automation

MDPI

*Article*

# The Road to Accountable and Dependable Manufacturing

**Jan Pennekamp [1,*], Roman Matzutt [1], Salil S. Kanhere [2], Jens Hiller [1] and Klaus Wehrle [1]**

[1] Communication and Distributed Systems, RWTH Aachen University, 52074 Aachen, Germany; matzutt@comsys.rwth-aachen.de (R.M.); hiller@comsys.rwth-aachen.de (J.H.); wehrle@comsys.rwth-aachen.de (K.W.)

[2] School of Computer Science and Engineering, University of New South Wales, Sydney 2052, Australia; salil.kanhere@unsw.edu.au

* Correspondence: pennekamp@comsys.rwth-aachen.de; Tel.: +49-241-80-21411

**Abstract:** The Internet of Things provides manufacturing with rich data for increased automation. Beyond company-internal data exploitation, the sharing of product and manufacturing process data along and across supply chains enables more efficient production flows and product lifecycle management. Even more, data-based automation facilitates short-lived ad hoc collaborations, realizing highly dynamic business relationships for sustainable exploitation of production resources and capacities. However, the sharing and use of business data across manufacturers and with end customers add requirements on data accountability, verifiability, and reliability and needs to consider security and privacy demands. While research has already identified blockchain technology as a key technology to address these challenges, current solutions mainly evolve around logistics or focus on established business relationships instead of automated but highly dynamic collaborations that cannot draw upon long-term trust relationships. We identify three open research areas on the road to such a truly accountable and dependable manufacturing enabled by blockchain technology: blockchain-inherent challenges, scenario-driven challenges, and socio-economic challenges. Especially tackling the scenario-driven challenges, we discuss requirements and options for realizing a blockchain-based trustworthy information store and outline its use for automation to achieve a reliable sharing of product information, efficient and dependable collaboration, and dynamic distributed markets without requiring established long-term trust.

**Keywords:** blockchain; supply chain management; Industry 4.0; manufacturing; secure industrial collaboration; scalability; industrial Internet of Things; Internet of Production



**Citation:** Pennekamp, J.; Matzutt, R.; Kanhere, S.S.; Hiller, J.; Wehrle, K. The Road to Accountable and Dependable Manufacturing. *Automation* **2021**, *2*, 202–219. https://doi.org/10.3390/automation2030013

Communicated by: Duc Truong Pham

Received: 24 August 2021
Accepted: 8 September 2021
Published: 13 September 2021



## 1. Introduction

Manufacturing is expected to significantly benefit from recent advances regarding the Internet of Things (IoT) and Cyber-Physical Systems (CPS). Particular development directions include establishing highly dynamic business relations and creating interconnected and automated production environments, even for short-lived collaborations, through increasing degrees of automation based on (sensor) data [1,2]. Beyond promising better product quality and associated costs—usually, two conflicting goals—such advanced and automated production environments also embrace improved "soft" factor properties that have an increased influence on decision-making, especially environmental (sustainability), social, and governance criteria [3]. The need to improve in these regards is increasing particularly for stakeholders from industrial domains [4,5]. Hence, several complementary research directions dedicated to new concepts such as the Industrial IoT (IIoT) or the Internet of Production (IoP) [6] aim to incorporate corresponding advances into industrial processes, especially manufacturing. The IIoT is a subdomain of the IoT, which is especially concerned with machine-to-machine communication in industrial domains with the explicit goal of enabling further automation potentials for industrial processes [7]. In contrast to the consumer IoT, IIoT solutions are more machine-oriented than centered around human

interaction, and they can rely on structured infrastructures planned ahead of time. Still, at the same time, they have to handle much higher data volumes while simultaneously providing stricter guarantees, e.g., regarding tight real-time and security requirements [7]. Extending upon the IIoT's advancements and the concept of Industry 4.0, the IoP envisions a tighter integration of industrial machines and processes across company borders [6], e.g., to further automate information flows and data sharing between collaborators along a supply chain [8].

The goal of this work is to structure the upcoming challenges and required research efforts to help seize these automation potentials. To this end, we develop a framework that accounts for three layers of research challenges for the additional and increasingly inter-organizational dataflows as envisioned by the IoP. Furthermore, we identify four pillars of required research to specifically tackle different aspects of data-related and other process-oriented challenges to facilitate increasingly open collaborations despite new scenario-driven challenges. With this framework, we intend to provide a structured overview of related research challenges that currently remain open or under-addressed to spark further targeted research efforts and to aid practitioners in their decision-making.

Current research mainly revolves around three pillars (P0–P2), which consider either local improvements or rely on long-term trust relations between stakeholders:

**(P0)** CPS and site-related improvements (↻) with limited external influences,
**(P1)** Extended data sharing along the supply chain (⇄), e.g., to reduce the bullwhip effect [9], and
**(P2)** Secure industrial collaborations across supply chains (↑↓), e.g., to reduce ramp-up costs [10]. To cover **P1** and **P2** not only with today's (established) long-term trust but also in settings with dynamically evolving and flexible short-term relationships, we identify a new research pillar
**(P3)** That has to provide accountable and dependable dataflows even for stakeholders who have not yet established any (trusted) relationships (❖).

In this article, to capture the benefits of (global) data sharing, we focus on the research pillars P1–P3 that consider multiple stakeholders in automated collaborative processes.

Such industry-driven multi-stakeholder settings mandate special needs that traditional solutions in the (I)IoT cannot satisfy. These aspects encompass improved accountability and verifiability to deal with uncertainty concerning the origin [11] and reliability [12] of data, but also security and privacy requirements have to be considered as information leakage can have tremendous consequences in highly competitive environments [8]. We envision that the consequent integration of blockchain technology provides these desired features by design. Its tamperproofness offers verifiability and reliability once information has been recorded on the blockchain. Similarly, blockchains are decentralized and thus well-suited for securing interactions among mutually distrustful parties. Finally, their extensibility enables scalability features, such as sidechains or sharding [13], as needed for solutions across different use cases and domains.

Existing work already suggests leveraging the benefits of blockchain technology to advance established processes. However, these efforts mainly focus on logistics or supply chain-specific improvements [14–22], i.e., they are usually considering a single, well-established pillar of research (P1 ⇄). Similar to the focus of our work, first efforts to combine blockchain technology with manufacturing [23–25] or IIoT [26] have been made. However, to the best of our knowledge, even research does not yet address the unique challenges and opportunities of the more sophisticated pillars that look beyond (established) supply chains, i.e., that consider dataflows across supply chains (P2 ↑↓), potentially in untrusted constellations (P3 ❖).

Given that corresponding research at the intersection of IIoT and blockchain is still in its infancy, our framework centers around challenges that currently prevent industrial stakeholders from seizing the promising potentials of combining both paradigms to turn the vision of an interconnected, automated production landscape into reality. Altogether, we identify three emerging key research areas and further discuss them in this paper:

First, we discuss *blockchain-specific research questions* for the industrial setting, which mainly revolve around the general scalability of proposed solutions and the privacy of participants. Similarly, we identify a lack of manufacturing-specific solutions that integrate blockchains to improve accountability in this domain. Second, we thus detail *scenario-driven research directions* that close this gap and realize fast, versatile, sustainable, automated, accountable, and dependable manufacturing enabled by blockchains. Finally, we elaborate on arising *socio-economic challenges*. Particularly, new legal frameworks will need to take the increased usage of external data, especially in automated, safety-critical applications, into account. However, we primarily discuss how to establish trust in the authenticity and correctness of data on the blockchain with the goal of facilitating further process automation. This way, a solid foundation for future inter-organizational data sharing within the IIoT/IoP can be established that eventually enables stakeholders to leverage the data reliability promised by blockchain technology in a sustainable production landscape.

**Contributions.** Our main contributions in this article are as follows.

- We raise the awareness for a new research pillar (P3 ❖) evolving around dataflows between stakeholders without any trusted or previous relationship.
- We identify three main groups of scenario-driven research challenges in the context of accountable and dependable manufacturing that are accompanied by related blockchain-inherent and socio-economic challenges.
- Using blockchain technology, we propose the idea of a trustworthy information store (*TrustedStore*) to realize a reliable and automated production landscape.

**Organization.** The remainder of this article is structured as follows. In Section 2, we outline the foundations of our work, including today's methods and approaches in research, to define the scope of our article. Subsequently, in Section 3, we give a brief overview of blockchain technology to highlight its potential for applications in quite diverse use cases. Then, we present the results of our work in Section 4: We develop a framework for classifying research challenges that considers three layers (blockchain-inherent, scenario-driven, and socio-economic challenges), including different pillars for realizing increasingly open and inter-organizational data exchanges and automated processes based on scenario-driven research challenges along with our proposed concept of a *TrustedStore*. We draw our scenario-driven research challenges from our work with researchers and practitioners concerned with industrial processes, who are especially familiar with realizing the vision of the IoP. Finally, we conclude this article in Section 5.

