IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 May 2024, accepted 23 July 2024, date of publication 29 July 2024, date of current version 30 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3435374

SURVEY

An Overview of Blockchain for Industry 5.0: Towards Human-Centric, Sustainable and Resilient Applications

PAULA FRAGA-LAMAS[1,2], (Senior Member, IEEE), TIAGO M. FERNÁNDEZ-CARAMÉS[1,2], (Senior Member, IEEE), ANTÓNIO M. ROSADO DA CRUZ[3,4], AND SERGIO IVAN LOPES[3,5,6], (Senior Member, IEEE)

[1]Department of Computer Engineering, Faculty of Computer Science, Universidade da Coruña, 15071 A Coruña, Spain
[2]Centro de Investigación CITIC, Universidade da Coruña, 15071 A Coruña, Spain
[3]ADiT-Lab, Instituto Politécnico de Viana do Castelo, 4900-348 Viana do Castelo, Portugal
[4]ALGORITMI Research Centre, Escola de Engenharia, Universidade do Minho, 4800-058 Guimaraes, Portugal
[5]CiTin—Centro de Interface Tecnológico Industrial, 4970-786 Arcos de Valdevez, Portugal
[6]IT—Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

Corresponding author: Paula Fraga-Lamas (paula.fraga@udc.es)

This work has been funded by the Xunta de Galicia (by grant ED431C 2020/15), and by grants PID2020-118857RA-100 (ORBALLO) and TED2021-129433A-C22 (HELENE) funded by MCIN/AEI/10.13039/501100011033 and the European Union NextGenerationEU/PRTR. We wish to acknowledge the support received from the Centro de Investigación de Galicia "CITIC", funded by Xunta de Galicia and the European Union. Paula Fraga-Lamas and Tiago M. Fernández-Caramés would like to thank CITIC for its support for the research stay that led to this article. Sergio Ivan Lopes has been funded by grant NORTE-01-0145-FEDER-000043, in the scope of project TECH–Technology, Environment, Creativity and Health, supported by Norte Portugal Regional Operational Program (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF).

ABSTRACT Industry 5.0 is an evolving concept that aims to enhance the way modern factories operate by seeking long-term growth, production efficiency and the well-being of industrial workers. Human-centricity, sustainability and resilience are the three pillars of Industry 5.0, which are developed on Industry 4.0 enabling technologies. One of the most compelling technologies to help implement the communications architecture proposed by Industry 5.0 is blockchain, which can provide trustworthy, secured and decentralized information to different industrial domains. This article provides an analysis of the transition between Industry 4.0 and Industry 5.0 paradigms. Moreover, it examines the benefits and challenges that arise when using blockchain to develop Industry 5.0 applications and analyzes the design factors that should be considered when developing this type of applications. Furthermore, it presents a thorough review on the most relevant blockchain-based applications for Industry 5.0 pillars. Therefore, the main goal of this article is to provide a comprehensive and detailed guide for future Industry 5.0 developers that allows for determining how blockchain might benefit the next generation of human-centric, sustainable, and resilient applications.

INDEX TERMS Industry 5.0, blockchain, human-centricity, sustainability, resilience, smart factories, Society 5.0.

I. INTRODUCTION

Industry 5.0 is a concept that has been put forward by the European industry and that has been fostered by the European Commission [1]. Such a concept harnesses previous Industry 4.0 technologies [2] not only for increasing growth and efficiency, but also towards reaching societal goals focused on production sustainability and the well-being of workers. Thus, Industry 5.0 complements the Industry 4.0 paradigm to make industry human-centric, sustainable and resilient.

The previous Industry 4.0 paradigm represented a natural evolution of traditional factories towards smart factories, whose main objective was to make efficient use of resources

The associate editor coordinating the review of this manuscript and approving it for publication was Daniela Cristina Momete.

and to be able to adapt to the ever-changing production requirements [3]. The term Industry 4.0 was coined initially in 2011 as 'Industrie 4.0' by the German government [4], [5] and shares similarities with the concepts behind the Industrial Internet of Things (IIoT) [6]. Other countries have also proposed similar initiatives, like Internet Plus [7] or Made in China 2025 [8].

During the last years, Industry 4.0 focused essentially on how to digitalize factories to make production processes more efficient and flexible, leaving part of its original principles related to social fairness and sustainability. As a consequence, Industry 5.0 seeks to focus more on such principles while supporting industry in its long-term service to society and without removing workers from the realm of industrial manufacturing.

Although Industry 5.0 is an evolving concept [9], its foundations come from the Industry 4.0 paradigm, which establishes that a smart factory should collect as much data as possible from the multiple processes involved in the value chain. Moreover, the gathered information needs to be collected fast, efficiently and sustainably to be useful for an Industry 5.0 factory. For such an aim, it is necessary to make use of systems that can acquire, process, store and exchange data among devices deployed throughout a factory, with operators, industrial suppliers and customers.

