smart cities

MDPI

Article

Industrial Data Homogenization and Monitoring Scheme with Blockchain Oracles

Denis Stefanescu [1,2,*], Patxi Galán-García [3], Leticia Montalvillo [1], Juanjo Unzilla [2] and Aitor Urbieta [1]

[1] Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA), 20500 Arrasate-Mondragon, Spain
[2] Department of Communication Engineering, University of the Basque Country (UPV/EHU), 48013 Bilbao, Spain
[3] Entrii, 46024 Valencia, Spain
* Correspondence: distefanescu@ikerlan.es

Abstract: Research efforts on Distributed Ledger Technologies (DLTs) for industrial applications have constantly been increasing over the last years. The use of DLTs in the Industry 4.0 paradigm provides traceability, integrity, and immutability of the generated industrial data. However, Industry 4.0 ecosystems are typically composed of multiple smart factory clusters belonging to several companies, which are immersed in constant interaction with other business partners, clients, or suppliers. In such complex ecosystems, multiple DLTs are necessarily employed to maintain the integrity of the data throughout the whole process, from when the data is generated until it is processed at higher levels. Moreover, industrial data is commonly heterogeneous, which causes compatibility issues, along with security and efficiency issues in the homogenization process. Thus, the data needs to be pre-processed and homogenized in a secure manner before being exploited. Consequently, in this work, we address the issues mentioned above by providing an industrial raw data pre-processing and homogenization process according to a standard data model. We employ decentralized blockchain oracles to guarantee the integrity of the external data during the homogenization process. Hereafter, we design an interoperable plant blockchain for trustworthy storage and processing of the resulting homogenized data across several industrial plants. We also present a prototype implementation of the aforementioned scheme and discuss its effectiveness. Finally, we design a monitoring scheme to overview the usage the performance of the architecture processes and identify possible performance and security issues.

Keywords: blockchain; Industry 4.0; Internet of Things; blockchain oracles; monitoring

Citation: Stefanescu, D.; Galán-García, P.; Montalvillo, L.; Unzilla, J.; Urbieta, A. Industrial Data Homogenization and Monitoring Scheme with Blockchain Oracles. *Smart Cities* **2023**, *6*, 263–290. https://doi.org/10.3390/smartcities6010013

Academic Editors: Miguel Pincheira and Massimo Vecchio

Received: 30 November 2022
Revised: 30 December 2022
Accepted: 6 January 2023
Published: 10 January 2023

1. Introduction

Industry 4.0 covers a wide range of modern approaches and technologies that aim to improve the manufacturing industry greatly. The most relevant technologies that are included in the concept of Industry 4.0 are Big Data, Artificial Intelligence (AI), advanced robotics, edge computing, 5G networks, the Internet of Things (IoT), and overall digitalization of the manufacturing processes [1].

Recently, blockchains have started to become increasingly relevant in the field of Industry 4.0 due to their ability to provide immutability and traceability of stored data. Thus, data can be processed throughout DLTs in a decentralized and trustworthy manner [2]. However, the usage of blockchain in Industry 4.0, where there are many resource-constrained devices, is not straightforward since blockchains require high storage capacity, high computational power, and offer relatively low throughput [3]. However, recently, many researchers have designed lightweight blockchains for IoT [4,5]. Furthermore, recently, novel Distributed Ledger Technologies (DLTs) such as Directed Acyclic Graphs (DAGs) [6], which are specifically optimized for resource-constrained environments, have been introduced.

A DLT-based Industry 4.0 scenario is presented in [7], where there is a broad ecosystem of inter-connected smart plant clusters. Figure 1 shows an Industry 4.0 scenario with two industrial plants, where each plant has several production lines (e.g., Plant A has production lines "PL1-A1" and "PL2-A2"). Within each production line, several Industrial IoT (IIoT) devices operate and generate raw data that measures, among other data, machines' performance, process productivity, and quality, and machines' End-Of-Life. This production data is securely stored by means of DAG-type DLTs, which according to Wu et al. [8], are the most appropriate DLTs for IIoT devices due to their high throughput. As IIoT devices normally generate a high amount of data to reduce the storage burden of the DAGs, it is advisable to leverage appropriate storage without overloading the DLT. For example, in this scenario, we have an InterPlanetary File System (IPFS) (https://ipfs.io/, accessed on 20 November 2022) storage system, where the actual IIoT raw data is stored, whilst the DAGs store only the data hashes. This approach assures data integrity whilst keeping the DAG lightweight.

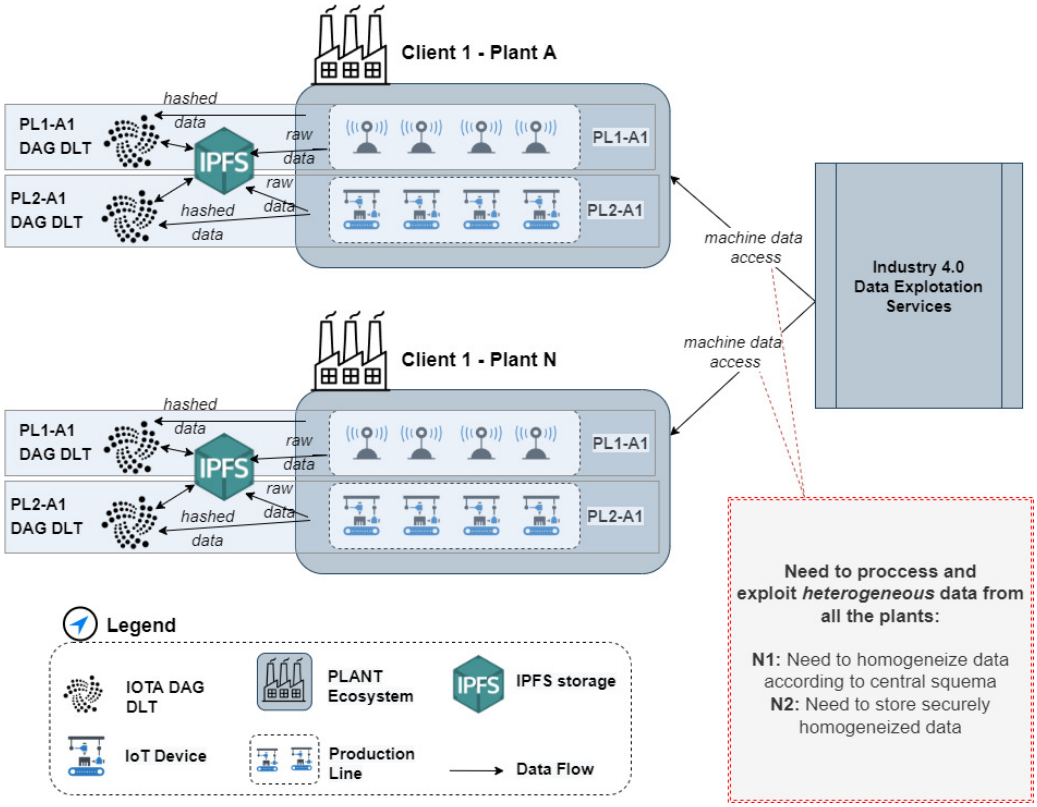

Figure 1. Industry 4.0 motivating Scenario.

So far, in the presented scenario, the data generated by IIoT devices is securely gathered and stored by the DAG DLTs and IPFS storage. However, Industry 4.0 does not stop at the machine data level, and this data that is being gathered at "the lowest level" needs to be exploited and processed by "higher" levels to derive and build actual information, such as machine and IIoT fleet status, machines predictive maintenance (by AI algorithms), compute overall process productivity, etc. Hence, these "upper" processes **need to access and process heterogeneous data from all cluster plants**. However, accessing and processing all the raw machine data from all production-level DAG-type DLTs is not a straightforward procedure, essentially due to the:

- Heterogeneous machine data. Data could be expressed in different units of measure depending on the machine provider, machine version, country, etc. They could have a distinct number of decimal places, obey different standards, or they can include certain errors or variations. This problem stems from the fact that according to Jirko et al. [9],

"machines within a complex system are produced by different manufacturers with different data models and interfaces". Consequently, this issue affects industrial interoperability and integration, thus, creating a detrimental impact on the ability to effectively process data using disruptive technologies, such as Big Data or AI.

- Lack of efficiency and security when accessing machine data [10]. It is not efficient nor secure to directly delegate the responsibility to external data exploitation services to access and process the raw machine data into "readable" plant-level data. Accessing machine data means that each data exploitation service needs to be a client of every production line DLT that wants to access data from. Additionally, these services would need to simultaneously process all the data from all machines and homogenize it accordingly. This approach lacks efficiency as the data exploitation services would spend a high amount of time accessing and homogenizing data before exploiting it. This is not utterly secure either since it breaks the data custody chain and mixes responsibilities, as in each data exploitation service, the actual data format being used to be exploited becomes obscure, and the traceability and integrity are compromised.

Furthermore, such complex ecosystems require proper monitoring to achieve higher efficiency rates by notifying human operators of probable performance gaps and possible disruptions through the presentation of data. Even though, theoretically, the use of DLTs improves the security of industrial processes, many attacks, such as Denial-of-Service (DoS) attacks, are still possible. Thus, they need to be identified and mitigated as soon as possible to avoid the disruption of industrial production. In addition, proper monitoring can also help mitigate errors, and optimize production processes and associated costs, which are known to be critical in industry [11].

In this context, this work aims to mitigate these problems, by providing means to that:

- The raw machine data that resides in DAG-type DLTs are securely and consistently homogenized by a secured and traceable process. This will ensure that the data conforms to a common data model, thus, providing interoperability so that processes at higher levels can exploit the data in a consistent manner.
- The homogenized data is securely stored and accessed, ensuring its integrity and availability. This will ensure trust in the data throughout the whole process, from where the data is generated from the production lines to where it is exploited and processed at a higher level. Processing raw IIoT data through a DAG DLT is a pointless approach if, at a higher level, we have a centralized and non-persistent data structure where the data can be easily tampered with [12].
- The whole industrial architecture must be carefully monitored using a monitoring system that is able to analyze all components securely; the IIoT sensors and actuators, the DLTs, the storage systems, etc. This analysis is required for performance and security optimizations and prevention to avoid the malfunction of critical processes.

Consequently, this work presents the following contributions to the described issues:

1. A "data homogenization" process for solving data interoperability issues that relies on the use of decentralized blockchain oracles as a trustworthy source for the target data model scheme the data needs to conform to. In this paper, we greatly improve the oracle architecture compared to a previous work [13] by employing a more versatile blockchain platform to improve simplicity and provide more interoperability capabilities. Finally, we store the resulting homogenized data in a blockchain-based solution for trustworthy access and processing.
2. A monitoring system for the proposed scheme to track the quality of the retrieved data, the performance of the network, the usage of each oracle, billing reports, security incidents, etc. We implement a monitoring architecture API for data retrieval, and we visualize it using the ELK (https://www.elastic.co/es/what-is/elk-stack, accessed on 21 November 2022) (Elasticsearch, Logstash, and Kibana) stack.
3. A prototype that implements the secure data homogenization process that: (i) accesses raw machine data stored in DAG DLTs, (ii) gets the target data model schema from

the oracles, (iii) performs the data homogenization from the source data scheme to the target data schema, and (iv) stores the homogenized data into a "plant level" blockchain network so that it can be consistently accessed and processed by other services. We also implement the monitoring system of the aforementioned scheme.

The remainder of the paper is organized as follows. In Section 2, we introduce the concepts of blockchain, smart contracts, and oracles to provide the background technologies based on which our proposal is made. In Section 3, we analyze the existing related work in this field and outline our contributions. In Section 4, we describe our proposed solution for solving the Industry 4.0 data interoperability and security challenges. In Section 5, we present the prototype of our solution. In Section 6, we discuss the results of the proposed solution and analyze the employed technologies. Finally, Section 7 includes the conclusion of the paper and future work insights.

2. Background

2.1. Distributed Ledgers

A DLT can be defined as a set of geographically distributed nodes that store and exchange data through a consensus mechanism. In contrast to a classic centralized database, DLTs do not depend on a centralized node, and consequently, they do not have a single point of failure [14]. DLTs generally use Peer-to-Peer (P2P) technology to exchange data. There are many types of DLTs. Blockchain is currently the most popular DLT since it is the technology behind cryptocurrencies like Bitcoin. In a blockchain, data is organized in "blocks" that are cryptographically linked to each other. However, blockchains tend to be slow and inefficient since consensus algorithms such as the widely used Proof-of-Work (PoW) have limited throughput, and high resource consumption [15]. The PoW algorithm effectively avoids malicious behavior in blockchains by requiring the transaction verifiers ("miners") to perform a certain amount of computational effort ("work") in exchange for a reward cryptocurrency. Apart from the heavy computational requirements, another issue is that in a blockchain, every node needs to store a copy of the entire chain, thus requiring each node to possess a significant amount of storage space.