## 2. Motivation and Potentials

Manufacturing is expected to compile vast amounts of process and product data in the near future [8,27]. Consequently, to enable automation and autonomous decision-making, we have to deal with associated big-data challenges [28,29] that are imminent due to virtually infinite volumes of available sensor data and the increased need for high-frequency sensing [1,2]. In that regard, efficiently utilizing existing computing and network infrastructure could be a key driver [30,31]. However, big data also provides opportunities when properly extracting its encapsulated knowledge [1]. Recently, related work increasingly focuses on the implications of the digitization on different industry sectors [32], and more specifically also in light of a shift towards environmental sustainability [33]. Another crucial aspect is to consider the security and safety consequences of said developments [34–36]. In the area of manufacturing, the potential of big data has previously been neglected due to a lack of globally available process information and exchange of knowledge. Even the comparably selective data sharing along existing supply chains was severely limited due to privacy concerns. In Figure 1, we illustrate the data sharing along (⇄) and across (↑↓) supply chains, which we detail hereafter based on the example of two fine blanking lines.

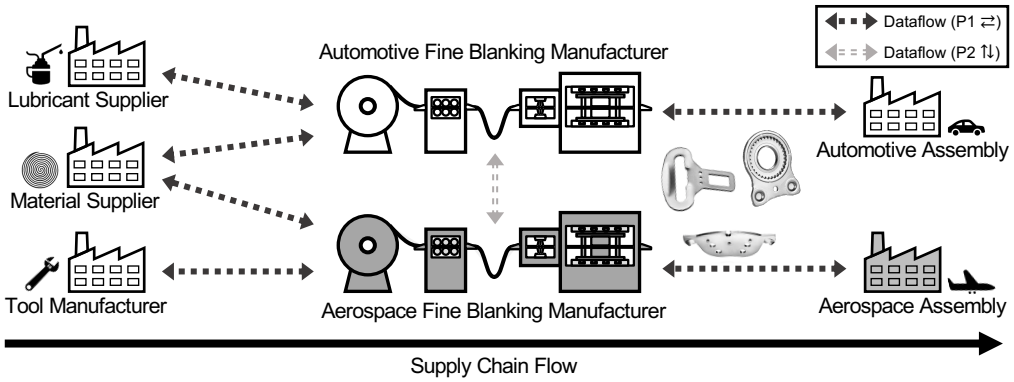


**Figure 1.** Manufacturing engulfs dataflows along the supply chain (P1 ⇄) and across supply chains (P2 ↑↓). Suppliers (here: for lubricants, material, and tools) support manufacturers, who provide subsequent assembly lines with production data. Similarly, manufacturers exchange process information (here: fine blanking lines), the processed material, and their interplay. A currently lacking relationship between both assembling companies could stem from the untrusted environment (P3 ❖). We adapted the figure from our previous dataflow analysis in industry [8].

### *2.1. Information Sharing along Supply Chains (P1 ⇄)*

Traditionally, sharing supply chain data is driven by large companies dictating their requirements. Information is collected in data sinks accessible only by single (large) players [12], e.g., automotive manufacturers. The data are usually shielded from external stakeholders due to privacy concerns. For instance, even rather insensitive data, such as delivery schedules or shipment tracking, is only retained locally. Extra data are only shared based on immediate financial benefits, even though sharing production data is expected to improve productivity and overall product quality [8].

This unsatisfactory situation fails to address several desired aspects. The current state cannot reliably provide (long-term) verifiability of relevant information [37] for legal purposes, e.g., provenance data for aerospace parts or associated maintenance protocols. Counterfeit or non-fair trade products can still enter legitimate supply chains occasionally despite corresponding quality assurance [38]. To improve the reliability of (obtained) data, new solutions must minimize manipulability and provide verifiable certifications for individual products efficiently. A holistic solution could further aid governmental oversight, especially regarding safety-critical products or food chains [39].

Another issue stems from the lacking identifiability of root causes of manufacturing or product failures [37]. Currently, accountability is mostly limited to contractually bound stakeholders. If not explicitly negotiated, single untrusted suppliers may be uncooperative for their own benefits, e.g., when covering up incidents. Simultaneously, missing feedback to estimate a product's lifetime or fit, which both might be application-dependent, hinders the implementation of improvements. Here, especially an increase in targeted, data-driven automation that reacts towards slight variations in received products, parts, or goods is likely. Naturally, suppliers must reliably provide the respective information for decision-making. Overall, more broadly accessible production and usage data can provide insights to overcome such limits [8].

### *2.2. Foundations for Expanding Secure Industrial Collaborations across Supply Chains (P2 ↑↓)*

In addition to the data sharing along supply chains (P1 ⇄), data exchanges across supply chains (P2 ↑↓) are basically non-existing in today's manufacturing landscape [1]. While manufacturers gather usage data from their customers (in centralized data silos), virtually no knowledge exchange happens between different operators of (identical) machines [8]. For example, experiences with in-use machine configurations or information about the (expectable) production quality can reveal valuable insights into newly configured manufacturing processes. Despite potentially tremendous benefits [8], all knowledge is retained locally without global availability instead.

By sharing, for instance, ideal machine configurations for their workpieces, companies could improve their productivity and reduce costs without having to reveal all details to the machine supplier. This exchange may reduce ramp-up times of new manufacturing processes by deriving machine parameters from already available information (cf. Figure 1). Non-competing companies then can cooperate and jointly assemble a shared knowledge base in a give-and-take manner or offer their valuable data for sale. Eventually, by deploying and sourcing federated machine learning, participating companies can potentially also adjust their processes using automated approaches. As of today, a lot of expected potential in this area is still unexplored.

### *2.3. Ad Hoc Relationships in Untrusted Environments (P3 ❖)*

When considering relationships with previously unaffiliated and thus untrusted companies (P3 ❖), several additional use cases emerge. Extending the utilization of relationships among previously unaffiliated parties can help to identify the ideal supplier for a component along the supply chain (P1 ⇄). Further exchanging information with other companies in related domains across supply chains (P2 ↑↓) is currently hindered by a lack of trust between stakeholders in a similar manner. We expect more use cases, also in light of additional automation, to surface after the first steps since businesses are cautious when sharing sensitive and valuable details, especially production and product data [8,40]. Finally, we observe a lack of standardization for exchanging data, which critically hinders forming flexible relationships because of required company-specific adjustments for each new partner [12,41].

In the context of automated accountable and dependable manufacturing, we also have to address privacy and safety concerns [36,42]. Appropriate means are not yet available, or they are neither proven nor tested in manufacturing [1]. A major milestone to establish trust can be achieved by providing accountability, verifiability, and transparency for all actions and traded information. Blockchains are promising tools to establish trust in markets for mutually distrusting competitors and to eventually allow for inter-organizational data sharing and novel applications.

## 3. The Influence of Blockchains

Blockchains have matured considerably since Bitcoin [43] incepted the concept in 2008. While blockchains were initially created for the decentralized, yet secure, operation of digital currencies [44], both academia and industries quickly identified its potential for managing larger and more diverse tasks [45].

### *3.1. The State of Industrial Blockchain Integration*

We now reiterate impactful milestones and applications of distributed ledgers [46], i.e., blockchains, to assess their current level of integration into business processes and to identify areas where blockchains have already been applied successfully [47].

#### 3.1.1. Financial Origins

Bitcoin paved the way for global financial transactions without banks as intermediaries [48]. In addition to inspiring numerous comparable cryptocurrencies, the banking sector also noticed the potential of blockchains to improve transactions between financial institutes. This development yielded major blockchain-based inter-bank networks, e.g., the Ripple payment [49,50] and exchange network or Liink by J.P. Morgan (formerly known as the Interbank Information Network) [51]. Blockchains promise to provide a better, more direct customer experience at lower costs due to more automated, disintermediated processes. Especially in scenarios where participants are known, and the majority is trusted, consortium blockchains [52] are seen as key enablers for shaping new transaction processes in highly distributed applications, e.g., accounting along supply chains.

#### 3.1.2. Digital Assets

One of the first non-cryptocurrency applications of blockchains was the establishment of digital assets and notary services. While dedicated solutions, such as Namecoin [53], were launched early, numerous related services rely on existing blockchains, commonly Bitcoin [54]. Users can, for example, tie assets such as property, coupons, or stock-marketing shares to their transactions to transfer digital ownership of those assets via the blockchain. Beyond that, notary services immutably attest to the existence of a document at a given time by storing its cryptographic hash as a tamperproof document identifier on the blockchain [55].