To provide the necessary connectivity, Industry 5.0 relies on most of the technologies previously developed by Industry 4.0, as well as new promising technologies that have arisen in the last years and that are called to disrupt the way current factories operate. Figure 1 illustrates how some of the most relevant Industry 5.0 technologies are related to the eight main application domains established by the European Commission [10]:

- Artificial intelligence and robots.
- Human-Machine Inferfaces (HMI) and biomimetics.
- Electronics and computing.
- Biohybrids.
- Biomedicine.
- Printing and materials.
- New green materials, processes, and technologies.
- Energy.

In addition, the European Commission indicates that Industry 5.0 companies should also consider new societal innovation aspects, like the use of collaborative innovation spaces, gamification, new education and training platforms, or cryptocurrencies [10]. Thus, technologies like Augmented Reality (AR) [12], [13], IIoT [14], Unmanned Aerial Vehicles (UAVs) [15], [16], Industrial Cyber-Physical Systems (ICPSs) [17], Artificial Intelligence (AI) and federated learning [18], fog [19] or Edge Computing [20], [21], which have been extensively used in the last years by Industry 4.0 factories, enable fulfilling requirements of the previously mentioned application domains and societal innovations [22], and allow for interconnecting all the involved entities in a way that is similar to a Peer-to-Peer (P2P) network (as illustrated in Figure 2).

Distributed Ledger Technologies (DLTs) are among the technologies that can help to jointly implement the communications architecture proposed by Industry 5.0. The most well-known DLT was officially brought to the public in 2008 with the release of Bitcoin, a cryptocurrency capable of tracking and storing financial transactions and avoiding the double-spending problem in a decentralized way [23]. In such a kind of initial application of blockchain, transactions are first verified by computing nodes, packed in blocks linked by hashes, and then added to the blockchain by following a consensus protocol (i.e., nodes reach a consensus on how to add the transaction block to the blockchain) [24].

A detailed explanation of the inner workings of DLTs is out of the scope of this article, but the interested reader can find additional details on the fundamentals and the different platforms in Section II-E and in [28] and [29].

This article analyzes how blockchain can help Industry 5.0 to enhance previous Industry 4.0 technologies and then develop human-centered, sustainable and resilient industrial systems. Specifically, this article includes the following significant contributions, which have not previously been found together in the literature:

- A comparative analysis between Industry 4.0 and 5.0 paradigms is provided together with their essential concepts, in order to guide in the transition between Industry 4.0 and 5.0 paradigms.
- A thorough analysis of the benefits and challenges of the development of blockchain-based Industry 5.0 applications is provided.
- An analysis on the blockchain key design factors that impact Industry 5.0 application development is provided.
- The impact of the use of blockchain on the Industry 5.0 main pillars (i.e., human-centricity, sustainability, and resilience) is studied.
- A detailed review on the latest and most relevant blockchain-based Industry 5.0 applications is presented.
- The main challenges of the implementation of blockchain-based Industry 5.0 applications are identified and discussed.
- An extensive list of recommendations for future Industry 5.0 developers is provided to guide them in the selection and implementation of the next generation of human-centric, sustainable and resilient applications.

The rest of this paper is structured as follows. Section II describes the essential Industry 5.0 concepts together with their main challenges and benefits. In addition, such a Section provides a generic industrial process model that allows for illustrating the main areas where blockchain can help. Furthermore, the basics of blockchain are briefly presented. Section III analyzes the use of blockchain for industrial environments and studies the advantages, issues and design factors that should be considered when developing blockchain-based Industry 5.0 applications. Section IV provides a thorough review on current and potential Industry 5.0 applications based on blockchain. Finally,