Consequently, novel blockchains and different types of DLTs that intend to replace blockchains have been released. The most relevant and promising solution are DAG DLTs. DAGs were first introduced in [16] with the release of IOTA (https://www.iota.org/, accessed on 22 November 2022). In a DAG DLT, the nodes that issue a new transaction must approve two previous transactions and perform a small amount of computational processing to avoid spam in the network. Transactions can therefore be issued without fees, facilitating micro-transactions. DAG DLTs offer huge scalability and throughput, as the more transactions are issued, the faster and more secure the network becomes. Furthermore, the lack of mining makes DAGs highly efficient and suitable for lightweight devices. Thus, this type of DLT is much more suitable for resource-constrained environments that handle a huge number of transactions.

Due to the massive increase in distinct blockchain and DLT platforms over the last years, the interoperability issues have increasingly attracted the attention of the industry [17]. Naturally, there are many different use cases for which different blockchains have been designed. However, in such an interconnected world, isolated networks are not an option. The use of different blockchains and DLT could be enormously beneficial to take advantage of the latest state-of-the-art technological innovations.

Nonetheless, blockchain and DLT interoperability are not straightforward [18]. In response to this problem, some innovative solutions have been proposed. The most pioneer interoperability-oriented platform nowadays is Polkadot (https://polkadot.network/, accessed on 23 November 2022). Polkadot is a highly interoperable solution that consists of a main chain named "relay chain" that governs the network, along with multiple parallel chains that are fully compatible with each other, known as "parachains".

2.2. Smart Contracts and Oracles

Initially, blockchains could only process simple transactions. Consequently, in 2015, the Ethereum (https://ethereum.org/, accessed on 24 November 2022) project introduced the execution of smart contracts. Nonetheless, the concept of smart contracts is not new, since it was initially conceived in 1994 by Nick Szabo [19]. A smart contract is a program that is executed on top of a blockchain network. With smart contracts, the blockchain has greatly expanded its range of applications from simple financial transactions to more broad and complex applications in industry, smart homes, healthcare, etc. In the field of industry, blockchain and smart contracts could be used to establish automated and trustworthy agreements between different business partners, clients, and suppliers and increase the confidentiality, privacy, and security of IIoT data [20]. Nonetheless, many smart contracts require external information to make decisions properly. Besides the fact that off-chain data could be challenging to be accessed by a smart contract code, external dependability could also undermine the advantages of blockchain networks by removing decentralization and trust [21].

To solve the aforementioned issues, the concept of oracle has been introduced. In computer science, an oracle can be defined as a service that provides reliable data from outside a specific system [22]. However, centralized oracles introduce a single point of failure within blockchain networks. This issue might lead to the introduction of corrupted data inside smart contracts, which would compromise the whole blockchain network and make it pointless in terms of the security of the information. Thus, blockchain oracles are needed. A blockchain oracle is a decentralized oracle that is capable of analyzing the external world and providing trustworthy data to smart contracts [23]. A graphical representation of a decentralized oracle service is shown in Figure 2. Currently, there are many blockchain oracle services in the market, the best-known being ChainLink. ChainLink enables simple deployment of decentralized oracle networks that are capable of interacting with the Ethereum blockchain via Solidity smart contracts. Apart from ChainLink, there are other relevant solutions such as Augur, which is mostly focused on decentralized finance, and Gravity, which claims to be highly efficient and secure, but is in a too early stage of development [24].

However, taking into account the definition of oracle, we can state that any blockchain can be used as an oracle service. Nonetheless, oracle-oriented blockchains offer greater smart contracts compatibility and their software implementation graphical interface is oriented towards oracle monitoring. For example, most blockchain oracles incur economic costs, thus needing strict monitoring to maximize their efficiency and reduce costs. However, oracle-oriented services may have limited compatibility with other services or limited functionalities [25].

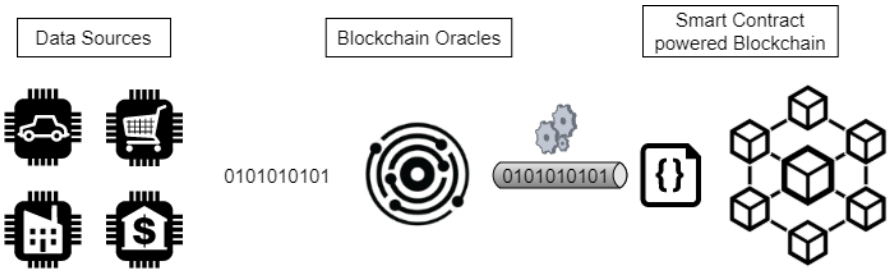

Figure 2. Blockchain Oracles representation.

2.3. Distributed Ledgers in Industry 4.0

Since the Industry 4.0 revolution started, enterprises have focused on digitizing their manufacturing and business processes. This approach increases efficiency, productivity and profits [20]. However, there are many challenges that need to be solved. These challenges are mostly related to the massive information exchange between a significant number of devices that are geographically distributed. Specifically, some of the most relevant

challenges are security, privacy, traceability, and interoperability [26]. Therefore, DLTs have been raised by many researchers and professionals as a possible solution to the aforementioned challenges. The use of DLTs could help eradicate possible single points of failure in industrial networks, along with guaranteeing the integrity of the data and providing traceability of the data from when it is generated up until it is processed at higher levels. Furthermore, smart contracts can provide secure and automated business agreements between various third parties, as well as maintenance and monitoring of industrial machines and processes.

Many big enterprises, such as Amazon, IBM, SAP, Jaguar, DNV-GL, etc., are already exploring the use of blockchain and even DAGs in their business processes. F. Chiacchio et al. [27] demonstrate the viability of blockchain and smart contracts in Industry 4.0 by studying the case of a blockchain-based technological solution for improving the packaging lines of an Italian factory. In this way, the actors that participate in the cycle can retrieve all sorts of information and guarantee the quality of the product.

2.4. Monitoring

Monitoring is a broad notion that can go from the classic concept of monitoring physical machines up to the more modern and software-oriented concept of monitoring [28]. Furthermore, monitoring has also evolved from an on-site approach to a remote approach due to the evolution of wireless technologies. Even though these concepts are not related at first sight, with the rise of Industry 4.0, there will be a growing number of industrial plants that are based on software and overall informatics-related technologies. Thus, both industrial monitoring as well as Information Technology (IT) monitoring will have to coexist. Therefore, in this subsection, we give a few insights on industrial remote monitoring and software monitoring, since, in this work, we cover the monitoring of an industrial environment that includes disruptive IT solutions.

Industrial remote monitoring consists of tracking in real time the data, performance, and security performance of a machine without the user being physically present at the equipment's site [29]. Remote monitoring helps industrial personnel perform a centralized tracking of many machines and even plants at the same time. Specifically, it enables technical personnel to visualize the manufacturing process in real-time by reading data from all the sensors throughout the facility at once. The retrieved information can be combined to have a detailed manufacturing insight. For example, in a filling machine, remote monitoring can track the remaining containers, the machine's actual speed, and how much liquid is remaining. A smart alarm scheme can also be assembled for problem reporting. Finally, remote monitoring can also be used to perform preventive and predictive maintenance. For example, monitoring systems can provide meaningful data regarding lifespan, output efficiency, and breakdown status.

IT monitoring is a complex activity, as many characteristics of many devices must be carefully analyzed to avoid performance degradation. IT monitoring is composed of three sections [30]: foundation, software, and interpretation. The foundation is the lowest part and includes the actual devices and their hardware. The software part includes the monitoring section and includes the analysis of the foundation devices. Finally, the interpretation section includes the gathered metrics, which are presented through graphs, often via a graphical interface dashboard. IT monitoring can be based on agents or be agentless. Agents are independent programs that must be installed on the monitored devices to collect data. Agentless monitoring relies on existing communication protocols to emulate agents, offering similar characteristics as the agent-based approach.

Typically, there are some critical aspects that must be monitored in IT [31]:

- CPU utilization and hardware health and availability.
- Bandwidth consumption between individual devices.
- Firewall and other cybersecurity-related programs, rules, and policies.
- Updates and overall configurations.
- Adherence to basic compliance measures.

- Scalability and throughput.

3. Related Work

In this section, we first analyze the most relevant works that are related to interoperable DLT networks and smart oracles in IoT and industrial environments. We also conduct a comparative study between the presented work and the related works regarding several characteristics. Finally, we also analyze the existing monitoring proposals in the industry and compare them with our monitoring approach.

3.1. Interoperable Blockchains and Oracle Services for Industry 4.0

P. Bellavista et al. [32] design a relay architecture based on Trusted Execution Environment (TEE) with the aim of providing trustworthy interoperability between blockchain networks in industrial environments. The authors claim that in an industry 4.0 ecosystem, it is impossible to have only one blockchain. The proposed solution makes use of an off-chain secure computation environment that is invoked by smart contracts. Nonetheless, this interoperability approach is achieved at high-performance costs and offers low scalability. Moreover, this solution relays on specific off-chain hardware equipment that might have vulnerabilities. Moreover, this solution only supports blockchains; thus, other solutions, such as DAGs, which are much more efficient in IoT environments, were not taken into account. Finally, the authors do not consider that industrial data might be heterogeneous, and they do not take into account secure methods of introducing external data in smart contracts.

Scheid et al. [33] present Bifröst, a modular blockchain interoperability API that acts like a notary agent. This API is currently available for seven blockchains. Thus, it has to be specifically adapted to each blockchain solution. However, this proposal incurs high latency to the network and has several critical security issues that might have no feasible solution. Furthermore, this API does not assure secure external data entry in blockchain smart contracts.

Y. Jiang et al. [34] aims to integrate DAG-type DLTs with a consortium blockchain by using sidechains. The consortium blockchain is used as the "main" chain to which several DAG sidechains are connected. To achieve interoperability, there are several notaries nodes that act like gateways between the main chain and its sidechains. This proposal might be useful to set an industrial scenario where IIoT data is processed by the DAGs at the data source level, and the consortium main chain is used to unify and exploit the data at a higher level. However, the proposed architecture adds a high grade of complexity, energy consumption, and latency to the network, since it employs the PoW consensus mechanism to guarantee decentralization and avoid the issues of the solution presented by E. Scheid et al. [33]. Furthermore, in this work, the heterogeneity of industrial data is not taken into account, and the main chain has no clear purpose.

Gao et al. [35] design a data exchange scheme by using an oracle service node that acts like a trusted notary between two or more blockchains. They also design a secure data migration protocol based on asymmetric encryption between the blockchains to avoid man-in-the-middle attacks. They also suggest novel methods of making the proposed scheme more applicable to real-world scenarios. However, this proposal creates a single point of failure in the network, thus making the use of blockchain pointless.

Wiraatmaja et al. [36] propose a custom-made oracle framework in JavaScript to enable safe data transactions between decentralized DLTs such as IOTA and Ethereum, and other decentralized solutions such as IPFS. However, similar to the work presented by Gao et al. [35], this architecture uses centralized notaries that create a single point of failure.

Unlike the works that have been described above, we design an efficient and trustworthy industrial scheme based on blockchain where we aim to achieve data integrity and interoperability throughout the whole process from where data is generated up until it is standardized and managed at a higher level. We start from a scenario where raw IIoT

data is processed by efficient production line DAG DLTs and design a data homogenization process using decentralized oracles along with a monitoring interface for improved data analytics. Finally, we store the resulting homogenized data in an interoperable plant blockchain for trustworthy data management and processing of the homogenized IIoT data originating in many production lines.

Table 1 shows a comparison between the related works and the presented work. We compare six characteristics: the used approach to achieve interoperability: trusted hardware, notary [18], or sidechains [37]) (Approach) if the proposal includes oracles (Oracles) if the solution is completely decentralized (Decentralized) if it does not incur a significant burden (Efficient) if it guarantees the integrity of the data throughout the whole process (Data Integrity) and the types of DLTs that it supports (Support). In our case, we employ a notary scheme approach to exchange data between distinct DLTs. We use oracles to provide trustworthy external data within the homogenization process. Our solution is completely decentralized throughout the whole process, and it does not incur a significant burden in any phase, thus, is efficient. Finally, it guarantees data integrity throughout the whole process and supports blockchain and DAG DLTs.

Table 1. Related works comparison study.