#### 3.1.3. Process Automation

*Smart contracts* realize the automated execution of transactions once the blockchain's state satisfies their one-time programmable conditions [42]. This tamperproof programmability allows for the transparent automation of global processes. While Ethereum [56] popularized blockchain-based smart contracts, business applications are commonly built using consortium blockchains, e.g., created through *Hyperledger Fabric* [57] or the Ethereum-compatible *Quorum* [58]. Beyond the banking sector, insurers process insurance claims without human interaction through smart contracts. An increased demand for blockchain-based process automation sparked the creation of Blockchain-as-a-Service solutions, e.g., offered by Microsoft, IBM, or AWS. These services lower the barrier for creating blockchain-backed architectures but also introduce an infrastructure provider as a new *centralized* entity.

#### 3.1.4. Internet of Things

Advances in process automation proliferated the vision of coupling autonomous IoT devices with blockchains. The main advantages of blockchain-based IoT infrastructures lie in the immutable and decentralized IoT-based sensing of physical environments in conjunction with the accountable recording of actuation events. If seized well, these capabilities can significantly simplify applications for smart cities, e.g., smart microgrids [59] or vehicular networks [60]. Here, blockchains aid the trust management and access control for sensed data alike.

#### 3.1.5. Supply Chains

Blockchains may be used as an architectural pillar for reshaping supply chains [37,38,61,62], especially due to improved financial transactions, asset management, process automation, and data management. However, smooth integration is still lacking [42]. TrustChain [39], ProductChain [11], PrivChain [63], TradeChain [64], and PrivAccIChain [62] already tackle important issues of supply chain deployments, such as reputation-based trust management among suppliers and provenance tracking for customers. Still, holistic approaches to improve supply chains based on distributed ledgers are yet to come [65].

### *3.2. Useful Properties for Diverse Applications*

Already today's limited integration of blockchains into business processes highlights that distributed ledgers have proved to provide *valuable foundations* for various domains, applications, and use cases. Blockchain technology can, in particular, provide long-needed contributions regarding more flexible collaborations and especially applications involving supply chains. First, the *decentralized* nature of blockchain platforms suits the highly distributed and heterogeneous environments created by collaborating companies and supply chains. Second, blockchains can provide data *integrity* and *verifiability* even if collaborators are partially distrusting each other. As part of this process, recorded data are kept on a *tamperproof* ledger. Finally, established measures to keep track of digital assets and to prevent double-spending enable the public, transparent *traceability* of products or their components. However, the decentralization and immutability of blockchains create issues that were not present in traditional business processes. Next, we thus highlight the

resulting challenges that, once tackled, will help realize suitable full-stack solutions for improving business processes via distributed ledgers.

## 4. Open Research Areas

In this section, we develop a framework for classifying currently open or under-addressed areas for further research technical and process-oriented improvements for the automation of IIoT-based and blockchain-backed dataflows as required to realize the IoP's vision of increasingly inter-organizational and dynamic information exchanges. Following the best practice of "security-by-design", we regard security aspects as a necessary and acknowledged foundation to establish automation within the IIoT and IoP alike. Thus, we specifically focus on use case-specific aspects, i.e., challenges for manufacturing and automation, instead. Overall, we identify three layers of open research areas that we illustrate in Figure 2:

**(L1)** Yet unaddressed challenges for the use of blockchain technology in manufacturing,
**(L2)** New opportunities for a fast, versatile, accountable, and dependable manufacturing enabled by blockchains, i.e., scenario-driven challenges, and
**(L3)** Socio-economic challenges stemming from immutably recorded production data and highly flexible cross-company collaborations.

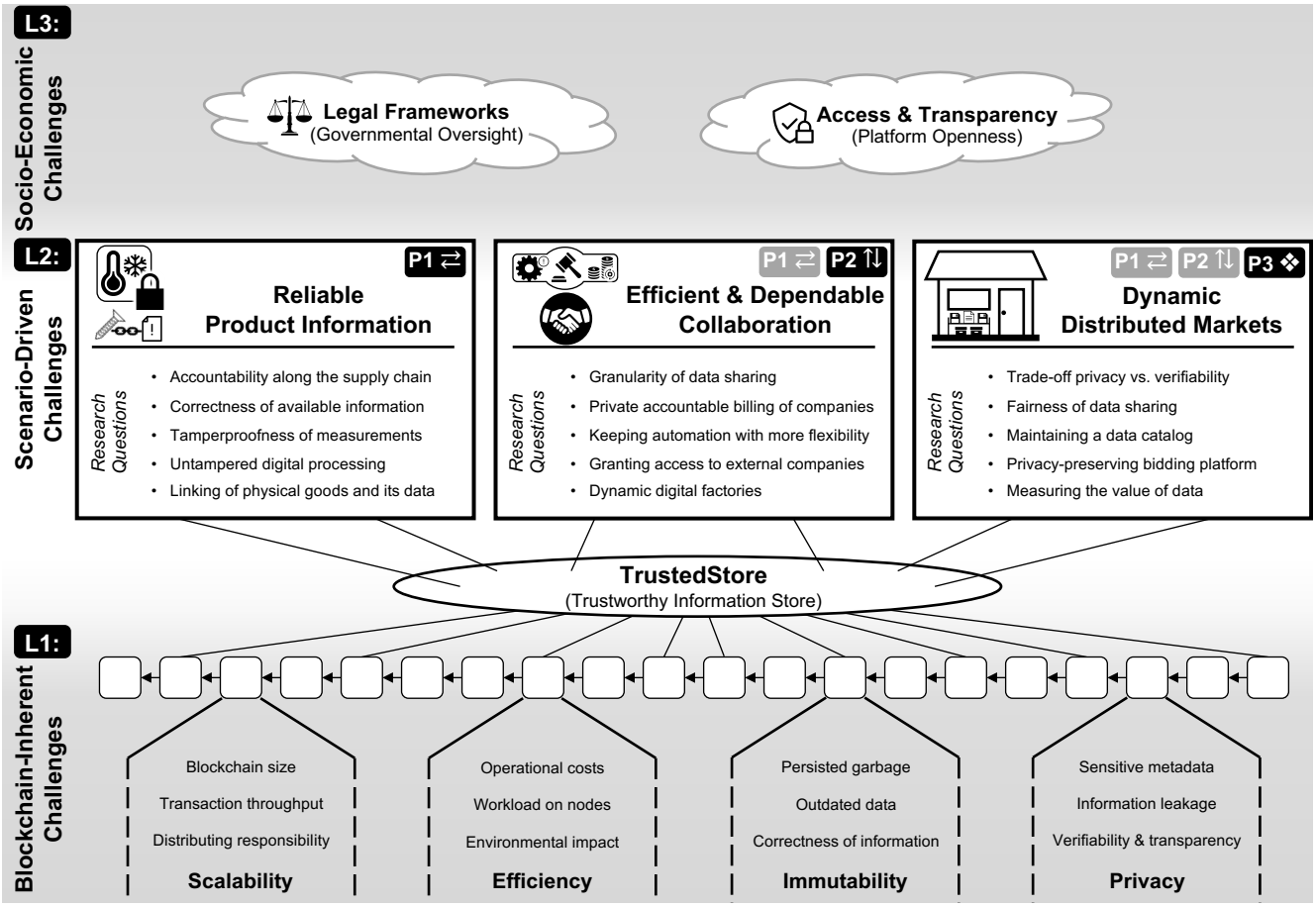


**Figure 2.** We group our research towards accountable and dependable manufacturing into three layers (from bottom to top). **L1**: Blockchain-inherent challenges that concern the properties of blockchain technology, which is expected to serve as an underlying key component of our envisioned TrustedStore. **L2**: Scenario-driven challenges that can be grouped into three main research directions that each focus on a specific research pillar, i.e., *along supply chains* (P1 ⇄), *across supply chains* (P2 ↑↓), and *situations with insufficient trust between stakeholders* (P3 ❖). **L3**: Socio-economic challenges that have an impact on underlying collaborations and improvements. To offer viable solutions for accountable and dependable manufacturing, research must consider and tackle all layers and their individual research challenges.

We consider these layers to be highly relevant when shaping the future of interconnected manufacturing and, thus, we identify research questions to address the challenges on each layer, and we provide pointers to promising approaches to tackle these challenges.

### *4.1. Open Blockchain-Inherent Challenges (L1)*

We first identify general blockchain-centered challenges that emerge from applying the technology to achieve accountable and dependable manufacturing, which in turn allows for further process automation.