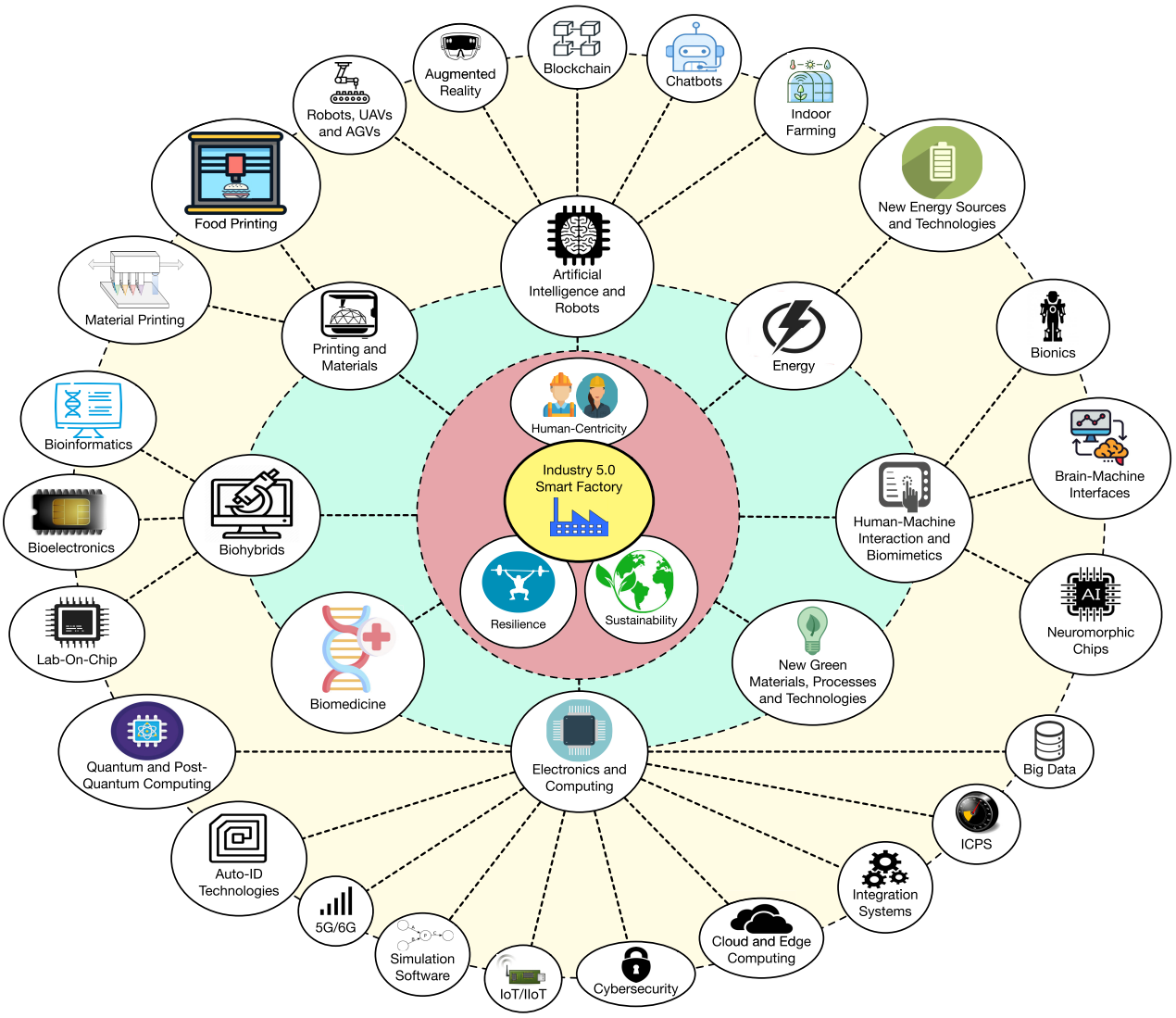

FIGURE 1. Main Industry 5.0 application domains and technologies.

Section V details the most relevant challenges involved in the application of blockchain to Industry 5.0, while Section VI is devoted to conclusions.

II. ABOUT INDUSTRY 5.0 AND BLOCKCHAIN

Before delving into how blockchain can benefit Industry 5.0, it is first necessary to understand the objectives and challenges of such a new paradigm. Thus, the next subsections describe the basics of Industry 5.0, the reasons to move from Industry 4.0 to Industry 5.0, and the main issues and opportunities that may arise along such a transition. In addition, a generic industrial process model for Industry 5.0 is briefly introduced, along with the main concepts of blockchain and DLTs.

A. ESSENTIAL CONCEPTS

Although the definition of the concept of Industry 5.0 is still open, the European Commission has already stated that it is the basis for the development of the future European industry [1]. Such a basis contemplates the potential of the industry to reach societal goals beyond just jobs and economic growth, focusing on production sustainability and industrial worker well-being [47], [48]. However, Industry 5.0 has not been proposed as a chronological continuation to Industry 4.0, but as a complement to it that adds emerging societal trends to industrial development [49]. Since 2011, Industry 4.0 has set the foundations for the creation of smart digitalized factories, but the changes brought by Industry 4.0 have usually forgotten two essential principles: social fairness and sustainability. Therefore, Industry 5.0 focuses not only on efficiency or technological aspects, but also on environmental and social issues.

Industry 5.0 seems to be inspired by the concept of Society 5.0 [50], which was first proposed by the Japanese government in 2015 [51] and then (in 2016) promoted by one of the most relevant business federations of Japan