	Approach	Oracles	Decentralized	Efficient	Data Integrity	Support
[32]	Trusted HW	✗	✗	✗	✓	Blockchain
[33]	Notary	✗	✗	✓	✗	Many DLTs
[34]	Sidechains	✗	✓	✗	✓	Blockchain & DAG
[35]	Notary	✓	✗	✓	✗	Blockchain
[36]	Notary	✓	✗	✓	✗	Blockchain & DAG
This work	Notary	✓	✓	✓	✓	Blockchain & DAG

3.2. Modern Industry Monitoring

Industrial monitoring is a broad area with many relevant works [38,39]. However, in this subsection, we focus on relevant monitoring schemes that are relatively recent and include some degree of technological application (i.e., software, IoT, wireless networking, etc.), since our work is included within the modern framework of Industry 4.0. We mainly aim to analyze and compare the coverage depth of the monitoring systems within the scenario for which they are used.

Shi and Gindy [40] present an automatic software-based monitoring architecture that is capable of performing automatic online acquisition, presentation, and analysis of sensor signals. This monitoring system is able to acquire, analyze, and present the data simultaneously and automatically by using a multi-thread programming approach. The software was developed to function in a retriggerable manner so it can register signals successively without manual interference.

The work presented by Sung and Hsu [41] employs ZigBee [42] wireless transmission technology in combination with embedded hardware to perform comprehensive remote monitoring of the industrial equipment. This proposal is intended to improve the safety and efficiency of industrial environments by measuring critical aspects such as energy consumption, temperature, or CO_2 levels.

Zhao et al. [43] design a modern monitoring system for IIoT environments. This proposal intends to provide real-time monitoring to improve technical and financial matters within industrial companies. Field-programmable Gate Arrays (FPGAs) are used in this work due to their high reliability and processing speed. Finally, a developed IoT platform provides remote real-time visualization.

A recent monitoring system is presented by W. Chen [44]. This paper presents a reference architecture for IoT data monitoring and designs a theoretical model of the system. The authors also address several issues that can be found in modern manufacturing environments, such as the large amounts of data that has to be processed, the integration of key technologies such as Wireless Sensors Network (WSN) [45] or Radio-Frequency Identification (RFID) [46], and the correlation between data.

Magadán et al. [47] design a low-cost scheme for real-time monitoring of electric motors. The developed module gathers real-time information on the vibrations and temperature of the electric motors and stores it in a lightweight IoT analytic platform. The information is further processed and analyzed to provide operating reports and improvement suggestions. Using this proposal, several anomalies of electric motors have been successfully identified and mitigated. Furthermore, relevant predictive maintenance reports have been generated. The authors also intend to use machine learning to predict better and mitigate failures.

Mourtzis et al. [48] design a monitoring system based on an augmented reality mobile application tool for real-time machine monitoring and maintenance. The system includes all the required connections from the sensors to enable precise monitoring of the remaining operating lapse, plan maintenance tasks on the available time slots, update the machine schedule based on the length of the maintenance and connect to a remote database. Moreover, to improve the maintenance instructions and secure the generated result, the maintenance technician is aided by a set of functionalities, such as an algorithm that breaks down the assembly tasks and pre-creates the graphical interface. The proposed system increases interoperability, efficiency, and communication, providing useful data that can be further analyzed and transformed.

The main difference between the presented works and our own is that the purpose of our work is not to provide a novel approach to industrial monitoring. The main goal is to provide a broader approach that is adapted to the disruptive technologies that are being applied in this paper. In our case, apart from monitoring IIoT devices as is already done in other works, we intend to monitor other technologies such as IPFS, DLTs, and blockchain oracles. Furthermore, our measurements preserve data privacy since we employ a zero-trust approach and thus do not capture actual data. The necessity of this approach is to assure the maximum efficiency of the industrial processes, including the present IT technologies, and the maximum reduction of costs as well as cyber-attacks defense. As far as we know, there is no monitoring system that covers the monitoring of all technologies involved in an Industry 4.0 scenario.

Table 2 shows a comparison between the characteristics of the related works regarding monitoring systems and the one that we design in this work. We analyze the transmission technologies that each proposal is based on (Technology), if it covers the monitoring of IIoT devices (Covers IIoT) if it is based on some kind of software program (Software-based), if it covers the monitoring of disruptive Industry 4.0 technologies such as blockchain, AI, Edge Computing, etc. (Monitoring I4.0 Technologies) and if it assures the privacy of the data during the monitoring process (Data Privacy).

Table 2. Monitoring systems comparison.

	Technology	Covers IIoT	Software-Based	Monitoring I4.0 Technologies	Data Privacy
[40]	Internet	✗	✓	✗	✗
[41]	ZigBee	✗	✗	✗	✗
[43]	Internet	✓	✓	✗	✗
[44]	RFID	✓	✓	✗	✗
[47]	Internet	✓	✓	✗	?
[48]	Internet	✓	✓	✗	?
This	Internet	✓	✓	✓	✓

4. Interoperable Plant Blockchain for Homogenized Data via Smart Oracles

In this section, we describe the proposed solution for machine data interoperability and trustworthy storage of plant-level data. First, we describe the proposed data homogenization process using smart oracles, and then we present the design of a monitoring scheme for the proposed architecture.

Figure 3 depicts the proposed solution, in orange, on top of the motivating industrial scenario that was presented above. Specifically, in grey, we have N smart factories where the IIoT data is processed using DAG DLTs along with IPFS decentralized storage. Additionally, in orange, we have the proposed extension that we address in this work. We added a data homogenization service that makes use of blockchain oracles and has the resulting data stored in an interoperable external blockchain. On top of the scheme, we also have a monitoring system for the whole architecture.

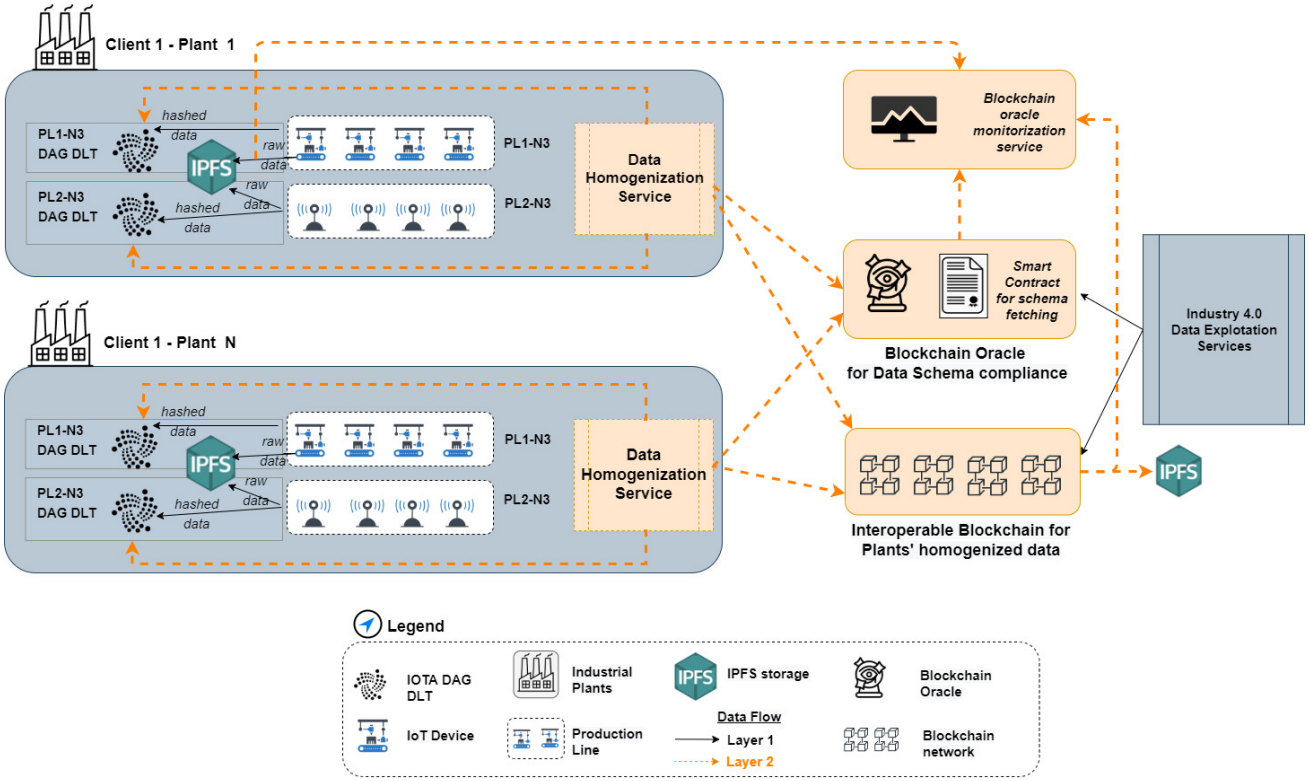

Figure 3. The proposed interoperable plant blockchain and data homogenization via decentralized Oracles scheme.

4.1. Data Homogenization via Decentralized Oracles

As mentioned in the motivating scenario, the actual IIoT data is stored inside an IPFS storage system, while the data-source DAGs would only store the hashes to reduce the storage burden of the DLTs. In the proposed scheme, after receiving and storing the raw IIoT data hashes from IPFS, a data homogenization service that is executed periodically would make a call to an external decentralized oracle service to retrieve the data model used for the data homogenization process. Blockchain oracles are needed since smart contracts are unable to access external data sources in a trustworthy manner. Hereafter, once the data model is received from the oracle, the data homogenization process starts its execution. The homogenization process consists of converting raw IIoT data into a standardized data scheme according to the given data model. Finally, the data homogenization service would then send the homogenized data to an interoperable plant blockchain, which in turn stores it inside the IPFS storage system and keeps its references within the immutable ledger. Figure 4 depicts the sequence diagram of the presented homogenization process.

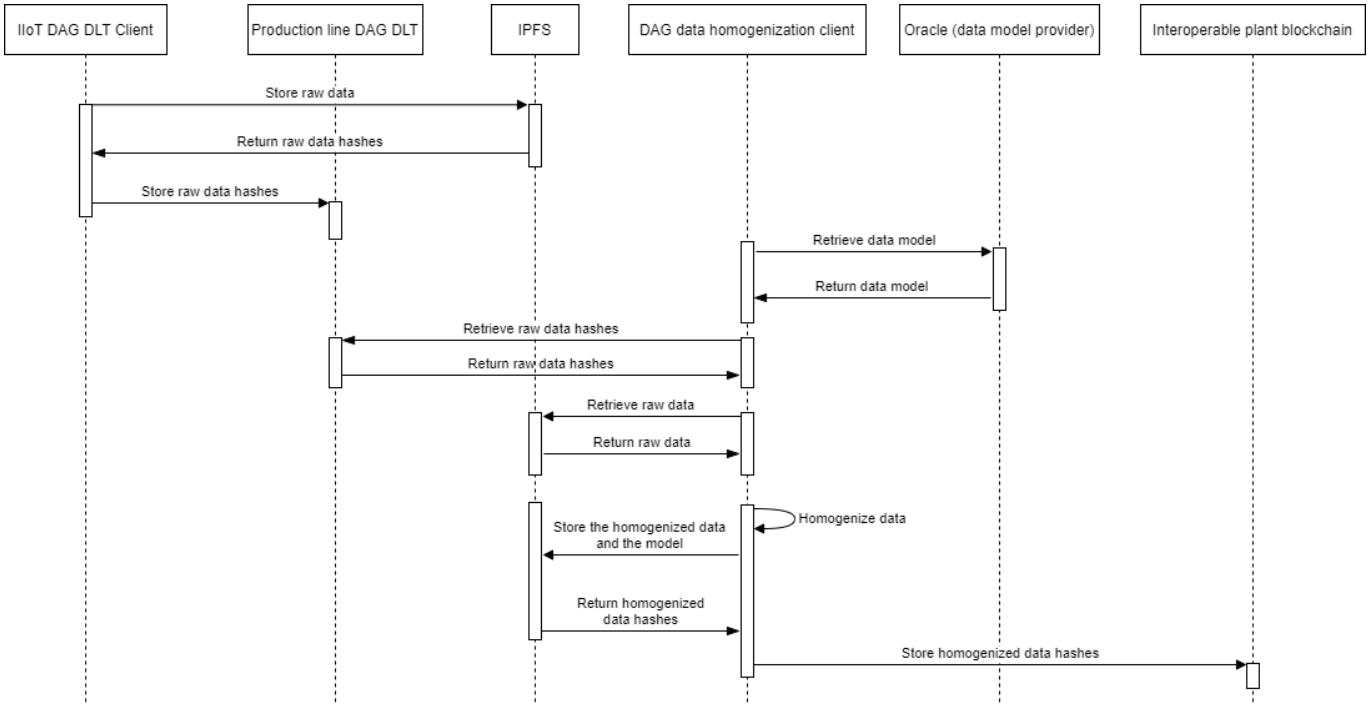

Figure 4. Sequence diagram of the proposed oracle-based architecture.