#### 4.1.1. Scalability

Permissionless blockchains traditionally struggle with limited scalability in terms of transaction throughput [66], transaction latency [67], and storage requirements [13]. For instance, Bitcoin famously has a low transaction throughput and a large payment delay [66], which has users waiting for up to an hour before they can safely accept payments. Even though consortium blockchains can utilize more efficient consensus algorithms [68], recording large numbers of events on-chain still remains challenging. Further research must thus address the question of how to improve the data throughput of blockchain-backed storage to reduce the impact of the blockchain's limitations on the overall system performance. Solutions may aggregate multiple events into single or few (on-chain) transactions, similar to micropayment channels that boost transaction throughputs in today's cryptocurrencies. Furthermore, *sharding schemes* [69–71] may improve the transaction throughput as these schemes target to partition the network and to distribute the responsibility for transaction processing. In the context of industrial data, researchers should investigate to what extent distributing the responsibility to operate the blockchain as a shared data-exchange medium can be achieved in industrial scenarios, where stakeholders are only beginning to become more open toward other collaborators and also competitors.

Another scalability issue is the ever-increasing storage requirement to operate blockchains [13,72]. This problem is aggravated in the context of supply chains once suppliers are required to tie their process data to the blockchain. Pruning strategies have been proposed to unburden blockchain nodes from storing historic data that has become obsolete [72,73]. However, applications relying on blockchain-extrinsic data cannot immediately seize this potential since what constitutes obsolete data has to be defined on a per-application basis. Again, partitioning data storage across the network with sharding schemes can reduce per-node requirements. Overall, research needs to account for long-term data availability to allow for efficient and scalable solutions. A fundamental question in this regard is how to define, depending on the respective scenarios, what data can be pruned, and when it can be pruned. For instance, some records may become obsolete entirely after a certain time, while other records must be kept indefinitely, either with reduced granularity or as raw data, e.g., manufacturing data of aerospace suppliers [62,74]. In addition to defining prunable data, stakeholders need to be able to mark their data to be pruned correspondingly. At the same time, full accountability must be provided even if data become pruned in the future.

#### 4.1.2. Efficiency

The widespread adoption of blockchain technology in supply chains necessitates an efficient operation of the infrastructure. To this end, any proposed architecture must take deployment and operation costs into account, with a special focus on computing overhead for securely referencing data on-chain. Improvements in efficiency mainly originate from more fundamental lines of research, e.g., advances in authentication [75], distributed consensus [76], or secure communication [77]. However, a proper integration of these advances into a full blockchain-based architecture is mandatory to seize this potential for efficient data management and to not undermine any requirements of the overall system. The redundant execution of various tasks, such as verifying digital signatures or maintaining a local state, has become the main bottleneck of traditional blockchains [72]. Solutions, such as sidechains or sharding, that distribute the workload without lowering security

guarantees will help to reduce the operating costs [66,78]. While these concepts are primarily being researched for public settings, the envisioned high-frequency utilization and large volumes of data call for similar developments for consortium blockchains. Research efforts that tackle efficiency challenges can thus further investigate methods to lower the financial investments and operational costs companies currently face when shifting to blockchain-backed solutions, for instance, by reducing the required workload for individual nodes without forfeiting the blockchain's security guarantees. As we further anticipate a widespread application of blockchain technology in industrial contexts in the nearer future, questions regarding the environmental sustainability of such solutions become more pressing.

#### 4.1.3. Immutability

Recording events immutably despite the presence of adversaries eager to alter history is arguably the blockchain's key achievement. Thus, storing non-financial, application-specific data on-chain or referencing such data through on-chain fingerprints has become a frequent proposition [54]. However, this immutability is also known to create further issues than only impacting the long-term scalability of blockchains. For instance, distributing and storing unwanted blockchain data can cause legal liability [73]. While the prevalence of known identities within consortium blockchains mitigates such risks, different stakeholders may nevertheless be in conflict about the value of recorded data, e.g., whether data are outdated or when unknown raw data formats pollute the shared storage. Overall, the quality of recorded information becomes more important as participants should be able to rely on data that are recorded by other parties that exhibit varying individual levels of trust. Today, a link between a physical (product) property and its digital data is missing, limiting the consensus algorithms' ability to verify claimed events before persisting them on-chain, e.g., sensor readings from inaccessible, remote environments [47,79]. Correcting identified errors is possible by overwriting data in a new transaction, but this approach requires more complex processing for all involved parties to obtain an up-to-date state. Hence, further research is required to explore the trade-off between data availability and data utility, as well as data verifiability and efficient corrections.

#### 4.1.4. Privacy

Tightly related to the individual value data has for different stakeholders involved in the consortium blockchain is the notion of data privacy, which applies not only to traditional privacy, e.g., storing and trading customer data, but to information leakage in general [73]. On the one hand, blockchains may disclose business secrets [61], such as machines' capabilities or process details, e.g., required temperatures or metal alloys, both directly and indirectly. On the other hand, meta-information such as the frequency of transactions between two collaborators or key performance indicators may be inferred, putting affected stakeholders at a disadvantage against competitors, e.g., during price negotiations or when company acquisition is imminent. A key challenge for consortium blockchains will be gauging the desired level of point-to-point collaborations and consequently tackling trust barriers through both trust and data management. To reflect these requirements on the blockchain-level, further research should not only investigate how to allow for fine-granular access control and, where needed, access tracking, but also how blockchain developers can ease the process of defining the required policies to mitigate the risks of misconfiguration.

### *4.2. Scenario-Driven Research Directions (L2)*

On top of the blockchain-inherent challenges, further research directions may lead to a fast, versatile, sustainable, automated, accountable, and dependable blockchain-backed manufacturing (cf. Figure 2). Research into (i) *reliable product information* will ensure the availability of high-quality data (to adapt the automation) alongside all production steps of a supply chain (P1 ⇄), ranging from tamperproof sensing to secure blockchain

storage. Based on this reliable, high-quality information, more (ii) *efficient and dependable collaborations* that will increasingly affect dataflows across supply chains (P2 ↑↓) can form in the future. Ultimately, (iii) *dynamic distributed markets* allow for an increasingly flexible sharing of data and advertising of services, especially when stakeholders without any trusted or previous relationships intend to collaborate (P3 ❖). This way, collaborators can efficiently foster fast, versatile, and dependable business relations to (sustainably) improve even established automated processes.

#### 4.2.1. Reliable Product Information

Today, large-scale production and supply chains (P1 ⇄) are opaque regarding processes and the origin of processed goods [12]. Hence, root causes of failures and other issues cannot be tracked down efficiently, creating massive administrative overheads [37,62,80], e.g., hampering legal investigations, causing over-dimensioned product recalls, or an inefficient lookup of compatible spare parts for repairs or assembling bigger workpieces. Similarly, feeding back information from mid-term or long-term field experience into processes for improvements is hard [8]. To overcome these limitations, manufacturing needs a *reliably accessible*, *tamperproof* information store that links *identifiable* products to their physical state in a *verifiable* manner. In the following, we develop the requirements for such an information store from the object-level monitoring to long-term data storage using a blockchain.

First, this process requires measures to *achieve a tamperproof gathering of physical-state information*. On the one hand, companies need access to such relevant information, i.e., a method to accurately derive digital representations. While several concepts, such as digital twins [81–83] and digital shadows [84,85], emerged, our work is orthogonal to the exact extraction or modeling of these data. We refer to existing work [86,87] for an overview on how to accurately create and express digital representations of physical objects, and assume their availability for our work. On the other hand, processes may require extensive monitoring to ensure a required or desired product quality. For example, fresh produce, which mandates a strict cold chain, requires the container's temperature to be continually monitored, and tricking the sensors in case the cold chain is violated must be infeasible [39]. Here, we identify tailored anomaly detection via machine learning as a promising research area. Machine learning can be based on the following data in our context: (i) Using multiple sensors allows for cross-checking gathered data. For instance, sensors redundantly monitoring the container from different vantage points can increase tamper resilience as already subtle monitoring inconsistencies could unveil manipulations. (ii) Similarly, different sensor types and measuring methods further increase the range for sensing correlation to detect anomalies regarding the coherence of real-world physical effects. As sensor nodes cheapen and allow for long-lasting battery-based operation, these solutions are also becoming increasingly economically viable. (iii) Further, high sampling rates also improve tamper resilience, as more readings are available to identify inconsistencies. Overall, the gathered data provide a promising input for a machine learning-based anomaly detection. In addition to investigating the promising area of digital representations in more detail, researching additional fine-grained and low-cost solutions to monitoring processes (across company borders) will further improve the achievable degree of automation based on reliable product information.