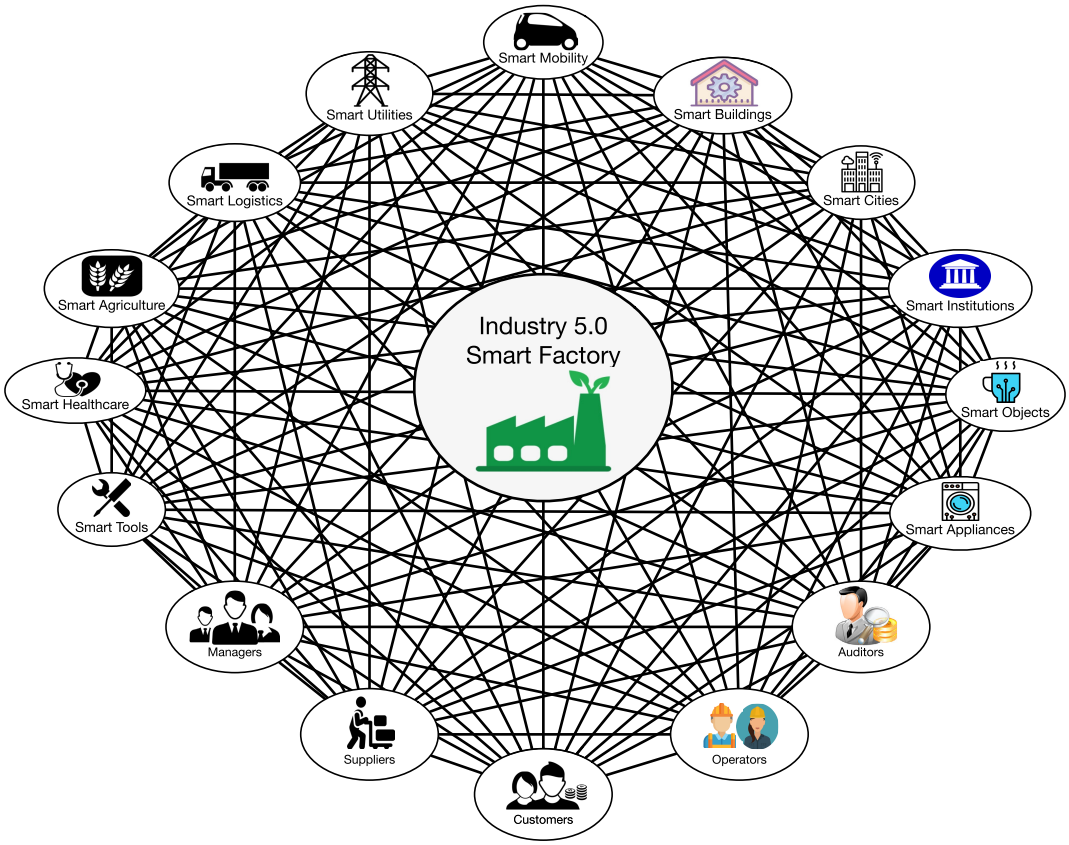

FIGURE 2. Ideal communications architecture of an Industry 5.0 factory with examples of some the most commonly involved entities (e.g., stakeholders, sectors).

(Keidanren) [52]. Society 5.0 goes beyond mere individual company transformations and proposes a collective strategy to transform Japanese society like it has happened in the past with radical ways of living and technological changes. Thus, hunting and gathering are considered, respectively, to be the basis for 'Society 1.0' and 'Society 2.0'; the industrial revolution initiated in the 18th century derived in the creation of a 'Society 3.0'; and information and digitalization have arisen as the foundations of current 'Society 4.0'. Society 5.0 fosters economic development while solving societal and environmental problems. Such a vision requires that both industry and society solve the issues and challenges that arise from the integration of the physical and virtual worlds. As a consequence, Society 5.0 is based on the use of some of the aforementioned IT technologies (e.g., Internet of Things (IoT) devices, AI, robotics, or AR) in our daily lives and by the industry.

B. MOVING FROM INDUSTRY 4.0 TOWARDS INDUSTRY 5.0

Industry 4.0 and similar paradigms have fostered digitalization and industrial efficiency during the last years, but there are significant challenges still to be faced and new ones that have arisen with the application of new technologies. The following are the main reasons to move forward and follow the guidelines provided by Industry 5.0:

- Industry 4.0 contributes to globalization, although the extent and the manner of its impact varies among companies, depending on factors such as company size, objectives, capabilities and industry domain. Initially, this impact was felt at the Operational Technology (OT) level, controlling physical devices and processes and eliminating data and communication silos, while the integration at the information technology (IT) level from Manufacturing-Execution Systems (MES) and Enterprise Resource Planning (ERP) solutions remained an area of ongoing research and development within the context of digitalization (e.g., interoperability), with implications for globalization. As manufacturers adopt Industry 4.0 principles and take steps towards IT/OT convergence, they emerge as a driving force behind the new wave of globalization. Nonetheless, although globalization has brought economic prosperity to many parts of the world, it has also increased inequality. Such a situation has weakened critical supply value chains and, in many cases, resulted in environmental problems and overuse of natural resources.
- Certain technologies have brought innovation to the industrial sector, but their use can also pose risks to humans (i.e., worker well-being) and ecosystems.

TABLE 1. Moving from Industry 4.0 towards Industry 5.0.

Aspect	Industry 4.0	Industry 5.0
Focus	Automation, digitization of processes, data exchange, IoT	Human-centric collaboration (unique abilities of humans with efficiency and accuracy of machines) for flexible and personalized manufacturing
Motivation	Mass production, Efficiency, Automation, Cost Reduction	Smart Society, Society 5.0, Sustainability and inclusive growth, Optimizing Human Potential, Well-being
Integration	Cyber-Physical Systems	Human-Machine symbiosis
Role of workforce	Machines work alongside humans, human supervision and intervention	Boosting unique human abilities that add value, such as creativity, decision-making, and complex problem-solving in a collaborative environment.
Key technologies	IoT, cloud Computing, AI, edge computing, robotics	All Industry 4.0 technologies and new promising technologies (e.g., advanced human-machine interfaces, bioeconomy technologies, post-quantum computing)
Data utilization	Data-driven decision-making	Enhanced human experience
Flexibility	Adaptive and customizable manufacturing	Human-driven adaptability
Customization	Mass customization and personalization	Tailored products and experiences
Responsiveness	Real-time data analysis and reaction	Real-time human-machine interaction
Supply Chain	Smart Logistics, predictive maintenance	Human-enhanced supply chain integration, distributed supply chain
Safety and ergonomics	Enhanced safety through automation	Prioritizing human well-being
Environmental concerns	Energy efficiency, sustainable practices, discharge of waste, intensive use of raw materials	Holistic environmental impact mitigation (preservation of society and environment), circular economy, bio-economy
Resilience	Emphasis on reactivity and adaptability	Focus on anticipating disruptions and strategic autonomy