Therefore, the main purpose of the interoperable plant blockchain is to store and manage the smart plant securely homogenized data references and provide access control to IPFS. This blockchain would also unify the data management of different industrial plants belonging to the same business conglomerate. Finally, this ledger would act as a bridge between the DAG DLTs that process the data from IIoT devices inside production lines, and other hypothetical DLT connections with other organizations within a hypothetical decentralized business consortium network.

Consequently, interoperability capabilities are required at this level. To connect the production lines DAGs and the plant blockchain, we propose to make use of a smart contract-based notary scheme that interacts with a smart contract from the destination blockchain to transfer the data securely.

Application Example

One real-world example application of the approach described could be a system for collecting and storing data from sensors in an industrial plant. In this system, the raw data from the sensors would be stored in IPFS, and the hashes of this data would be recorded in

a DAG DLT. The data homogenization service would periodically retrieve a data model from a decentralized oracle service, and use this model to convert the raw sensor data into a standardized format. The homogenized data would then be stored in IPFS and recorded in the interoperable plant blockchain.

This system could be used to ensure the integrity and traceability of the sensor data, as the data would be stored in a decentralized and immutable manner. It could also help to facilitate data interoperability, as the standardized data format would make it easier for different systems and applications to make use of the data. Additionally, the use of oracles to retrieve the data model from an external source could allow the data homogenization process to be updated and improved over time, as the oracle could provide access to the most recent data model. Finally, this approach also enables the data homogenization process to be updated and improved over time.

4.2. Monitoring System Architecture

The purpose of the proposed monitoring system is to visualize and analyze the industrial data throughout the whole process, since it is generated at an IIoT level up until it is homogenized and exploited at a plant level, along with all the elements that intervene in the aforementioned process. These elements go from the IIoT devices to the DLTs, and IPFS storage until the blockchain oracles. A monitoring scheme covering all the elements apart from the IIoT devices is required to check the quality and integrity of the retrieved data, the status and usage of each element, accrued financial costs, and other financial information for future business-related use cases. Furthermore, in modern Industry 4.0, strict monitoring is also required so cyber-attacks or performance issues can be rapidly identified and mitigated. For example, monitoring the number of active devices, their effectiveness, or temperature can provide a holistic picture of the overall productivity and weaknesses of the plant. Monitoring of IT elements such as blockchains and oracles could help us identify performance bottlenecks, vulnerabilities, and cyber-attacks, and optimize the IT infrastructure associated costs [49].

To make the monitoring system as efficient and secure as possible, we followed three guidelines when designing it [50]: (i) the collection of metrics should not have a significant impact on the performance of the employed DLTs or on the data homogenization process, nor it should create a massive data traffic overhead; (ii) it should be as modular as possible to support different DLTs and oracle services; and lastly, (iii) the defined metrics should be defined to cover multiple industrial scenarios.

The proposed monitoring system consists of five modules: (1) IIoT data monitoring agent; (2) storage monitoring agent; (3) oracles monitoring agent; (4) the DLTs monitoring agent; and (5) the monitoring system core. Figure 5 shows the architecture of the monitoring system.

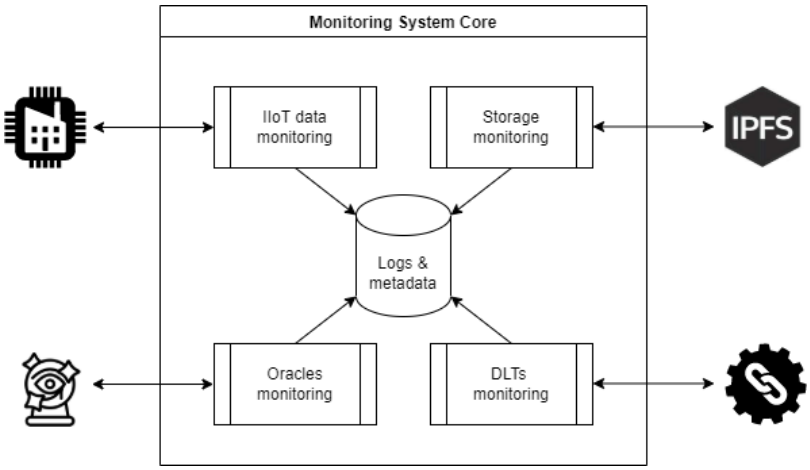

Figure 5. Monitoring system architecture.

Effective monitoring requires strategic placement of measurement probes, without affecting in any manner the flow of the data and thus causing more latency and overall poorer performance. Furthermore, the monitoring system must be designed in such a way so the data cannot be fraudulently accessed and tampered with through it. Consequently, similarly to other works such as [43], we propose the use of cheap lightweight FPGA devices with limited access to the actual data for the monitoring tasks. Thus, apart from avoiding illegal access to the data, using cheap devices avoids a significant increase in the operating costs of the architecture. Figure 6 shows the monitoring probes placement process across the presented architecture.

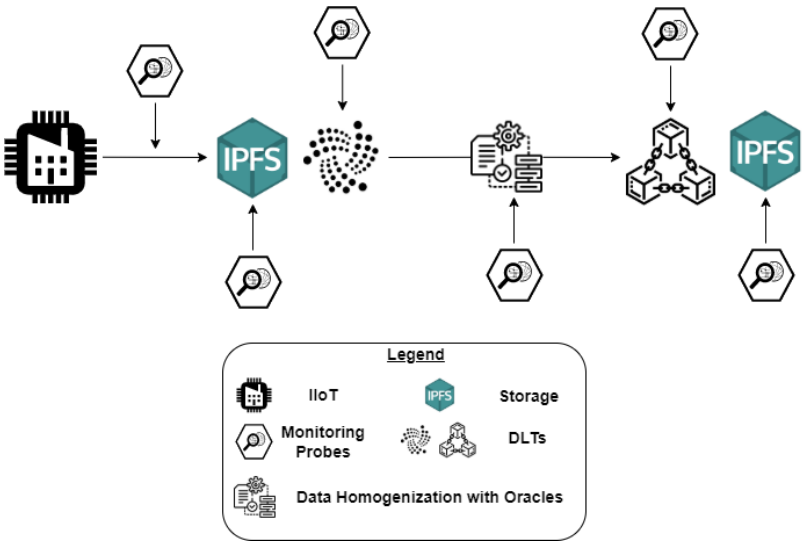

Figure 6. Monitoring probes placement across the presented process.

The monitoring process is composed of the following four steps:

1. First, we need to place a monitoring probe at the IIoT level so the original raw data can be monitored at the exact source before being stored or processed by any other agent.
2. The second step is to monitor the data when it arrives at the IPFS-DAG tandem. The comparison between the data that comes from the IIoT devices with the data that is finally stored and processed in IPFS and the DAG can help identify possible man-in-the-middle and DDoS attacks or mere transmission failures. Apart from monitoring the data, we can also monitor performance and other status data from the IPFS and DAG structures.
3. The third step is to monitor the data homogenization process, along with the employed oracles, so we can ensure that the process has been correctly executed. Regarding the oracle scheme, we can comprehensively examine the usage of the oracles and possible incurred costs, as well as possible performance and security issues.
4. Finally, the last probes would monitor the homogenized data at the plant level structures; the interoperable plant blockchain, and the related IPFS partition. Monitoring this part of the architecture helps us ensure that the homogenized data has been correctly stored and processed. We also need to make sure that there are no performance or security issues that can compromise the data prior to exploitation for business processes.

5. Implementation

In this section, we describe the implementation process of the prototype that we have developed to prove the viability of our proposal.

5.1. Data Homogenization Process with Decentralized Oracles

The machine data that we employ in this prototype is based on a real-world JSON structure that was obtained from actual industrial sensors. The IIoT devices from the simulated scenario collect data on the performance of the production line, the quality of the products being produced, timestamp data, diagnostics, and many other factors. These data can be used to optimize the production process and improve efficiency. When implementing the prototype, we simulate heterogeneous data similar to a real-world environment that was previously described in Section 1. Thus, this implementation aims to solve the challenges related to the security, integrity, and heterogeneity of industrial data.

Specifically, we simulate the following Industry 4.0 IIoT equipment:

- Smart sensors: These sensors can collect and transmit data about the performance and operation of machines, processes, and systems in real time.
- Predictive maintenance systems: These systems use machine learning and data analytics to predict when maintenance is needed, helping to reduce downtime and improve efficiency.
- Robotic systems: These systems can automate tasks such as material handling, assembly, and inspection, helping to increase productivity and reduce the need for manual labor.

We use IOTA as the production line DAGs to process the raw data since IOTA is currently known to be the most advanced DAG DLT solution [2], especially in terms of performance. As for the oracle service, there are many relevant options from which we can choose. As mentioned before, the most well-known oracle platform is ChainLink, which is focused on deploying Ethereum-compatible oracles.

However, in this work, we are not making use of the Ethereum blockchain since it lacks interoperability capabilities, along with low-performance capabilities. Furthermore, to provide interoperability, we have chosen Polkadot as our oracle service, as well as the blockchain solution in which we will store the homogenized data. In this case, we have implemented a relay chain in which the homogenized data is stored, along with a parachain that acts as an oracle service.

This implementation leaves the possibility of extending the functionality of our architecture by connecting other parachains in the future, which for example, could carry out the execution of smart contracts that could establish business relationships with other entities (i.e., suppliers, customers, etc.).

Finally, we use the JSON-based Eclipse Unide data model, as shown in Listing 1. The Unide data model is specifically designed for manufacturing processes, and it is trusted by several major parties, such as SAP or Bosch.

Listing 1. Eclipse Unide data model

```
{
  ``type'': ``object'',
  ``properties'': {
    ``content-spec'': {
      ``type'': ``string'',
      ``default'': ``urn:spec://eclipse.org/unide/machine-message#v3'',
      ``description'': ``Defines what the format version is''
    },
    ``device'': {
      ``$ref'': ``definitions.json#/definitions/device''
    },
    ``part'': {
      ``$ref'': ``definitions.json#/definitions/part''
    },
    ``measurements'': {
      ``allOf'': [
        {
          ``$ref'': ``definitions.json#/definitions/measurements''
        },
        {
          ``items'': {
            ``properties'': {
              ``series'': {
                ``required'': [
                  ``time''
                ]
              }
            }
          }
        }
      ]
    }
  },
  ``required'': [
    ``content-spec'',
    ``device'',
    ``measurements''
  ]
}
```

First, we have implemented a NodeJS client that emulates several industrial devices and periodically sends industrial raw data to an IPFS file system. Then the resulting IPFS hash is sent to the IOTA DAG DLT. Afterward, we implemented the data homogenization client in NodeJS. This client performs the following sequence of six tasks:

1. Access the IPFS raw data using the hash that is stored in the production line IOTA DAG DLT. An example of an industrial raw data JSON is shown in Listing 2.
2. Request the oracle service to retrieve the data model. Figure 7 shows the retrieval of the data model by the Polkadot parachain that we set as the oracles service.
3. Perform the data homogenization process. We defined the mapping between the raw data schema to the standard Eclipse Unide data model schema using the *jsonpath-object-transform* (https://www.npmjs.com/package/jsonpath-object-transform, accessed on 25 November 2022) NPM package. Listing 3 shows the NodeJS code of the transformation process of the data according to the Unide model.
4. To assure that the process was correctly executed, we validate the resulting JSON using the Ajv JSON schema validator (https://ajv.js.org/, accessed on 25 November 2022).
5. Add the used data model and the resulting homogenized data JSON to IPFS. An example of the homogenized raw data from Listing 2 is shown in Listing 4.
6. Send a transaction to the Polkadot relay chain (interoperable plant blockchain) to store the IPFS hash of the homogenized data. Figure 8 shows the stores IPFS hash pointer of the homogenized data within the Polkadot blockchain.