Still, storing these large amounts of raw data (i–iii) in globally replicated tamperproof storages, such as the blockchain, remains challenging. Instead, we envision a combination of *mid-term local storages* maintained by companies and a *long-term distributed information store*. In this deployment model, companies store their raw production data locally and signal its availability on-chain via fingerprints. Further, the blockchain stores (small-sized) insights that result from analyses of the locally stored raw data. This storage needs to happen in a certified manner, overall creating a *trustworthy information store*, which we refer to as *TrustedStore*. To ensure that companies preserve raw data locally, certified service providers (verifiers) periodically check if local stores match with the TrustedStore, so that

misbehavior can be detected in a timely manner and appropriately acted upon (legally). As the amount of data renders full-blown checks impracticable from remote locations and on-site checks involve high costs, they have to happen only rarely. In between, verifiers remotely request data for randomly selected fingerprints to frequently, yet economically, check for data availability. Today, methods to digitally attest these checks already exist [74]. Alternatively, companies store raw data in globally distributed certified data stores and prove such storage to the TrustedStore. Overall, research efforts should investigate how to properly decouple the storage of *large amounts of raw data* from *derived insights and key properties* to ensure the immutability and availability of rich raw data while keeping reasonable loads for globally maintained infrastructures. Furthermore, future research must ensure the interoperability of this process, such that different entities, e.g., manufacturers, collaborators, verifiers, and optionally customers, can get easy access to all data required for their respective tasks.

Second, researchers must develop means for the *tamperproof digital processing of gathered data* to ensure that original sensor readings enter the blockchain-backed TrustedStore correctly. This way, data can be collected even from untrusted or hostile environments, e.g., to realize new collaborations without sufficient trust levels. One highly promising research area in this regard is *tamperproof sensors*, which can provide this form of dependable data gathering and processing [79]. Such devices combine traditional sensors, e.g., RFID scanners, or temperature or humidity sensors [88,89], with trusted computing mechanisms, such as hardware security modules (HSMs). These security-enhanced sensors are able to immediately hand over data to HSMs for processing, thereby minimizing the attack surface for tampering. Ultimately, the HSM uploads the sensor readings to the local storage and stores their fingerprints on the TrustedStore. From this point on, the reliably-sensed data are persisted immutably.

Assuming that mechanisms for tamperproof sensing and blockchain inclusion are in place, the sensor readings must be reliably linked to the respective physical products, e.g., via camera tracking, RFID tags, imprints, or other markings such as special chemical signatures [90]. Importantly, this identification must also be tamperproof, using mechanisms from before.

In summary, this envisioned line of further research will yield a reliably accessible, tamperproof TrustedStore for production data to establish *accountability along any supply chain*. Beyond aiding legal investigation, managing recalls, optimizing parts utilization, and automation, this TrustedStore can further serve as a medium to foster collaborations among well-known and novel companies alike.

#### 4.2.2. Efficient and Dependable Collaboration

After having outlined challenges for realizing a dependable TrustedStore in Section 4.2.1, we now focus on opportunities for inter-organizational data sharing and process automation based on this TrustedStore architecture to be further investigated by future research. Especially in this collaborative environment, i.e., when considering dataflows across supply chains (P2 ↑↓), relying on a TrustedStore could improve the productivity in manufacturing quality [8], even when applying sophisticated, large-scale automation. Sharing workpiece data, production machine schedules, and states in a timely manner enables close collaborations and allows accumulating companies into automated *digital factories* with production efficiencies similar to single, multi-factory companies. Rich information flows allow for a cross-company allocation of machine time and flexible handling of process deviations [8], e.g., by automatically reallocating machine capacity in case of delays [91]. Here, the TrustedStore enables trustworthy tracking methods for workpieces along the full (multi-factory) supply chain. As a result, problems can easily be tracked, and clearly assigned responsibilities motivate participants to comply with their obligations. Most basically, this information allows for detecting infringements, such as misconfiguration, early on.

Beyond supply chain management, TrustedStores simplify the billing of goods or machine usage (Manufacturing-as-a-Service) [8]. Especially with environments shifting from generic mass production to individual products, companies require verifiable and highly automated payment processes to maintain reasonable administrative burdens. Even pay-as-you-go contracts for cost-efficient machine usage in adaptive production are conceivable where customers pay only for the resources required to create the requested (potentially low-quantity) workpieces. Thereby, high degrees of automation enable manufacturers to maintain a high utilization as multiple customers can share machines with almost no downtime.

Managing data from mid-term and long-term field experience on the TrustedStore promises further benefits. In contrast to less sensitive product data, process data are more valuable and, thus, must be protected accordingly. Nowadays, information on product life cycles, required maintenance intervals, or production quality variations is exclusively accessible to the manufacturer. Using the TrustedStore, such data become accessible to current and prospective machine users alike (cf. Figure 1). Here, the TrustedStore provides evidence of data correctness. Data of individual machines further facilitate reselling as prior usage and output quality become assessable.

Research has to address the required granularity of sharing data to achieve the envisioned benefits. As business secrets are potentially at risk when providing information to external (untrusted) collaborators [8,92], companies have to make informed decisions when trading off efficiency and profit for privacy.

#### 4.2.3. Dynamic Distributed Markets

Ultimately, we envision (distributed and transparent) blockchain-based bidding platforms that realize versatile, yet dependable markets for *goods*, *services* (e.g., machine rentals), and *configuration knowledge*, especially fostering collaborations between—previously unknown and potentially untrusted—business partners (P3 ❖). Today's business relations typically evolve over long time periods and trust builds up slowly or is enforced through complex contracts. Blockchains can largely substitute social trust through technical guarantees and thus foster the establishment of new business relations. Distributed TrustedStores allow for efficient automation, e.g., the allocation of machine time, and achieve high utilization even in adaptive manufacturing processes. Manufacturers can then generate profit even from short-time business relations for single workpieces, which would otherwise be uneconomical and incur high risks.

Customers can search for the best-matching offer and benefit from reasonable prices due to increased market competition. Especially smaller manufacturers can profit from a low-barrier market access to appeal to customers and business partners and easily increase (domain) knowledge through the TrustedStore.

However, realizing these distributed markets faces a big challenge, i.e., the potential disclosure of business secrets. For example, big companies could exploit the TrustedStore's information to suppress competitors, e.g., by engaging in well-informed price dumping. Thus, a fundamental question is how to match partners based on desired capabilities and quality-guarantees without requiring manufacturers to reveal sensitive details upfront. Promising building blocks for such a *privacy-preserving catalog* are known from privacy-preserving computing. However, they require extensive research to fit the desired scenario of (semi-)automated privacy-preserving bidding platforms.

Such mechanisms must realize *fair data sharing*, i.e., participants must not obtain details about other participants, especially competitors, without providing said information themselves. To this end, mechanisms to *assess the value of data* can provide measures to rate-limit or charge participants. While initial approaches to implement trustworthy data-sharing platforms have already emerged [93,94], research is still in its infancy in this area. Hence, solutions to the aforementioned challenges regarding the potential leakage of business secrets must be addressed to bring the otherwise promising concept of distributed data-sharing markets to (full) fruition.

### *4.3. Socio-Economic Challenges (L3)*

Beyond the outlined technical measures to realize accountable and dependable manufacturing, we also briefly discuss overarching and predominantly interdisciplinary socio-economic challenges (cf. Figure 2).

#### 4.3.1. Legal Frameworks

Legislation currently fails to cover blockchain-based smart contracts and analyses have to show whether general rules suffice to enable the envisioned business relations. Especially when considering global supply chains, also different legal frameworks and multi-national agreements must be taken into account. To realize the desired accountability, legal frameworks must further clarify the responsibility for the accuracy of information in a TrustedStore. An exemplary question is whether manufacturers should be responsible only for the data they provide or whether they should also be responsible for consistency checks on the received data.

In terms of privacy, all systems must comply with local as well as multi-national rules for data privacy, such as the GDPR, including the right to erasure of recorded data. Thus, an extensive analysis has to show which data are safe to be stored on-chain, and systems must prevent the inclusion of data that falls under the right to be forgotten or provide mechanisms for data removal without undermining the desired goals.

Furthermore, several third-party services that use the available data are conceivable, e.g., utilizing individual usage data to offer improved maintenance for all customers. To this end, legal frameworks have to clarify who owns the data on the blockchain and who is allowed to process which data in which way. Similar questions also arise for any derived knowledge.

#### 4.3.2. Access and Transparency

Before realizing immutable TrustedStores, research must work out the access requirements for different entities and the trade-off between verifiability and privacy. On the one hand, broad access to information increases transparency such that customers can obtain information more easily. Research must reveal which information is necessary, e.g., to alleviate the required trust from today's slowly forming business relations via technical measures to ease collaboration without pre-established trust. Legal entities may further demand access, e.g., to discover cartels.