- Industry 4.0 technologies need to evolve to adapt to initiatives like the European Green Deal [53], which describes a strategy to make Europe climate-neutral in 2050. Currently, Industry 4.0 lacks key design and performance dimensions to decouple resource use from negative environmental and climate impacts [54]. These dimensions comprise three main aspects. First, to include regenerative features into industrial transformation to embrace circular economy and positive restorative feedback loops as a key pillar of the design of entire value chains. Second, to include a mandatory environmental dimension, which leads to the elimination of fossil fuels, the promotion of energy efficiency and on nature-based solutions, regeneration of carbon sinks, restoration of biodiversity and respectful interdependence with natural systems. Third, to include an inherently social dimension, emphasizing the well-being of workers, the need for social inclusion and the adoption of technologies that complement rather than substitute human capabilities.
- Despite the benefits of Industry 4.0 technology adoption, digitalization varies significantly from one company to another. In fact, in certain industrial sectors, the fragmentation in multiple small companies prevents them from making the large investments required to make use of certain state-of-the-art technologies that would allow them to compete in a global market. Moreover, certain technologies like AI, despite their usefulness, have not been adopted by many companies because they are limited by their previous developments (i.e., such companies would need to carry out a significant transformation in their hardware or software to make use of technologies like AI). In addition, technologies like Artificial Intelligence (AI) face sustainability and ecological footprint challenges. Thus, there is increasing pressure on computing resources to train as well as to run AI models, which are becoming more accurate but also more computationally intensive. There are novel and more environmentally friendly practices to implement and deploy AI solutions like Green AI (where efficiency often takes precedence over model accuracy) or Edge AI (where decisions are taken faster and in a more secure way as the processing of data collected is performed at the edge of the network). Nevertheless, the aforementioned approaches still have to face additional challenges in terms of latency, cybersecurity and, most importantly, energy efficiency [55].
- Technology has evolved remarkably since the conception of Industry 4.0 in 2011, and new technologies were not even considered by such a paradigm (e.g., generative AI, quantum blockchain). Therefore, after more than 12 years, it is necessary to evolve and to expand the guidelines provided by Industry 4.0 to consider the latest disruptive technologies [10], [11] (e.g., individualized human-machine-interaction; bio-inspired technologies and smart materials; digital twins and simulation; data transmission, storage, and analysis technologies; Artificial Intelligence; technologies for energy efficiency, renewables, storage and autonomy to achieve emission neutrality), which face additional challenges for value generation and require a more systematic innovation approach to integrate social, economical and ecological perspectives on industrial ecosystems [11].

- Society has also evolved and societal concerns remain paramount. For example, one of the primary challenges in the field of AI lies in the spread of fake news and deepfakes [56], both of which have, for instance, significant implications for the integrity of democratic processes.
- In addition, relevant recent events have impacted value chains and have dramatically changed the way many people live and how certain industries operate. For example, the COVID-19 pandemic led to a significant contraction in both demand and supply due to the implementation of lockdown measures worldwide [57]. This situation exposed firms involved in international trade to disruptions on a global scale, in addition to domestic ones. These disruptions manifested as a decline in foreign demand for exporters and a supply reduction resulting in a shortage of intermediate inputs for importers. Moreover, the Russia-Ukraine conflict has significantly impacted the global supply chain, obstructing the movement of goods, triggering substantial cost increases, and causing product shortages [58]. Other conflicts, like the war in Gaza or the U.S.-China trade conflict have drastically influenced value chains, affecting not only the countries directly involved but also global economy [59], [60].

As a summary, Table 1 compares the main reasons for moving from Industry 4.0 towards Industry 5.0.

C. MAIN CHALLENGES AND BENEFITS FROM INDUSTRY 5.0

The foundations of Industry 5.0 rely on three main principles:

- Industry needs to be human-centric [48], so we, as humans, need to ask what new technology can do for us instead of what we can do with such a technology. Similarly, instead of forcing industrial workers to adapt to new technologies, we should wonder how such technologies can be adapted to the worker's needs to perform a production task efficiently and safely while respecting his or her rights (e.g., worker privacy). Moreover, Industry 5.0 needs to consider the impact on society regarding the use of new technologies, which is essential for workers whose jobs may be threatened or whose tasks may change significantly, thus requiring them to acquire new skills. As a consequence, Industry 5.0 researchers have to focus more on the analysis of how technologies can benefit industrial workers, rather than threatening their jobs at the cost of not respecting the environment or human rights.
- Industry needs to be sustainable [61], [62]. Such sustainability requires minimizing energy consumption, reducing greenhouse emissions, and avoiding degrading natural resources. In the case of the European economy, the Green Deal will have to be considered by Industry 5.0 since it will involve transitioning to a circular economy [63] and to the use of sustainable resources and renewable energy sources.
- Industry production not only has to be flexible and adaptable (as Industry 4.0 already requires) but also agile and resilient [64]. Regarding the latter, it is related to the enhancement of production robustness against disruptions (e.g., geopolitical events like Brexit or trade-wars, or natural crises like the COVID-19 pandemic or climate change) or cyberattacks, especially those aimed at critical infrastructures linked to current globalized production chains. Therefore, an Industry 5.0 factory needs to develop resilient value chains and has to be able to adapt its production capacity and business processes in an agile way.

The previous principles, when implemented correctly, can derive the following main benefits:

- Better worker safety and well-being.
- Industrial worker empowerment focused on the collaboration between them and the deployed smart devices. Thus, high-speed devices that will carry out repetitive or dangerous tasks can be merged with the cognitive abilities of the workers.
- Improved resource efficiency may end up reducing costs and the reliance on imports.
- Attraction to the industry to the best 'millennial' talent, which is more prone to be driven by social values rather than high salaries respect to previous generations [65].
- Easier training by adapting it to the worker's skills and previous knowledge.
- Better competitiveness in new markets where technology is a differential factor.

Table 2 outlines the differences between Industry 4.0 and Industry 5.0, comparing them through examples of relevant Key Performance Indicators (KPIs).

D. GENERIC INDUSTRIAL PROCESS MODEL

The process model for any industrial product can be generically defined as depicted in Figure 3. The presented process model is centered on the value chain activities that should be traced. These activities are important in the business process model of each participant, but as the focus here is on the value chain, these participants are represented as external participants in the process model and linked to the activities for which they may be responsible.

The participants in the generic industrial process model are:

1) Producer: Collects or produces raw materials for industrial processes.
2) Industry: Transforms raw materials and assembles components for the production of an industrial product. Some of the materials or components may be reconditioned, even as a result of recycling processes. Some industry participants deal with products for recycling, where they use parts separated from used products to produce new materials for industrial processes.
3) Logistics Company: Transports and distributes intermediate and final products.
4) Retailer: Sells final products to end customers.

TABLE 2. Examples of KPIs, their associated categories and brief definitions for both Industry 4.0 and the concept of Industry 5.0.

Category	KPI	Brief KPI definition	Industry 4.0	Industry 5.0
Operational efficiency	Overall Equipment Effectiveness (OEE)	Measures the overall efficiency of a manufacturing process, considering availability, performance, and quality.	Core KPI	N/A
	Downtime percentage	Tracks the percentage of time that machinery or systems are not operational due to unplanned outages or maintenance.	Core KPI	Enhanced significance
	Utilization of IoT devices	Evaluates the percentage of active IoT devices contributing to data-driven decision-making.	Core KPI	N/A
	Energy efficiency	Monitors energy consumption.	Core KPI	Enhanced significance
	Quality yield	Measures the percentage of produced goods meeting predefined quality standards.	Core KPI	Adjusted for human-centric approach
	Supplier defect rate	Measures the rate of defects in supplied materials or products.	Core KPI	N/A
	Emergency purchases rate	Measures the frequency of unplanned purchases due to emergencies or shortages.	Core KPI	Enhanced significance
	Supplier lead time	Measures the time taken for a supplier to deliver goods after receiving an order.	Core KPI	N/A
	PO cycle time	Measures the time taken for a purchase order to be processed from initiation to completion.	Core KPI	N/A
	Lead time	Measures the time taken for a process to be completed from start to finish.	Core KPI	N/A
	Vendor/Material availability	Measures the availability of vendors or materials needed for production.	Core KPI	Enhanced significance
	Cash flow	Tracks the flow of cash in and out of the business over a specific period.	Core KPI	N/A
	Cost per product/invoice	Measures the cost associated with producing a single unit or processing an invoice.	Core KPI	Adjusted for human-centric approach
	ROI	Measures the return on investment of the business.	Core KPI	Adjusted for human-centric approach
	Operation expenses	Tracks the expenses associated with ongoing operations of the business.	Core KPI	Adjusted for human-centric approach
Human-Centricity	Workforce skills	Measures the overall level of skills and adaptability of the workforce in relevant technical and soft skills.	Core KPI	Adjusted for enhanced human-machine collaboration (re-skilling, up-skilling, long-life training)
	Worker wellbeing	Measures the physical and mental well-being of workers in the workplace.	N/A	Core KPI
	Human-centric approach for digital technologies	Emphasizes the extent to which digital technologies are designed with a user-centered approach.	N/A	Core KPI
	Human well-being index	Provides a holistic measure of the impact of operations on the well-being of individuals.	N/A	Core KPI
	Human-AI collaboration ratio	Evaluates the extent of collaboration between human and AI systems in achieving tasks or goals.	N/A	Core KPI
	User Experience (UX) rating	Assesses the satisfaction and usability of interfaces and interactions.	N/A	Core KPI
	Customization index	Quantifies the degree of tailoring products or services to individual customer preferences.	N/A	Core KPI
Sustainability	Efficiency of natural resources	Measures the efficiency of resource utilization in production processes to minimize waste, make better use of natural resources and maximize the value obtained from each unit of resource [62].	N/A	Core KPI
	Circular production models	Focuses on implementing circular economy principles, such as recycling and reusing materials, in production processes.	N/A	Core KPI
	Environmental impact index	Measures the ecological footprint and overall environmental impact of operations. Measures the extent to which operations are conducted in a sustainable and environmentally responsible manner.	N/A	Core KPI
	Energy consumption and savings	Tracks energy consumption and identifies opportunities for energy savings in operations.	Core KPI	Enhanced significance
Resilience	Resilience to disruptions or unexpected events	Measures the ability of systems to adapt and recover from disruptions or unexpected events.	N/A	Core KPI
	Supply chain visibility	Measures the availability of real-time data and insights throughout the supply chain.	Core KPI	Adjusted for human-centric approach
	Supply chain responsiveness	Assesses how quickly the supply chain can adapt to changes in demand, disruptions, or market trends.	N/A	Core KPI
Innovation	Innovation rate	Tracks the frequency and success of new technological or process innovations.	Core KPI	Core KPI