Listing 2. Raw industrial data JSON example

```
{
  ``device'': ``20131''
  ``metadata'': { ``origin'': ``StrokeData'' },
  ``keys'': {
    ``id_stroke'': 4705340,
    ``id_die'': 18,
    ``id_die_string'': ``69-14'',
    ``press_vel'': 17.1,
    ``isstrokecalssification'': 2,
    ``bvalidstroke'': false,
    ``dipartcounter'': 4704419
  },
  ``data'': [
    {
        ``filter'': true,
        ``cs_workmode'': 5,
        ``cs_partcntr_shift1'': 2,
        ``cs_partcntr_shift2'': 0,
        ``cs_partcntr_shift3'': 0,
        ``cs_availablesamples'': 1180315,
        ``cs_productionsamples'': 1110909,
        ``cs_measuredsamples'': 4401216,
        ``cs_oee'': 25.2409,
        ``ts'': ``2019-07-04T13:33:03.969Z'',
        ``series'': [Object]
    }
  ]
}
```

Listing 3. Data transformation in NodeJS code

```
const schema = dataModel;

var transform = require('jsonpath-object-transform');
var template = {
    ``type'': ``'',
    ``content-spec'': '$.metadata.origin',
    ``device'': {
        ``id'': '$.device'
    },
    ``part'': '$.keys',
    ``measurements'': '$..data'
}
const homogenizedData = transform(IPFSRawdata, dataModel, template);
```

Listing 4. Homogenized industrial data JSON according to the Eclipse Unide model

```
{
  ``type'': ``object'',
  ``content-spec'': ``StrokeData'',
  ``device'': {``id'': ``20131''},
  ``part'': {
    ``id_stroke'': 4705340,
    ``id_die'': 18,
    ``id_die_string'': ``69-14'',
    ``press_vel'': 17.1,
    ``isstrokecalssification'': 2,
    ``bvalidstroke'': false,
    ``dipartcounter'': 4704419,
    ``id'': 98
  },
  ``measurements'': [
    {
        ``filter'': true,
        ``cs_workmode'': 5,
        ``cs_partcntr_shift1'': 2,
        ``cs_partcntr_shift2'': 0,
        ``cs_partcntr_shift3'': 0,
        ``cs_availablesamples'': 1180315,
        ``cs_productionsamples'': 1110909,
        ``cs_measuredsamples'': 4401216,
        ``cs_oee'': 25.2409,
        ``ts'': ``2019-07-04T13:33:03.969Z'',
        ``series'': [Object]
    }
  ]
}
```

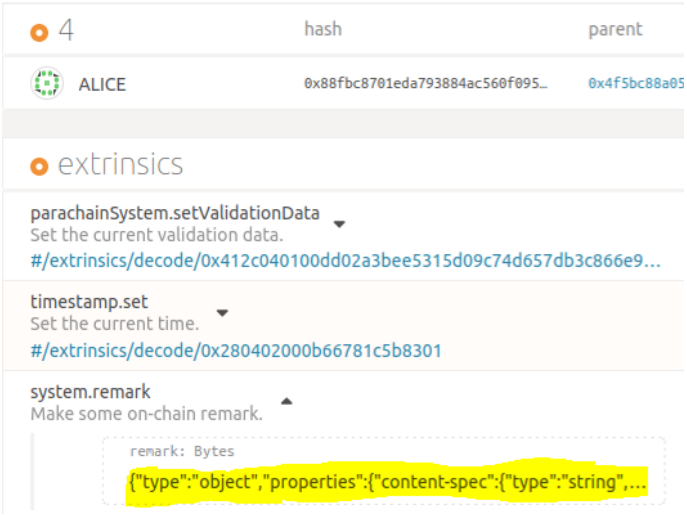

Figure 7. The data model (highlighted) after being retrieved by the Polkadot parachain oracles.

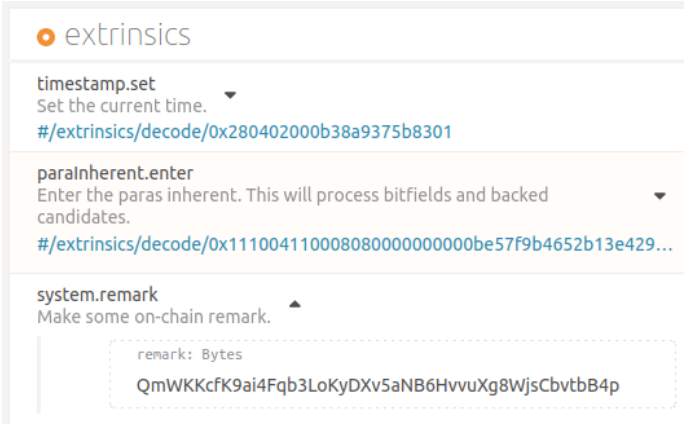

Figure 8. The reference of the homogenized data (system.remark) within the Polkadot relay chain.

5.2. Monitoring System

In this subsection, we present the implementation of the monitoring system that we designed for the proposed architecture. In this implementation, we use NodeJS and ExpressJS for data retrieval to provide compatibility with the rest of the architecture. For this preliminary version, we create an API that includes information on the four modules that we explain in Section 4.2. To properly show the monitoring data, we employ the ELK Stack. The aforementioned tools enable advanced real-time data visualization and monitoring with an easy-to-use dashboard. Thus, we do not need to create a dashboard from scratch, which would be a highly complex process. The ELK stack has been proven to be an ideal solution for our needs, as shown in other relevant works [51].

In the implemented API modules, we show the following information:

1. **The IIoT data monitoring.** This module shows several metrics that are related to the raw data that comes from industrial machines. We set the monitoring probes directly at the sensor level when the data is generated. We measure the total number of devices within the industrial plant, the number of active devices, the percentage of active devices, the number of sent messages (i.e., raw data transactions), the data generation rate, and the average temperature of the devices. Listing 5 shows an example of the returned IIoT metrics from the monitoring API.
2. **The DLTs monitoring.** This module shows several metrics that are related to IOTA (production line DLT) and Polkadot (interoperable plant blockchain). It shows the overall throughput of each DLT, the transaction validation times, the associated costs (if any), information about the peer nodes, the consensus model, throughput, number

of blocks, smart contract information (if any), etc. Listing 6 shows a trimmed example of the returned plant blockchain metrics from the monitoring API.

3. **The oracles monitoring.** This module shows several metrics that are related to the oracles. It shows which oracles have been used the most, which are currently available, the throughput capacity, the accumulated usage fees, the latest retrieved data, the quality of the data, etc. The "quality of data" metric shows whether the retrieved data model JSON is valid or not. Listing 7 shows a trimmed example of the returned blockchain oracles metrics from the monitoring API.
4. **The storage monitoring.** This module shows several metrics that are related to the storage of the data within the IPFS file system, such as performance, storage usage, peer nodes information, the generated hashes, version, IP addresses, etc. Listing 8 shows a trimmed example of the returned IPFS storage metrics from the monitoring API.

5.3. Results

In this subsection, we show the gathered results from the monitoring system based on a test run of the data homogenization architecture over several days. However, after running the process for several days, we observed that a 12 to 14 h simulation generates sufficiently robust and realistic results. Thus, we did not observe major variations in longer simulations. The simulated smart factory includes a total number of 500 IIoT devices that send random data at a random rate using the IoT-sim package (https://www.npmjs.com/package/iot-sim, accessed on 28 November 2022). During the tests, the number of active IIoT devices varies randomly to simulate a realistic scenario.

The main purpose of the simulations is to demonstrate the viability and security, and performance sufficiency of our architecture. Furthermore, the use of the designed monitoring system also demonstrates its usefulness.

Listing 5. IIoT devices monitoring API data example

```
{
``Total devices'':41,
``Number of active devices'':27,
``Devices ID list'':[
   [
      77579,
      56457,
      42678,
      90564,
      35677,
      38909,
      38322,
      98532,
      ...
   ]
],
``Percentage of active devices'':66,
``Number of sent messages'':41,
``Data generation rate each second'':2.7,
``Average temperature'':36
}
```

Listing 6. Polkadot plant blockchain monitoring API data example

```
{
   ``Validators'':{
      ``address'':``5GNJqTPyNqANBkUVMN1LPPrxXnFouWXoe2wNSmmEoLctxiZY'',
      ``balance'':``999,997,674,890,367,678'',
      ``nonce'':``478''
   },
   ``Account nonce'':``89'',
   ``Last block timestamp'':``1668064292'',
   ``Chain Info'':{
      ``ss58Format'':34,
      ``tokenDecimals'':[
         12
      ],
   },
   ``Account nonce'':``127'',
   ``Last block timestamp'':``1664197980005'',
   ``Blocks'':``4114'',
   ``Current throughput'':979,
   ``Max throughput capacity'':997,
   ``Smart Contracts'':``No smart contracts found''
}
```

Listing 7. Polkadot oracles monitoring API data example

```
{
   ``Validators'':{
      ``address'':``5GrwvaEF5zXb26Fz9rcQpDWS57CtERHpNehXCPcNoHGKutQY'',
      ``balance'':``999,993,268,520,263,875'',
      ``nonce'':``108''
   },
   ``Account nonce'':``47'',
   ``Last block timestamp'':``1664198880029'',
   ``Chain Info'':{
      ``ss58Format'':42,
      ``tokenDecimals'':[
         12
      ],
   },
   ``Blocks'':``1047'',
   ``Current throughput'':981,
   ``Max throughput capacity'':1003,
   ``Number of active oracles'':4,
   ``Latest retrieved data'': {...},
   ``Accumulated fees'':``0.013 EUR'',
   ``Quality of the data'':``Good''
}
```

Listing 8. IPFS storage monitoring API data example

```
{
``IPFS ID'':[
  {
    ``id'':``12D3KooWRuhwh6FSafpj88cBYZsTzprU1pybo9hPbcNddniPXQbE'',
    ``publicKey'':``CAESIO8ZQSXXfe3JQ3RHxnuBP9BiZjiRCoYzhsckxj81tHHt'',
    ``addresses'':[
      ``/ip4/10.0.2.15/tcp/4001/p2p/12D3KooWRuhwh6FSafpj88cBYZsTzprU1pybo9hPbcNddniPXQbE'',
      ``...''
    ]
  }
],
``IPFS version'':``0.13.0'',
``Config'':[
  {
    ``Addresses'':{
      ``API'':``/ip4/127.0.0.1/tcp/5001'',
      ``Gateway'':``/ip4/127.0.0.1/tcp/8082''
    },
    ``Datastore'':{
      ``HashOnRead'':false,
      ``StorageGCWatermark'':90,
      ``StorageMax'':``10GB''
    }
  ],
  ``Repo stats'':[
    {
      ``numObjects'':4345,
      ``repoSize'':25088708,
      ``repoPath'':``/home/denis/.ipfs'',
      ``version'':``fs-repo@12'',
      ``storageMax'':10000000000
    }
  ]
}
```

The raw data is processed by IOTA and IPFS at the production line level, and then it is homogenized and processed by a Polkadot plant blockchain. We also set a Polkadot parachain network of a random number of active oracles from a total number of ten. The simulation has been executed using a computer with an i7 9th generation CPU, 16 GB of RAM, and an SSD drive. We generate several Kibana graphs showing the following metrics generated from the monitoring system:

- **IIoT devices.** The number of active devices (Figure 9), the average temperature (Figure 10) and the Overall Equipment Effectiveness (OEE) (Figure 11). By generating these graphs, we can deeply analyze the production flow, identify possible device failures, overheating problems, and optimize the effectiveness of the industrial equipment by utilizing data-driven techniques as shown in [52].
- **Storage.** We measure the number of raw data JSONs that are inserted in IPFS from the IIoT devices, and compare it with the data that is finally processed by the IOTA DLT (i.e., processed JSON hashes in IOTA), as shown in Figure 12. These measurements could help us identify possible anomalies regarding the generating of the data from the IIoT devices. We also compare the size of the data inside IPFS compared to the amount of size of the processed IPFS hashes in IOTA, as shown in Figure 13. The data size monitoring could be useful to optimize storage space and also visualize the enormous storage burden we avoid putting on the DLT by using decentralized IPFS storage.
- **The DLTs.** The average throughput of IOTA and Polkadot during the simulation, as shown in Figure 14. Measuring the throughput of the DLTs is crucial in terms of data flow optimization and bottlenecks avoidance [53].
- **The oracles.** We measure the average number of oracles during the simulation, as shown in Figure 15. By analyzing the number of blockchain oracles that are involved in providing external data to our architecture, we are able to determine the degree of centralization of the system. For example, having only one active oracle would imply a high degree of centralization, which could affect the security of the whole industrial

architecture. Furthermore, the number of active oracles is also useful when calculating the associated costs of this service.