On the other hand, information stored on a (semi-)public blockchain must not subvert privacy legislation. Specifically, granting broad access to information may put privacy at risk. Furthermore, reasonable freedom of action for market participants must be maintained. For example, adequate measures must prevent customers from exploiting the knowledge of a participant's low machine utilization to achieve an uneconomic price. Socio-economic research must develop guidelines for blockchain-based platforms that do not only optimize cost but lead to a healthy ecosystem with incentives for high quality, economically healthy companies, and employee well-being.

## 5. Conclusions

We envision future manufacturing to be driven by exciting advances that are based on a combination of (I)IoT and blockchain technology and realize a dependable and accountable ecosystem. Most notably, this ecosystem can boost the flexibility, efficiency, and sustainability of future manufacturing processes by allowing stakeholders to share the information required to establish new collaborations without prior trust in an automated manner. In this article, we identified corresponding future use cases for both supply chain-related and unrelated aspects that should significantly improve the utilization of manufacturing data (cf. Figure 1).However, research must first address open challenges from three different layers, ranging from blockchain-intrinsic questions to measures for ensuring the reliability of exchanged data, and ultimately engulf overarching socio-economic challenges (cf. Figure 2).Regardless, we believe that most effort must be invested in

scenario-driven tasks to enable trustworthy information stores, i.e., *TrustedStores*, in competitive, business-driven, and potentially distrustful industry environments. Fortunately, smaller advances are already achievable in increments, such that first changes should be realizable in the near future.

Considering the limitations of our work, we must note that, despite the shown potential, the actual realization of the envisioned dependable and accountable ecosystem for manufacturing depends on hardly foreseeable market influences. On the one hand, companies are reserved when it comes to such visionary work, i.e., these visions rarely stem from real-world deployments and practitioners. On the other hand, other actors, especially startups, are very enthusiastic, e.g., when publishing white papers or proof of concepts to demonstrate novel ideas and technologies. Thus, our analysis may only cover a subset of proposed approaches and ongoing efforts in the industry. Especially, we may overestimate the outlined potential given that we do not investigate if too many decision-makers cultivate a possibly irrevocable attitude against data sharing. However, we focused on the technical challenges and possible achievements when a readiness for secure data sharing exists. Therefore, we are confident that the reported findings are well-founded and meaningful for researchers and practitioners and may even help to remove objections in principle.

Nevertheless, due to this primary focus on the scenario-driven challenges (L2), an area where we felt that a current analysis is missing, we only briefly reported on the socio-economic challenges (L3). We leave a more in-depth exploration of this layer for future work and especially encourage scholars with a detailed background in this field to analyze the corresponding research directions and challenges, also in light of the interplay between safety risks and increased automation. Finally, we emphasize that our work should be considered as a starting point for work that particularly focuses on specific aspects in detail. Our main intention is to stimulate research at this novel intersection of IIoT and blockchain technology. In particular, efforts from both researchers and practitioners are needed to turn the vision of an interconnected, sustainable production into reality. Eventually, even if decision-makers favor data sharing, market dynamics will finally decide whether these new advances will prove successful in real-world deployments. For now, monetary aspects are still the primary reason for decisions. However, with the increasing importance of environmental footprints and sustainability, we believe that additional "soft" factors (cf. Section 1) will implicitly influence the industry decision-making, thereby considering the research directions that we outlined in our work. Overall, given our findings and their potential impact, we hope that our study encourages and helps researchers and practitioners to identify and work on the future steps that transform the production landscape accordingly.

**Author Contributions:** Conceptualization, J.P., R.M., J.H.; visualization, J.P.; writing—original draft preparation, J.P., R.M., J.H.; writing—review and editing, J.P., R.M., J.H., S.S.K., K.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy–EXC-2023 Internet of Production–390621612.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The funders had no role in the conceptualization of the manuscript; in the writing of the manuscript, or in the decision to publish the results.

## References

1. Kusiak, A. Smart manufacturing must embrace big data. *Nature* **2017**, *544*, 23–25. [CrossRef] [PubMed]
2. Coito, T.; Firme, B.; Martins, M.S.E.; Vieira, S.M.; Figueiredo, J.; Sousa, J. Intelligent Sensors for Real-Time Decision-Making. *Automation* **2021**, *2*, 62–82. [CrossRef]

3. Friede, G.; Busch, T.; Bassen, A. ESG and financial performance: Aggregated evidence from more than 2000 empirical studies. *J. Sustain. Financ. Invest.* **2015**, *5*, 210–233. [CrossRef]
4. Rosen, M.A.; Kishawy, H.A. Sustainable Manufacturing and Design: Concepts, Practices and Needs. *Sustainability* **2012**, *4*, 154–174. [CrossRef]
5. Seuring, S.; Müller, M. From a literature review to a conceptual framework for sustainable supply chain management. *J. Clean. Prod.* **2008**, *16*, 1699–1710. [CrossRef]
6. Pennekamp, J.; Glebke, R.; Henze, M.; Meisen, T.; Quix, C.; Hai, R.; Gleim, L.; Niemietz, P.; Rudack, M.; Knape, S.; et al. Towards an Infrastructure Enabling the Internet of Production. In Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS '19), Taipei, Taiwan, 6–9 May 2019; pp. 31–37. [CrossRef]
7. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
8. Pennekamp, J.; Henze, M.; Schmidt, S.; Niemietz, P.; Fey, M.; Trauth, D.; Bergs, T.; Brecher, C.; Wehrle, K. Dataflow Challenges in an *Internet* of Production: A Security & Privacy Perspective. In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC'19), London, UK, 11 November 2019; ACM: New York, NY, USA, pp. 27–38. [CrossRef]
9. Moyaux, T.; Chaib-draa, B.; D'Amours, S. Information Sharing as a Coordination Mechanism for Reducing the Bullwhip Effect in a Supply Chain. *IEEE Trans. Syst. Man, Cybern. Part C (Appl. Rev.)* **2007**, *37*, 396–409. [CrossRef]
10. Pennekamp, J.; Buchholz, E.; Lockner, Y.; Dahlmanns, M.; Xi, T.; Fey, M.; Brecher, C.; Hopmann, C.; Wehrle, K. Privacy-Preserving Production Process Parameter Exchange. In Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC '20), Virtual Conference, 7–11 December 2020; ACM: New York, NY, USA; pp. 510–525. [CrossRef]
11. Malik, S.; Kanhere, S.S.; Jurdak, R. ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA '18), Cambridge, MA, USA, 1–3 November 2018. [CrossRef]
12. Gleim, L.; Pennekamp, J.; Liebenberg, M.; Buchsbaum, M.; Niemietz, P.; Knape, S.; Epple, A.; Storms, S.; Trauth, D.; Bergs, T.; et al. FactDAG: Formalizing Data Interoperability in an Internet of Production. *IEEE Internet Things J.* **2020**, *7*, 3243–3253. [CrossRef]
13. Matzutt, R.; Kalde, B.; Pennekamp, J.; Arthur, D.; Henze, M.; Bergs, T.; Wehrle, K. How to Securely Prune Bitcoin's Blockchain. In Proceedings of the 19th IFIP Networking 2020 Conference (NETWORKING'20), Paris, France, 22–26 June 2020; pp. 298–306.
14. Kouhizadeh, M.; Sarkis, J. Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains. *Sustainability* **2018**, *10*, 3652. [CrossRef]
15. Tijan, E.; Aksentijević, S.; Ivanić, K.; Jardas, M. Blockchain Technology Implementation in Logistics. *Sustainability* **2019**, *11*, 1185. [CrossRef]
16. Varriale, V.; Cammarano, A.; Michelino, F.; Caputo, M. The Unknown Potential of Blockchain for Sustainable Supply Chains. *Sustainability* **2020**, *12*, 9400. [CrossRef]
17. Tan, B.Q.; Wang, F.; Liu, J.; Kang, K.; Costa, F. A Blockchain-Based Framework for Green Logistics in Supply Chains. *Sustainability* **2020**, *12*, 4656. [CrossRef]
18. Trautmann, L.; Lasch, R. Smart Contracts in the Context of Procure-to-Pay. In *Smart and Sustainable Supply Chain and Logistics—Trends, Challenges, Methods and Best Practices*; Springer: Cham, Switzerland, 2020; Volume 1, pp. 3–23. [CrossRef]
19. Wang, M.; Wang, B.; Abareshi, A. Blockchain Technology and Its Role in Enhancing Supply Chain Integration Capability and Reducing Carbon Emission: A Conceptual Framework. *Sustainability* **2020**, *12*, 10550. [CrossRef]
20. Park, A.; Li, H. The Effect of Blockchain Technology on Supply Chain Sustainability Performances. *Sustainability* **2021**, *13*, 1726. [CrossRef]
21. Bekrar, A.; El Cadi, A.A.; Todosijevic, R.; Sarkis, J. Digitalizing the Closing-of-the-Loop for Supply Chains: A Transportation and Blockchain Perspective. *Sustainability* **2021**, *13*, 2895. [CrossRef]
22. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
23. Ko, T.; Lee, J.; Ryu, D. Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings. *Sustainability* **2018**, *10*, 4274. [CrossRef]
24. Lohmer, J. Applicability of Blockchain Technology in Scheduling Resources Within Distributed Manufacturing. In *Logistics Management*; Springer: Cham, Switzerland, 2019; pp. 89–103. [CrossRef]
25. Lohmer, J.; Lasch, R. Blockchain in operations management and manufacturing: Potential and barriers. *Comput. Ind. Eng.* **2020**, *149*, 106789. [CrossRef]
26. Müller, J.M.; Kiel, D.; Voigt, K.I. What Drives the Implementation of Industry 4.0? The Role of Opportunities and Challenges in the Context of Sustainability. *Sustainability* **2018**, *10*, 247. [CrossRef]
27. Glebke, R.; Henze, M.; Wehrle, K.; Niemietz, P.; Trauth, D.; Mattfeld, P.; Bergs, T. A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems. In Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS '19), Wailea, HI, USA, 8–11 January 2019; AIS: Atlanta, GA, USA; pp. 7252–7261. [CrossRef]
28. Oussous, A.; Benjelloun, F.Z.; Lahcen, A.A.; Belfkih, S. Big Data technologies: A survey. *J. King Saud-Univ.-Comput. Inf. Sci.* **2018**, *30*, 431–448. [CrossRef]
29. Jagadish, H.V.; Gehrke, J.; Labrinidis, A.; Papakonstantinou, Y.; Patel, J.M.; Ramakrishnan, R.; Shahabi, C. Big Data and Its Technical Challenges. *Commun. ACM* **2014**, *57*, 86–94. [CrossRef]

