Manufacturing and Intelligent Manufacturing: A Comparative Review. *Engineering* **2021**, *7*, 738–757. [CrossRef]
15. Cheng, J.; Chen, W.; Tao, F.; Lin, C.L. Industrial IoT in 5G environment towards smart manufacturing. *J. Ind. Inf. Integr.* **2018**, *10*, 10–19. [CrossRef]
16. Zhang, C.; Ji, W. Digital twin-driven carbon emission prediction and low-carbon control of intelligent manufacturing job-shop. *Procedia CIRP* **2019**, *83*, 624–629. [CrossRef]
17. Zhang, Y.; Xu, X.; Liu, A.; Lu, Q.; Xu, L.; Tao, F. Blockchain-based trust mechanism for IoT-based smart manufacturing system. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1386–1394. [CrossRef]
18. Tao, F.; Zhang, Y.; Cheng, Y.; Ren, J.; Wang, D.; Qi, Q.; Li, P. Digital twin and blockchain enhanced smart manufacturing service collaboration and management. *J. Manuf. Syst.* **2020**, *62*, 903–914. [CrossRef]
19. Teisserenc, B.; Sepasgozar, S. Adoption of Blockchain Technology through Digital Twins in the Construction Industry 4.0: A PESTELS Approach. *Buildings* **2021**, *11*, 670. [CrossRef]
20. 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]
21. Fang, Y.; Peng, C.; Lou, P.; Zhou, Z.; Hu, J.; Yan, J. Digital-Twin-Based Job Shop Scheduling Toward Smart Manufacturing. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6425–6435. [CrossRef]
22. Shahbazi, Z.; Byun, Y.-C. Integration of Blockchain, IoT and Machine Learning for Multistage Quality Control and Enhancing Security in Smart Manufacturing. *Sensors* **2021**, *21*, 1467. [CrossRef]
23. Singh, S.K.; Azzaoui, A.E.; Kim, T.W.; Pan, Y.; Park, J.H. DeepBlockScheme: A deep learning-based Blockchain driven scheme for secure smart city. *Hum.-Cent. Comput. Inf. Sci.* **2021**, *11*, 12. [CrossRef]
24. Lattanzi, L.; Raffaeli, R.; Peruzzini, M.; Pellicciari, M. Digital twin for smart manufacturing: A review of concepts towards a practical industrial implementation. *Int. J. Comput. Integr. Manuf.* **2021**, *34*, 567–597. [CrossRef]
25. Lu, Y.; Liu, C.; Kevin, I.; Wang, K.; Huang, H.; Xu, X. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robot. Comput.-Integr. Manuf.* **2019**, *61*, 101837. [CrossRef]
26. Liao, S.; Wu, J.; Bashir, A.K.; Yang, W.; Li, J.; Tariq, U. Digital Twin Consensus for Blockchain-Enabled Intelligent Transportation Systems in Smart Cities. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 22619–22629. [CrossRef]
27. Hazra, A.; Adhikari, M.; Amgoth, T.; Srirama, S.N. A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions. *ACM Comput. Surv.* **2021**, *55*, 1–35. [CrossRef]
28. Lu, Z.; Wang, C.; Zhao, S. Cyber deception for computer and network security: Survey and challenges. *arXiv* **2020**, arXiv:2007.14497. [CrossRef]
29. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 760–776. [CrossRef]
30. Lin, H.; Yan, Z.; Chen, Y.; Zhang, L. A Survey on Network Security-Related Data Collection Technologies. *IEEE Access* **2018**, *6*, 18345–18365. [CrossRef]
31. Jayasree, S.; Sushmita, R.; Sipra, D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481–102500. [CrossRef]