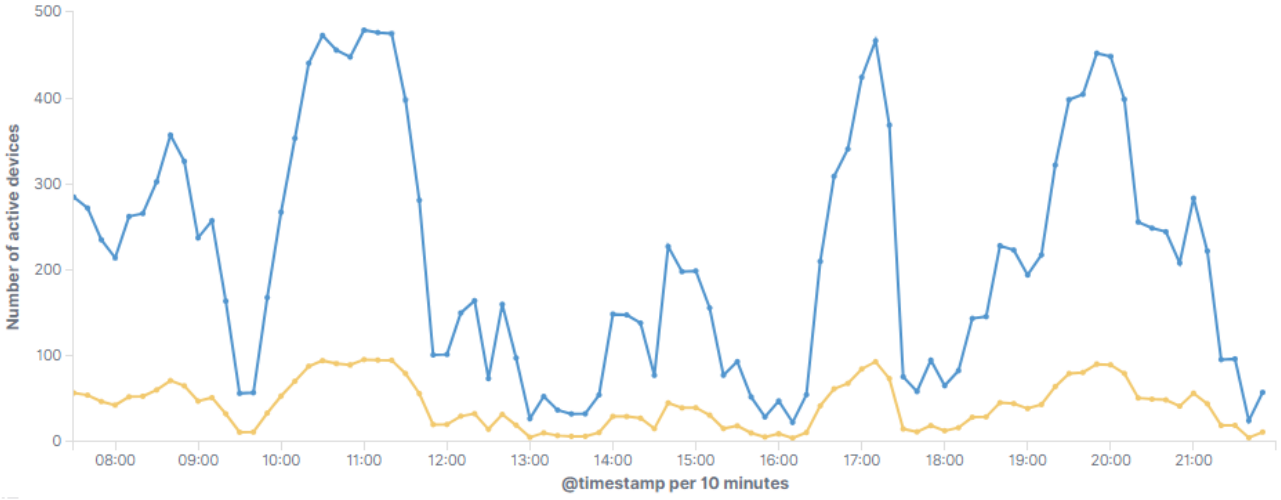

Figure 9. Active devices (absolute number in blue, percentage in orange).

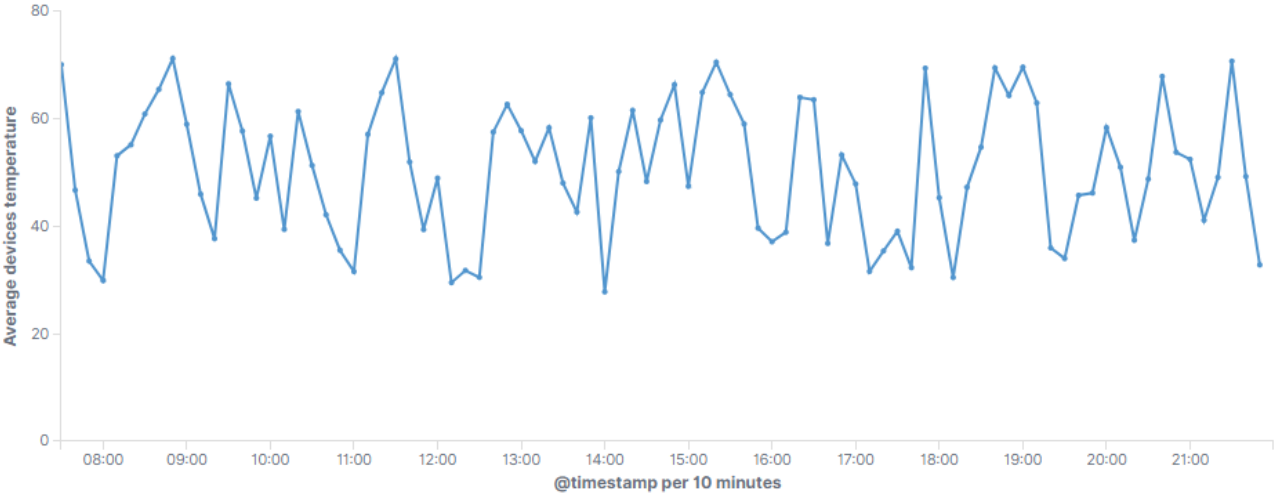

Figure 10. Average temperature of the devices (ºC).

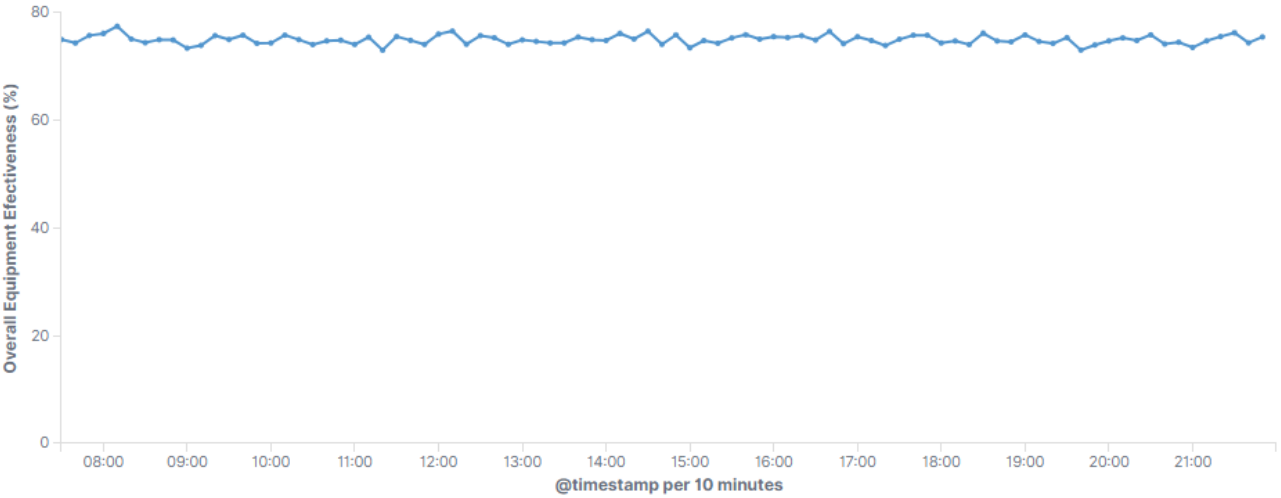

Figure 11. Overall Equipment Efectiveness (OEE).

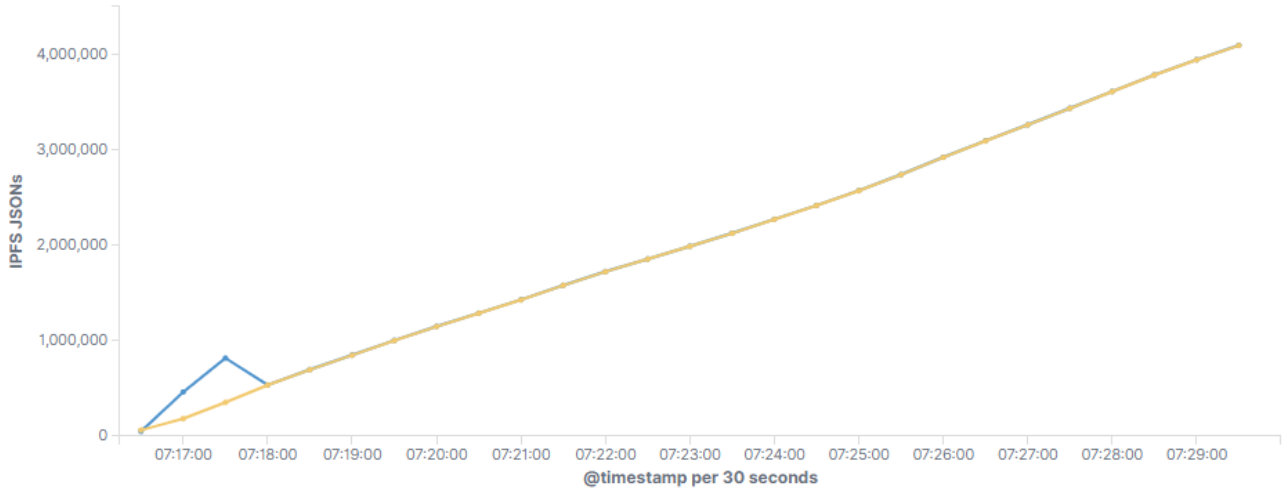

Figure 12. Number of processed JSONs: IPFS (blue) and IOTA (orange).

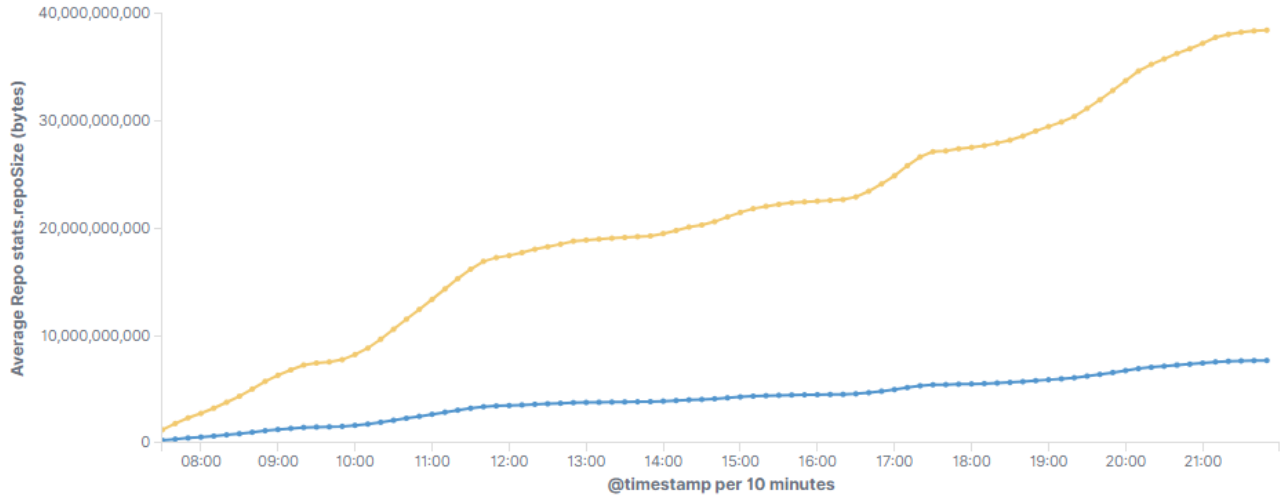

Figure 13. Comparison in bytes between storage in IPFS (blue) and IOTA (orange).

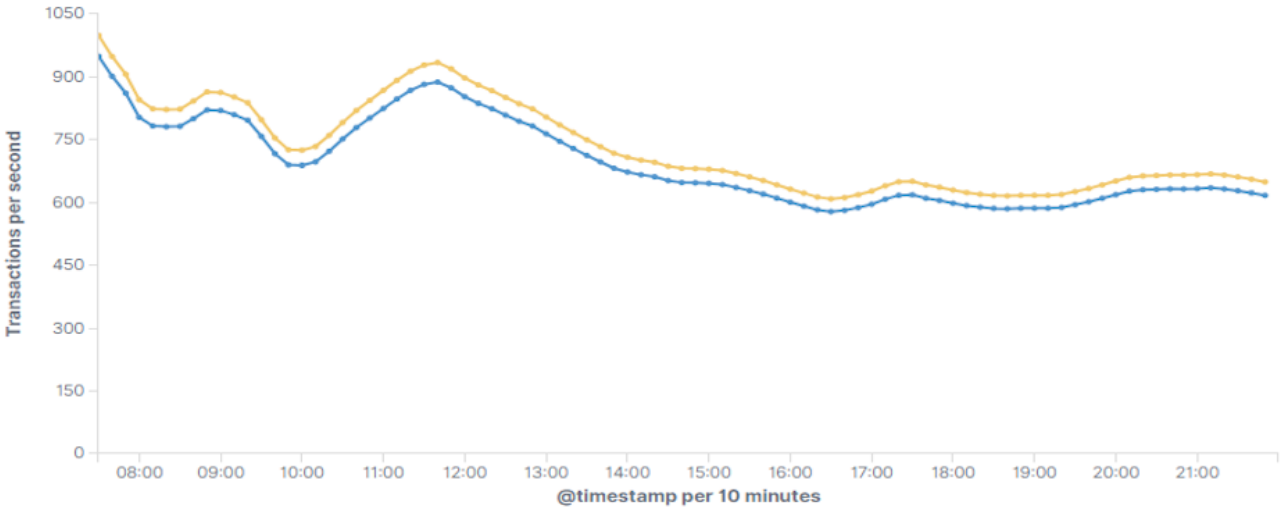

Figure 14. Average DLTs throughput: IOTA (orange) and Polkadot (blue).