5) Recycling Company: Collects and separates end-of-life products to recover their original components and materials or to produce new materials incorporating recycled products.

The generic industrial process depicted in Figure 3 focuses on Business-to-Business (B2B) activities, which are activities towards producing an industrial product for an end-customer, and Business-to-Customer (B2C) activities, which focus on the relation between business partners and end-customers. We deliberately left at an abstract level the Customer-to-Customer (C2C) activities, which, in a circular economy process, may involve repair and maintenance activities to extend the useful lifespan of products and rental or transaction of second-hand products.

Industry 5.0 provides a novel framework for understanding and organizing B2B, B2C/C2B and C2C activities. For instance, Industry 5.0 promotes sustainability in B2B interactions by encouraging businesses to adopt environmentally friendly practices. It also emphasizes a human-centric approach by considering the welfare of employees in business processes. Regarding B2C/C2B, the human-centric pillar of Industry 5.0 puts the consumer at the center of business activities. Businesses are encouraged to tailor their products and services to meet the specific needs of consumers. The resilience pillar also comes into play, as businesses need to be adaptable to changing consumer demands. In a C2C setting, Industry 5.0 emphasis on sustainability can encourage consumers to engage in environmentally friendly

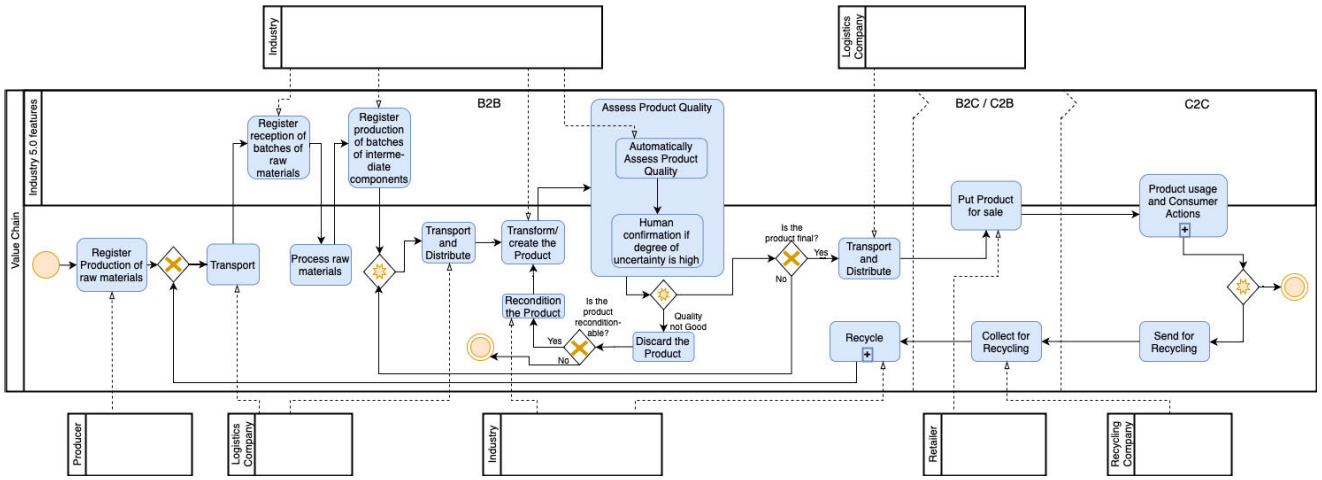

FIGURE 3. B2B/B2C Industrial business process model (adapted from [239]).

transactions. The resilience pillar also promotes adaptability in the face of changing market conditions.

Blockchain, with its ability to involve multiple stakeholders and to react to events that impact the value chain through smart contracts, provides a trustworthy, transparent, and efficient platform for managing these B2B, B2C/C2B and C2C interactions.