30. Kunze, I.; Glebke, R.; Scheiper, J.; Bodenbenner, M.; Schmitt, R.H.; Wehrle, K. Investigating the Applicability of In-Network Computing to Industrial Scenarios. In Proceedings of the 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS '21), Victoria, BC, Canada, 10–13 May 2021; pp. 334–340. [CrossRef]
31. Kunze, I.; Niemietz, P.; Tirpitz, L.; Glebke, R.; Trauth, D.; Bergs, T.; Wehrle, K. Detecting Out-Of-Control Sensor Signals in Sheet Metal Forming using In-Network Computing. In Proceedings of the 2020 IEEE 29th International Symposium on Industrial Electronics (ISIE '21), Kyoto, Japan, 20–23 June 2021.
32. Ślusarczyk, B.; Tvaronavičienė, M.; Haque, A.U.; Oláh, J. Predictors of Industry 4.0 technologies affecting logistic enterprises' performance: International perspective from economic lens. *Technol. Econ. Dev. Econ.* **2020**, *26*, 1263–1283. [CrossRef]
33. Oláh, J.; Aburumman, N.; Popp, J.; Khan, M.A.; Haddad, H.; Kitukutha, N. Impact of Industry 4.0 on environmental sustainability. *Sustainability* **2020**, *12*, 4674. [CrossRef]
34. Peng, H.; Liu, C.; Zhao, D.; Ye, H.; Fang, Z.; Wang, W. Security Analysis of CPS Systems Under Different Swapping Strategies in IoT Environments. *IEEE Access* **2020**, *8*, 63567–63576. [CrossRef]
35. Peng, H.; Liu, C.; Zhao, D.; Hu, Z.; Han, J. Security Evaluation under Different Exchange Strategies Based on Heterogeneous CPS Model in Interdependent Sensor Networks. *Sensors* **2020**, *20*, 6123. [CrossRef] [PubMed]
36. Henze, M. The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS '20), the 6th International Workshop on Security and Privacy in the Cloud (SPC '20), Avignon, France, 29 June–1 July 2020. [CrossRef]
37. Wang, S.; Li, D.; Zhang, Y.; Chen, J. Smart Contract-Based Product Traceability System in the Supply Chain Scenario. *IEEE Access* **2019**, *7*, 115122–115133. [CrossRef]
38. Montecchi, M.; Plangger, K.; Etter, M. It's real, trust me! Establishing supply chain provenance using blockchain. *Bus. Horiz.* **2019**, *62*, 283–293. [CrossRef]
39. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. TrustChain: Trust Management in Blockchain and IoT supported Supply Chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain '19), Atlanta, GA, USA, 14–17 July 2019; pp. 184–193. [CrossRef]
40. Pennekamp, J.; Sapel, P.; Fink, I.B.; Wagner, S.; Reuter, S.; Hopmann, C.; Wehrle, K.; Henze, M. Revisiting the Privacy Needs of Real-World Applicable Company Benchmarking. In Proceedings of the 8th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC '20), Virtual Conference, 15 December 2020; HomomorphicEncryption.org: Toronto, ON, Canada; pp. 31–44. [CrossRef]
41. Gleim, L.; Pennekamp, J.; Tirpitz, L.; Welten, S.; Brillowski, F.; Decker, S. FactStack: Interoperable Data Management and Preservation for the Web and Industry 4.0. In Proceedings of the 19th Symposium for Database Systems for Business, Technology and Web (BTW '21), Virtual Conference, 19 April–21 June 2021; Gesellschaft für Informatik: Bonn, Germany; Volume P-311, pp. 371–395. [CrossRef]
42. Korpela, K.; Hallikas, J.; Dahlberg, T. Digital Supply Chain Transformation toward Blockchain Integration. In Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS '17), Waikoloa, HI, USA, 4–7 January 2017; AIS: Atlanta, GA, USA, pp. 4182–4191. [CrossRef]
43. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 8 September 2021).
44. Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability* **2017**, *9*, 2214. [CrossRef]
45. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
46. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
47. Wüst, K.; Gervais, A. Do you need a Blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT '18), Zug, Switzerland, 20–22 June 2018; pp. 45–54. [CrossRef]
48. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. *Financ. Innov.* **2016**, *2*. [CrossRef]
49. Armknecht, F.; Karame, G.O.; Mandal, A.; Youssef, F.; Zenner, E. Ripple: Overview and Outlook. In Proceedings of the 8th International Conference on Trust and Trustworthy Computing (TRUST '15), Heraklion, Greece, 24–26 August 2015; Springer: Cham, Switzerland; Volume 9229, pp. 163–180. [CrossRef]
50. Chase, B.; MacBrough, E. Analysis of the XRP Ledger Consensus Protocol. *arXiv* **2018**, arXiv:1802.07242.
51. JPMorgan Chase & Co. Liink by J.P. Morgan. 2020. Available online: https://www.jpmorgan.com/onyx/liink (accessed on 11 April 2021).
52. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress '17), Honolulu, HI, USA, 25–30 June 2017. [CrossRef]
53. Durham, V. Namecoin. 2011. Available online: https://namecoin.org (accessed on 11 April 2021).
54. Bartoletti, M.; Pompianu, L. An analysis of Bitcoin OP_RETURN metadata. In Proceedings of the 21st International Conference on Financial Cryptography and Data Security (FC '17), Sliema, Malta, 3–7 April 2017; Springer: Cham, Switzerland; Volume 10323, pp. 218–230. [CrossRef]