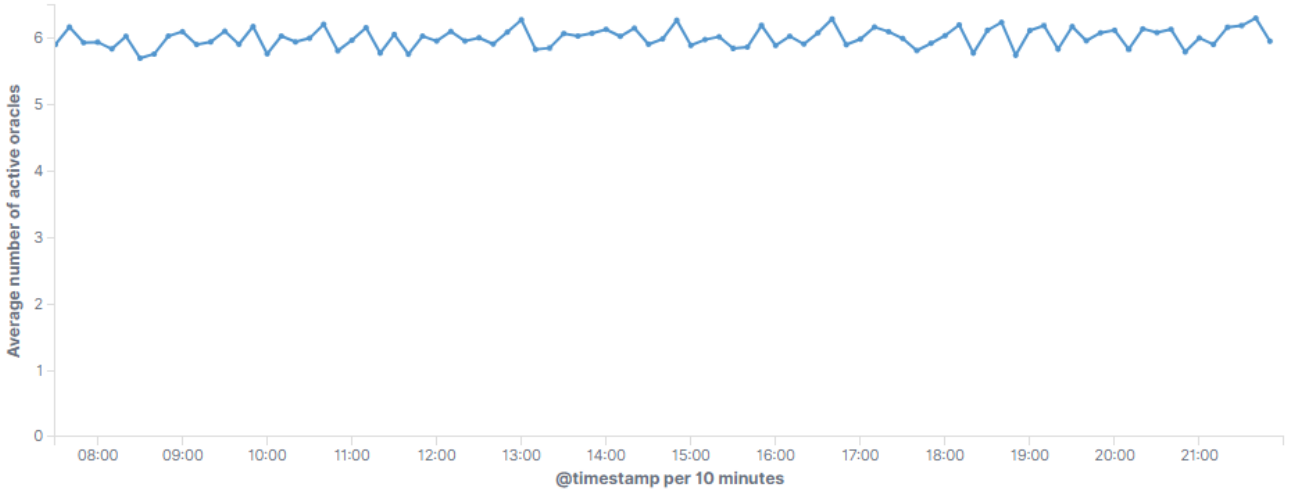

Figure 15. Average number of active oracles.

6. Discussion

6.1. Performance Analysis

In this work, we leverage decentralized oracles for data interoperability purposes, i.e., to securely gather the external IIoT data model and perform a homogenization process of machine raw data. Decentralized oracle platforms such as ChainLink intend to enable the development of fast, decentralized, and secure oracles for different applications. ChainLink, however, is strongly linked to the Ethereum ecosystem. On the other hand, Polkadot, despite not being focused on the oracle services field of application, is a highly versatile and interoperable platform in which an oracle solution can be implemented apart from other conventional uses. With Polkadot, we aim to achieve a high degree of interoperability to design a holistic DLT architecture for tomorrow's Industry 4.0.

However, despite the significant amount of security (i.e., data integrity) that a decentralized oracle mechanism brings to an architecture when providing data, some delays may be introduced due to the complexity of an additional decentralized network in between. Nonetheless, that would have been the case with ChainLink. By using Polkadot, we integrate the oracle platform with the plant blockchain since Polkadot "parachains" have direct connection and compatibility through the main "relay" chain. Furthermore, the performance of Polakdot is significantly higher than other blockchains, such as Ethereum, on which ChainLink is currently based. Moreover, the direct connection between the oracle parachain and the interoperable plant blockchain relay chain incurs near-zero latency. Therefore, we acknowledge that using a decentralized oracle service based on Polkadot for retrieving a JSON data model scheme does not have a significant impact on the performance of the scheme since, for each data model, only one request should be made. Finally, according to the measurements presented in Figure 15 from Section 5.3, on average, six oracles have been active for the given external data retrieval tasks. This number of oracles is appropriate to guarantee the complete decentralization of the architecture and almost instantaneously return the JSONs that comprise the Eclipse Unide data model.

As shown in the simulation results presented in Figure 14 from Section 5.3, in industrial environments, large amounts of data are generated, thus requiring significant processing and storage capacity. The presented monitoring system shows that our architecture is robust enough when handling great amounts of data. IOTA and Polkadot offer a great processing capacity, almost 1000 tps on average, which is sufficient in this type of environment. Even though Polkadot is not as fast as IOTA, this aspect is not relevant since the processing speed is most important where the data is generated. Furthermore, as shown in Figure 13 from Section 5.3, the use of IPFS greatly reduces the storage burden of the DLTs. In addition, the active devices measurements shown in Figure 9 from Section 5.3 prove that increasing the number of active devices does not incur a significant impact on performance.

The graphs generated from the continuous monitoring of the architecture help us to identify possible weak points in the process and, consequently, possible ways to improve the homogenization process, the data processing, as well as the management of possible costs. For example, the use of an oracle service could entail certain costs that should be optimized as much as possible by the companies. Thus, using the monitoring system, we could analyze and predict much more aspects, such as the incurred costs, the performance of the system, resource usage, device failures, etc. For example, in Figure 10 from Section 5.3, we analyze the average temperature of the devices, where we can see that it has significant fluctuations within the range of 30 and 70 degrees ºC, based on the intensity of the production process. Moreover, in Figure 11 from Section 5.3 we can visualize the effectiveness of the industrial equipment (OEE), which gives us clues about the effectiveness of the machines. This information shows that the effectiveness of the machines is highly optimal during the entire simulated period, but with a certain margin of improvement.

6.2. Security Analysis

Regarding the security of the information, we acknowledge that in the presented architecture, the integrity of the data is ensured during the whole process, from when the data is generated in production lines up until it is homogenized and finally exploited at the plant level. This is due to the use of secure DLT technologies throughout the whole process (i.e., production lines DAG DLTs, decentralized blockchain oracles for data homogenization, and plant processing blockchain). As shown in Figure 12 from Section 5.3, in the beginning, we simulate an attack in which great amounts of malicious data are generated. Nonetheless, the malicious data is finally discarded by the IOTA DLT. Such examples show that the monitoring of the architecture is also useful for visualizing possible cybersecurity attacks and other types of non-intentional incidents.

However, overall, the proposed architecture involves several components that may introduce potential security risks, including:

- IPFS. IPFS is a decentralized storage system, which means that it relies on a distributed network of nodes to store and retrieve data. While this can increase the availability and durability of the data, it also means that there is a risk that some nodes may not be trustworthy or may be compromised. To mitigate this risk, we implemented security measures such as encryption and access control to ensure that only authorized parties can access the data stored in IPFS.
- Decentralized oracles service. The proposed architecture involves using a decentralized oracle service to retrieve data models for the data homogenization process. This introduces a potential security risk, as oracle services are often centralized and may be subject to attacks or manipulation. To mitigate this risk, we use multiple oracle sources and implement security measures such as cryptographic signing and verification to ensure the integrity and authenticity of the data retrieved from the oracle service. Another security issue of oracles might be the supply of unreliable information [54]. However, monitoring the oracles could help mitigate this issue. Thus, in this work, we already make use of a monitoring system.
- Interoperable plant blockchain. The interoperable plant blockchain is responsible for storing and managing smart plant homogenized data references and providing access control to IPFS. To ensure the security of this blockchain, it is important to implement measures such as secure consensus algorithms, proper access control and permissions, and regular security audits. Additionally, we implement measures such as encryption and secure communication protocols to protect the data stored on the blockchain.
- Smart contract-based notary scheme: The data exchange scheme involves using smart contracts to securely transfer data between the production lines DAGs and the plant blockchain. It is important to ensure that these smart contracts are properly tested and audited to ensure their security and correctness. Additionally, we implement measures such as access control and permissions to ensure that only authorized parties can interact with the smart contracts.

- ELK-based monitoring. It is important to ensure that the ELK stack is properly configured and secured to protect against potential security risks and ensure the integrity and confidentiality of the data it processes. We use the latest version of the stack so we can ensure that all the current known vulnerabilities have been mitigated.

Overall, it is important to ensure that all components of the proposed architecture are properly secured, and that appropriate measures are taken to mitigate potential security risks. This process involves implementing a combination of technical and organizational measures such as encryption, access control, cryptographic signing, security audits, and secure communication protocols.

6.3. Comparison with Other Solutions

The most similar DLT-based proposal is the architecture proposed by Jiang et. al [34]. This work presents a cross-chain framework for efficient and secure IoT data management using a consortium blockchain as the control station and other blockchain platforms customized for specific IoT scenarios as the backbone for IoT devices. The framework merges transactions based on a notary mechanism and is implemented using Hyperledger Fabric and IOTA. However, this work shows a much lower throughput capacity (600 tps vs. 900 tps), and higher overall latency. Furthermore, the security robustness of the aforementioned architecture is not clear, since the authors tackle security concerns only by designing a simple access control system. Moreover, in this work, we go one step further and perform industrial data homogenization and exploitation instead of focusing exclusively on simple data transfer between DLTs. Finally, we also provide advanced monitoring of the whole scheme by using the ELK stack.

However, an industrial data processing, monitoring, and homogenization process can also be non-DLT based. In fact, nowadays, an overwhelming number of real-world industrial architectures are non-DLT based, since this technology is relatively new, and industrial processes take a considerable time to incorporate new technologies. However, here are some potential alternatives to DLTs that could be used for efficient and secure data management and homogenization in Industry 4.0:

- Centralized databases: A centralized database is a single repository of data that is managed and maintained by a single entity. This can be an efficient way to manage data in the IoT, as it allows for quick and easy access to data and can scale to handle large volumes of data. However, it can also be vulnerable to security threats, as a single point of failure can compromise the entire system. Furthermore, centralized databases could have serious bottlenecks and collapse in the face of a large amount of data that needs to be processed and homogenized.
- Peer-to-peer networks: Peer-to-peer networks allow devices to communicate directly with each other without the need for a central server or authority. This can be an effective way to manage data in the IoT, as it allows for decentralized control and can be highly scalable. However, it can also be less secure, as it relies on the security and reliability of individual devices, and the lack of a robust consensus and data blocks cryptography links, as is the case of the most used DLTs.
- Cloud-based solutions: Cloud-based solutions allow data to be stored and accessed on remote servers, which can be accessed over the internet. This can be a convenient and scalable way to manage data in IIoT, as it allows for easy access to data from any location. However, it can also be less secure, as data is stored on servers that may not be physically secure. Furthermore, cloud storage usually entails much higher economic costs than DLTs, especially compared to the more advanced solutions such as IOTA, which does not require fees, or Polkadot, whose fees are low or even zero in private networks.

Thus, our complete architecture not only ensures data integrity and security at every stage of the process but also delivers high performance for handling large amounts of IIoT data. Additionally, it is designed to be cost-effective, making it an attractive solution

for businesses looking to leverage the benefits of IIoT with relatively low monetary costs. Furthermore, the implemented monitoring system also provides comprehensive real-time analysis, threat detection, and optimization suggestions across the whole process.

7. Conclusions and Future Work

In this paper, we design a homogenization process for industrial IIoT data using decentralized oracles. We store the resulting data in an interoperable plant blockchain to guarantee the integrity of the data during the whole process, from when it is generated at each production line up until it is exploited at a plant level. We also present the design of a monitoring system that aims to provide a graphical representation of the whole process. Finally, we describe the implementation process in which we employ several cutting-edge technologies, such as IOTA DAG DLT, the Polkadot interoperable blockchain as an oracle service and storage blockchain, and the IPFS decentralized storage solution.

The use of the aforementioned technologies enables industrial companies to process and exploit the industrial data in an efficient manner (i.e., with high throughput and efficiency) while also guaranteeing the integrity and immutability of the data throughout the whole process. Furthermore, the use of an interoperable DLT such as Polkadot with automated smart contracts functionality allows companies to expand the aforementioned benefits to further networks and business processes in which there is a wide variety of different stakeholders.

In future work, we intend to develop a more automatized data homogenization process based on Model Driven Development (MDD) techniques. Despite the fact that in this work, we employed IIoT data that was generated by real-world industrial machines, the implementation and evaluation were performed in a laboratory environment. Thus, in a future work plan, if possible, we intend to go one step further and conduct on-field experiments in a real Industry 4.0 plant. Finally, the gathered data can also be analyzed and processed using AI to improve the production process and predict failures.

Author Contributions: Conceptualization, D.S., P.G.-G., J.U., L.M. and A.U.; methodology, D.S, P.G.-G., L.M. and J.U.; software, D.S. and P.G.-G.; validation, D.S., P.G.-G., L.M. and J.U.; formal analysis, D.S., P.G.-G., L.M. and J.U.; investigation, D.S., P.G.-G. and J.U.; writing—original draft preparation, D.S.; writing—review and editing, D.S., P.G.-G., J.U., L.M. and A.U.; visualization, D.S., P.G.-G., L.M., J.U. and A.U.; supervision, P.G.-G., L.M., J.U. and A.U.; project administration, D.S., P.G.-G., L.M. and J.U.; funding acquisition, A.U. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been financed by the European Commission through the Horizon Europe program under the IDUNN project (grant agreement number 101021911). It was also partially supported by the Ayudas Cervera para Centros Tecnológicos grant of the Spanish Centre for the Development of Industrial Technology (CDTI) under the project EGIDA (CER-20191012), and by the Basque Country Government under the ELKARTEK program, project ELKARTEK program, project REMEDY - REal tiME control and embeddeD securitY (KK-2021/00091).