55. Proof of Existence. 2015. Available online: https://proofofexistence.com (accessed on 11 April 2021).
56. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Available online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on 8 September 2021).
57. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the 13th EuroSys Conference (EuroSys '18), Porto, Portugal, 23–26 April 2018; ACM: New York, NY, USA. [CrossRef]
58. ConsenSys. Quorum. 2016. Available online: https://consensys.net/quorum (accessed on 11 April 2021).
59. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
60. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2019**, *6*, 1495–1505. [CrossRef]
61. Lin, Q.; Wang, H.; Pei, X.; Wang, J. Food Safety Traceability System Based on Blockchain and EPCIS. *IEEE Access* **2019**, *7*, 20698–20707. [CrossRef]
62. Bader, L.; Pennekamp, J.; Matzutt, R.; Hedderich, D.; Kowalski, M.; Lücken, V.; Wehrle, K. Blockchain-Based Privacy Preservation for Supply Chains Supporting Lightweight Multi-Hop Information Accountability. *Inf. Process. Manag.* **2021**, *58*. [CrossRef]
63. Malik, S.; Dedeoglu, V.; Kanhere, S.; Jurdak, R. PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains. *arXiv* **2021**, arXiv:2104.13964.
64. Malik, S.; Gupta, N.; Dedeoglu, V.; Kanhere, S.; Jurdak, R. TradeChain: Decoupling Traceability and Identity in Blockchain enabled Supply Chains. *arXiv* **2021**, arXiv:2105.11217.
65. Gonczol, P.; Katsikouli, P.; Herskind, L.; Dragoni, N. Blockchain Implementations and Use Cases for Supply Chains-A Survey. *IEEE Access* **2020**, *8*, 11856–11871. [CrossRef]
66. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Gün Sirer, E.; et al. On Scaling Decentralized Blockchains. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security (FC '16), Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany; Volume 9604, pp. 106–125. [CrossRef]
67. Barber, S.; Boyen, X.; Shi, E.; Uzun, E. Bitter to Better—How to Make Bitcoin a Better Currency. In Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC '12), Kinabalu, Malaysia, 10–14 February 2012; Springer: Berlin, Germany; Volume 7397, pp. 399–414. [CrossRef]
68. Cachin, C.; Vukolić, M. Blockchain Consensus Protocols in the Wild. In Proceedings of the 31st International Symposium on Distributed Computing (DISC '17), Vienna, Austria, 16–20 October 2017; Schloss Dagstuhl: Dagstuhl, Germany; Volume 91. [CrossRef]
69. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A Secure Sharding Protocol For Open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), Vienna, Austria, 24–28 October 2016; ACM: New York, NY, USA; pp. 17–30. [CrossRef]
70. Zamani, M.; Movahedi, M.; Raykova, M. RapidChain: Scaling Blockchain via Full Sharding. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), Toronto, ON, Canada, 15–19 October 2018; ACM: New York, NY, USA, pp. 931–948.
71. Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Syta, E.; Ford, B. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP '20), San Francisco, CA, USA, 21–23 May 2018; pp. 583–598. [CrossRef]
72. Matzutt, R.; Kalde, B.; Pennekamp, J.; Drichel, A.; Henze, M.; Wehrle, K. CoinPrune: Shrinking Bitcoin's Blockchain Retrospectively. *IEEE Trans. Netw. Serv. Manag.* **2021**. [CrossRef]
73. Matzutt, R.; Hiller, J.; Henze, M.; Ziegeldorf, J.H.; Müllmann, D.; Hohlfeld, O.; Wehrle, K. A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In Proceedings of the 22th International Conference on Financial Cryptography and Data Security (FC '18), Nieuwpoort, Curaçao, 26 February 26–2 March 2018; Springer: Berlin, Germany; Volume 10957, pp. 420–438. [CrossRef]
74. Mangel, S.; Gleim, L.; Pennekamp, J.; Wehrle, K.; Decker, S. Data Reliability and Trustworthiness through Digital Transmission Contracts. In Proceedings of the 18th Extended Semantic Web Conference (ESWC '21), Heraklion, Greece, 6–10 June 2021; Springer: Cham, Switzerland, Volume 12731, pp. 265–283.
75. Hohenberger, S.; Waters, B. Attribute-Based Encryption with Fast Decryption. In Proceedings of the 16th International Conference on Practice and Theory in Public Key Cryptography (PKC '13), Nara, Japan, 26 February–1 March 2013; Springer: Berlin, Germany, Volume 7778, pp. 162–179. [CrossRef]
76. Miller, A.; Xia, Y.; Croman, K.; Shi, E.; Song, D. The Honey Badger of BFT Protocols. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), Vienna, Austria, 24–28 October 2016; ACM: New York, NY, USA. pp. 31–42. [CrossRef]
77. Ozdemir, A.; Wahby, R.; Whitehat, B.; Boneh, D. Scaling Verifiable Computation Using Efficient Set Accumulators. In Proceedings of the 29th USENIX Conference on Security Symposium (SEC '20), Boston, MA, USA, 12–14 August 2020, USENIX Association: Berkeley, CA, USA; pp. 2075–2092.
78. Wang, G.; Shi, Z.J.; Nixon, M.; Han, S. SoK: Sharding on Blockchain. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT '19), Zurich, Switzerland, 21–23 October 2019; ACM: New York, NY, USA; pp. 41–61. [CrossRef]

79. Pennekamp, J.; Alder, F.; Matzutt, R.; Mühlberg, J.T.; Piessens, F.; Wehrle, K. Secure End-to-End Sensing in Supply Chains. Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS '20), Avignon, France, 29 June–1 July 2020. [CrossRef]
80. Pennekamp, J.; Bader, L.; Matzutt, R.; Niemietz, P.; Trauth, D.; Henze, M.; Bergs, T.; Wehrle, K. Private Multi-Hop Accountability for Supply Chains. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops '20), the 1st Workshop on Blockchain for IoT and Cyber-Physical Systems (BIoTCPS '20), Dublin, Ireland, 7–11 June 2020. [CrossRef]
81. Hu, L.; Nguyen, N.T.; Tao, W.; Leu, M.C.; Liu, X.F.; Shahriar, M.R.; Al Sunny, S.M.N. Modeling of cloud-based digital twins for smart manufacturing with MT connect. *Procedia Manuf.* **2018**, *26*, 1193–1203. [CrossRef]
82. Coronado, P.D.U.; Lynn, R.; Louhichi, W.; Parto, M.; Wescoat, E.; Kurfess, T. Part data integration in the Shop Floor Digital Twin: Mobile and cloud technologies to enable a manufacturing execution system. *J. Manuf. Syst.* **2018**, *48*, 25–33. [CrossRef]
83. Zambal, S.; Eitzinger, C.; Clarke, M.; Klintworth, J.; Mechin, P.Y. A digital twin for composite parts manufacturing: Effects of defects analysis based on manufacturing data. In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN '18), Porto, Portugal, 18–20 July 2018; pp. 803–808. [CrossRef]
84. Jarke, M.; Schuh, G.; Brecher, C.; Brockmann, M.; Prote, J.P. Digital Shadows in the Internet of Production. *ERCIM News* **2018**, *115*, 26–28.
85. Becker, F.; Bibow, P.; Dalibor, M.; Gannouni, A.; Hahn, V.; Hopmann, C.; Jarke, M.; Kröger, M.; Lipp, J.; Maibaum, J.; et al. A Conceptual Model for Digital Shadows in Industry and its Application. In Proceedings of the 40th International Conference on Conceptual Modeling (ER'21), St. John's, NL, Canada, 18–21 October 2021.
86. Bibow, P.; Dalibor, M.; Hopmann, C.; Mainz, B.; Rumpe, B.; Schmalzing, D.; Schmitz, M.; Wortmann, A. Model-Driven Development of a Digital Twin for Injection Molding. In Proceedings of the 32nd International Conference on Advanced Information Systems Engineering (CAiSE '20), Grenoble, France, 8–12 June 2020; Springer: Cham, Switzerland; Volume 12127, pp. 85–100. [CrossRef]
87. Schuh, G.; Häfner, C.; Hopmann, C.; Rumpe, B.; Brockmann, M.; Wortmann, A.; Maibaum, J.; Dalibor, M.; Bibow, P.; Sapel, P.; et al. Effizientere Produktion mit Digitalen Schatten. *ZWF Z. FüR Wirtsch. Fabr.* **2020**, *115*, 105–107. [CrossRef]
88. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM '16), Kunming, China, 24–26 June 2016. [CrossRef]
89. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Future Internet* **2019**, *11*, 161. [CrossRef]
90. Leng, J.; Jiang, P.; Xu, K.; Liu, Q.; Zhao, J.L.; Bian, Y.; Shi, R. Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing. *J. Clean. Prod.* **2019**, *234*, 767–778. [CrossRef]
91. Buckhorst, A.F.; Montavon, B.; Wolfschläger, D.; Buchsbaum, M.; Shahidi, A.; Petruck, H.; Kunze, I.; Pennekamp, J.; Brecher, C.; Hüsing, M.; et al. Holarchy for Line-less Mobile Assembly Systems Operation in the Context of the Internet of Production. *Procedia CIRP* **2021**, *99*, 448–453. [CrossRef]
92. Pennekamp, J.; Henze, M.; Wehrle, K. Unlocking Secure Industrial Collaborations through Privacy-Preserving Computation. *ERCIM News* **2021**, *126*, 24–25.
93. Matzutt, R.; Müllmann, D.; Zeissig, E.M.; Horst, C.; Kasugai, K.; Lidynia, S.; Wieninger, S.; Ziegeldorf, J.H.; Gudergan, G.; Spiecker gen. Döhmann, I.; et al. myneData: Towards a Trusted and User-controlled Ecosystem for Sharing Personal Data. In *INFORMATIK*; Gesellschaft für Informatik: Bonn, Germany, 2017; Volume 275, pp. 1073–1084. [CrossRef]
94. Zyskind, G.; Nathan, O.; Pentland, A.S. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Symposium on Security and Privacy Workshops (SPW '15), San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]