Data Availability Statement: Not applicable.

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

References

1. Lasi, H.; Fettke, P.; Kemper, H.G.; Feld, T.; Hoffmann, M. Industry 4.0. *Bus. Inf. Syst. Eng.* **2014**, *6*, 239–242. [CrossRef]
2. Bhandary, M.; Parmar, M.; Ambawade, D. A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; pp. 827–832.
3. Liu, Y.; Wang, K.; Lin, Y.; Xu, W. Lightchain: A lightweight blockchain system for industrial internet of things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3571–3581. [CrossRef]
4. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, Big Island, HI, USA, 13–17 March 2017; pp. 618–623.
5. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight Blockchain for Healthcare. *IEEE Access* **2019**, *7*, 149935–149951. [CrossRef]

6. Divya, M.; Biradar, N.B. IOTA-Next Generation Block chain. *Int. J. Eng. Comput. Sci.* **2018**, *7*, 23823–23826. [CrossRef]
7. Stefanescu, D.; Galán-García, P.; Montalvillo, L.; Unzilla, J.; Urbieta, A. Towards a Holistic DLT Architecture for IIoT: Improved DAG for Production Lines. In Proceedings of the International Congress on Blockchain and Applications, Barcelona, Spain, 16–18 November 2022; Prieto, J., Partida, A., Leitão, P., Pinto, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 179–188.
8. Wu, Y.; Dai, H.N.; Wang, H. Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0. *IEEE Internet Things J.* **2021**, *8*, 2300–2317. [CrossRef]
9. Jirkovsky, V.; Obitko, M.; Marik, V. Understanding data heterogeneity in the context of cyber-physical systems integration. *IEEE Trans. Ind. Inform.* **2017**, *13*, 660–667. [CrossRef]
10. Roman, R.; Najera, P.; Lopez, J. Securing the Internet of Things. *Computer* **2011**, *44*, 51–58. [CrossRef]
11. Büchi, G.; Cugno, M.; Castagnoli, R. Smart factory performance and Industry 4.0. *Technol. Forecast. Soc. Chang.* **2020**, *150*, 119790. [CrossRef]
12. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
13. Stefanescu, D.; Galán-García, P.; Montalvillo, L.; Unzilla, J.; Urbieta, A. Interoperable Industry 4.0 Plant Blockchain and Data Homogenization via Decentralized Oracles. In Proceedings of the International Congress on Blockchain and Applications, Barcelona, Spain, 16–18 November 2022.
14. Di Pierro, M. What Is the Blockchain? *Comput. Sci. Eng.* **2017**, *19*, 92–95. [CrossRef]
15. Dorri, A.; Jurdak, R. Tree-Chain: A Fast Lightweight Consensus Algorithm for IoT Applications. In Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, Australia, 16–19 November 2020.
16. Popov, S. *The Tangle*; Technical Report; IOTA Foundation: Berlin, Germany, 2018.
17. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards Blockchain Interoperability. In Proceedings of the International Conference on Business Process Management: Blockchain and Central and Eastern Europe Forum, Vienna, Austria, 1–6 September 2019; Di Ciccio, C., Gabryelczyk, R., García-Bañuelos, L., Hernaus, T., Hull, R., Indihar Štemberger, M., Kő, A., Staples, M., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 3–10.
18. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* **2021**, *54*, 1–41. [CrossRef]
19. Szabo, N. Smart contracts: Building blocks for digital markets. *Extropy J. Transhumanist Thought* **1996**, *18*, 28.
20. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]
21. Al-Breiki, H.; Rehman, M.H.U.; Salah, K.; Svetinovic, D. Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access* **2020**, *8*, 85675–85685. [CrossRef]
22. Mammadzada, K.; Iqbal, M.; Milani, F.; García-Bañuelos, L.; Matulevičius, R. Blockchain Oracles: A Framework for Blockchain-Based Applications. In Proceedings of the International Conference on Business Process Management: Blockchain and Robotic Process Automation Forum, Seville, Spain, 13–18 September 2019; Asatiani, A., García, J.M., Helander, N., Jiménez-Ramírez, A., Koschmider, A., Mendling, J., Meroni, G., Reijers, H.A., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 19–34.
23. Sheldon, M.D. Auditing the Blockchain Oracle Problem. *J. Inf. Syst.* **2020**, *35*, 121–133. [CrossRef]
24. Ezzat, S.K.; Saleh, Y.N.; Abdel-Hamid, A.A. Blockchain Oracles: State-of-the-Art and Research Directions. *IEEE Access* **2022**, *10*, 67551–67572. [CrossRef]
25. Caldarelli, G. Overview of Blockchain Oracle Research. *Future Internet* **2022**, *14*, 175. [CrossRef]
26. 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.
27. Chiacchio, F.; D'Urso, D.; Compagno, L.; Chiarenza, M.; Velardita, L. Towards a Blockchain Based Traceability Process: A Case Study from Pharma Industry. In Proceedings of the IFIP International Conference on Advances in Production Management Systems. Production Management for the Factory of the Future, Austin, TX, USA, 1–5 September 2019; Ameri, F.; Stecke, K.E.; von Cieminski, G.; Kiritsis, D., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 451–457.
28. Henao-Hernández, I.; Solano-Charris, E.L.; Muñoz-Villamizar, A.; Santos, J.; Henríquez-Machado, R. Control and monitoring for sustainable manufacturing in the Industry 4.0: A literature review. *IFAC-PapersOnLine* **2019**, *52*, 195–200. . [CrossRef]
29. Pătru, G.C.; Trancă, D.C.; Costea, C.M.; Rosner, D.; Rughiniş, R.V. LoRA based, low power remote monitoring and control solution for Industry 4.0 factories and facilities. In Proceedings of the 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), Galati, Romania, 10–12 October 2019; pp. 1–6.
30. Gao, J.; Zhu, E.; Shim, S.; Chang, L. Monitoring software components and component-based software. In Proceedings of the 24th Annual International Computer Software and Applications Conference (COMPSAC2000), Taipei, Taiwan, 25–28 October 2000; pp. 403–412.
31. van Hoorn, A.; Waller, J.; Hasselbring, W. Kieker: A Framework for Application Performance Monitoring and Dynamic Software Analysis. In Proceedings of the 3rd ACM/SPEC International Conference on Performance Engineering, Boston, MA, USA, 22–25 April 2012; Association for Computing Machinery: New York, NY, USA, 2012; pp. 247–248.

32. Bellavista, P.; Esposito, C.; Foschini, L.; Giannelli, C.; Mazzocca, N.; Montanari, R. Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing. *Sensors* **2021**, *21*, 4955. [CrossRef]
33. Scheid, E.J.; Hegnauer, T.; Rodrigues, B.; Stiller, B. Bifr'ost: A Modular Blockchain Interoperability API. In Proceedings of the Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 14–17 October 2019; pp. 332–339.
34. Jiang, Y.; Wang, C.; Wang, Y.; Gao, L. A cross-chain solution to integrating multiple blockchains for IoT data management. *Sensors* **2019**, *19*, 2042. [CrossRef]
35. Gao, Z.; Li, H.; Xiao, K.; Wang, Q. Cross-chain oracle based data migration mechanism in heterogeneous blockchains. In Proceedings of the International Conference on Distributed Computing Systems, Singapore, 29 November–1 December 2020; pp. 1263–1268.
36. Wiraatmaja, C.; Zhang, Y.; Sasabe, M.; Kasahara, S. Cost-Efficient Blockchain-Based Access Control for the Internet of Things. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6.
37. Singh, M.; Aujla, G.S.; Bali, R.S. ODOB: One drone one block-based lightweight blockchain architecture for internet of drones. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS 2020), Toronto, ON, Canada, 6–9 July 2020; pp. 249–254.
38. Williams, R.; Jia, X.; West, R.; Wang, M.; Cullivan, J.; Bond, J.; Faulks, I.; Dyakowski, T.; Wang, S.; Climpson, N.; et al. Industrial monitoring of hydrocyclone operation using electrical resistance tomography. *Miner. Eng.* **1999**, *12*, 1245–1252. . [CrossRef]
39. Holah, J.T., Industrial Monitoring: Hygiene in Food Processing. In *Biofilms — Science and Technology*; Melo, L.F., Bott, T.R., Fletcher, M., Capdeville, B., Eds.; Springer: Dordrecht, The Netherlands, 1992; pp. 645–659. [CrossRef]
40. Shi, D.; Gindy, N.N. Industrial Applications of Online Machining Process Monitoring System. *IEEE/ASME Trans. Mechatron.* **2007**, *12*, 561–564. [CrossRef]
41. Sung, W.T.; Hsu, Y.C. Designing an industrial real-time measurement and monitoring system based on embedded system and ZigBee. *Expert Syst. Appl.* **2011**, *38*, 4522–4529. [CrossRef]
42. Safaric, S.; Malaric, K. ZigBee wireless standard. In Proceedings of the Proceedings ELMAR 2006, Zadar, Croatia, 7–9 June 2006; pp. 259–262.
43. Zhao, L.; Brandao Machado Matsuo, I.; Zhou, Y.; Lee, W.J. Design of an Industrial IoT-Based Monitoring System for Power Substations. *IEEE Trans. Ind. Appl.* **2019**, *55*, 5666–5674. [CrossRef]
44. Chen, W. Intelligent manufacturing production line data monitoring system for industrial internet of things. *Comput. Commun.* **2020**, *151*, 31–41. [CrossRef]
45. Seah, W.K.; Eu, Z.A.; Tan, H.P. Wireless sensor networks powered by ambient energy harvesting (WSN-HEAP) - Survey and challenges. In Proceedings of the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Aalborg, Denmark, 17–20 May 2009; pp. 1–5.
46. Yao, W.; Chu, C.H.; Li, Z. The use of RFID in healthcare: Benefits and barriers. In Proceedings of the 2010 IEEE International Conference on RFID-Technology and Applications, Guangzhou, China, 17–19 June 2010; pp. 128–134.
47. Magadán, L.; Suárez, F.; Granda, J.; García, D. Low-cost real-time monitoring of electric motors for the Industry 4.0. *Procedia Manuf.* **2020**, *42*, 393–398. [CrossRef]
48. Mourtzis, D.; Vlachou, E.; Zogopoulos, V.; Fotini, X. Integrated Production and Maintenance Scheduling Through Machine Monitoring and Augmented Reality: An Industry 4.0 Approach. In Proceedings of the IFIP International Conference on Advances in Production Management Systems. The Path to Intelligent, Collaborative and Sustainable Manufacturing, Hamburg, Germany, 3–7 September 2017; L'odding, H., Riedel, R., Thoben, K.D., von Cieminski, G., Kiritsis, D., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 354–362.
49. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted Business Process Monitoring and Execution Using Blockchain. In Proceedings of the International Conference on Business Process Management, Rio de Janeiro, Brazil, 18–22 September 2016; La Rosa, M.; Loos, P.; Pastor, O., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 329–347.
50. Raposo, D.; Rodrigues, A.; Sinche, S.; Sá Silva, J.; Boavida, F. Industrial IoT Monitoring: Technologies and Architecture Proposal. *Sensors* **2018**, *18*, 3568. [CrossRef]
51. Rochim, A.F.; Aziz, M.A.; Fauzi, A. Design Log Management System of Computer Network Devices Infrastructures Based on ELK Stack. In Proceedings of the 2019 International Conference on Electrical Engineering and Computer Science (ICECOS), Batam Island, Indonesia, 2–3 October 2019; pp. 338–342.
52. Majeed, A.; Lv, J.; Peng, T. A framework for big data driven process analysis and optimization for additive manufacturing. *Rapid Prototyp. J.* **2018**, *25*, 30 –321. [CrossRef]
53. Zhao, W.; Jiang, C.; Gao, H.; Yang, S.; Luo, X. Blockchain-enabled cyber–physical systems: A review. *IEEE Internet Things J.* **2020**, *8*, 4023–4034. [CrossRef]
54. Bartholic, M.; Laszka, A.; Yamamoto, G.; Burger, E.W. A Taxonomy of Blockchain Oracles: The Truth Depends on the Question. In Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China, 2–5 May 2022; pp. 1–15.