In essence, the combination of blockchain and Industry 5.0 can help facilitate a smooth transition from a linear to a circular economy by effectively managing B2B, B2C, and C2C activities. This synergy could potentially revolutionize our economic system, making it more sustainable and inclusive.

E. BASICS OF BLOCKCHAIN AND DLTS

Distributed Ledger Technologies (DLTs) are based on a distributed transaction scheme in a P2P network without a central authority. Each network node has a copy of the data, which is verified and updated by a consensus protocol among the nodes. Such data are encrypted and secured by advanced cryptography, making it very difficult to tamper with.

As it was previously indicated, the most common form of DLT is the blockchain, where each transaction is recorded in blocks linked together by cryptographic hashes that form a chain [24].

Although blockchain is well known for being the technology behind cryptocurrencies, it can also be used for other applications that can take advantage of removing intermediaries and that require security, transparency, accountability and decentralization.

In blockchains like Bitcoin, block validation is carried out by nodes called miners, which are collectively responsible for preserving the trustworthiness of the blockchain in an environment where entities may not trust each other (i.e., blockchain nodes allow for implementing a solution to the Byzantine Generals' Problem [66]). The specifics of how a blockchain works internally are out of the scope of this article, but further information can be found in [67], [68], [69], and [70].

Table 3 shows the main characteristics of the most popular DLTs. As it can be observed, there exists a wide variety of blockchains/DLTs, each characterized by its different features.

In this regard, four main types of blockchains can be distinguished: public, private hybrid and federated. Public blockchains can be accessed by anyone, who can also publish and validate transactions (usually in exchange for a reward). The currently most relevant public blockchains are Bitcoin [23] and Ethereum [114].

In the case of private blockchains, access and inner rules (e.g., consensus mechanism, rewards) are controlled by the blockchain owner. Due to this way of operating, which differs significantly from the original Bitcoin and cannot be considered entirely decentralized (due to the existence of a blockchain regulator), some authors do not consider private blockchains as actual blockchains. The reason is that blockchains originated from the need to provide trust among non-trusted parties, so if there is a central regulator that is trusted to control the inner workings of the blockchain, then a blockchain would probably make no sense and a secure distributed transaction-based database would probably be a better choice for industrial scenarios. An example of a private blockchain is Ripple [115].

Hybrid blockchains combine elements of both private and public blockchains to leverage the advantages of both models. For example, some data can be restricted to specific organizations or they can restrict access to certain participants.

The fourth main type of blockchain is federated blockchains (also called consortium blockchains), whose access and rules are controlled by a reduced group of owners. Among the factors controlled by the owners is the way the implemented consensus mechanism operates, which, to react

TABLE 3. Main characteristics of the most popular DLTs.

DLT Platform	Type of DLT	Consensus Mechanism	Purpose	Features	Cryptocurrency	Data Model	Smart Contract Support	Throughput (TPS)
Hyperledger	Private, permissioned	Byzantine Fault Tolerance (BFT)	Enterprise	Permissioned blockchain, high levels of privacy and confidentiality, modular architecture, interoperability	No	Account-based model	Yes, using Hyperledger Fabric and Hyperledger Sawtooth frameworks	High (Hyperledger Fabric 2.5 Performance, 1500+ TPS [30])
Polkadot	Hybrid	Nominated Proof of Stake (NPoS)	Interoperability, cross-chain interoperability, scalability	Sharding, parachains, shared security, and cross-chain messaging features	DOT token	Account-based mode	Yes, using Substrate framework and Ink smart contract language	High (1000+ TPS [31])
Corda	Private, permissioned	Notary services	Financial services and supply chain management	Privacy, scalability and interoperability with other Corda networks	No	UTXO-based model with state objects called states	Yes, using Corda's Contract DSL smart contract language and Corda's Flow Framework for business logic implementation.	Very high (Corda Enterprise 4, 2580 TPS [32])
Ethereum 2.0	Public, permissionless	Proof of Stake (PoS)	Decentralized applications (dApps) and Smart contracts, decentralized and regenerative finance (DeFi/ReFi), non-fungible tokens (NFTs)	Sharding, eWASM virtual machine, Casper FFG consensus mechanism, and scalability features	Ether (ETH)	Account-based model	Yes (Solidity smart contract language)	Very high (100,000 TPS using ZK-Rollups [33])
Bitcoin	Public, permissionless	Proof of Work (PoW)	Digital currency	Decentralization, security, scarcity and censorship-resistance features	Bitcoin (BTC)	UTXO-based model	No smart contract support	Very low (7 TPS)
Polygon	Public, permissionless	Proof of Stake (PoS)	Scaling solution for Ethereum	Faster and cheaper transactions, interoperability with Ethereum	MATIC token	Account-based model with EVM compatibility	Yes (Solidity smart contract language)	Very high (Polygon PoS Chain (a sidechain), theoretical limit of 7200 TPS [34])
Avalanche	Public, permissionless	Avalanche consensus	Decentralized applications (dApps) and financial services	High throughput, low latency, interoperability with other blockchains	AVAX	UTXO	Yes	Very high (143,322 TPS, HyperSDK upgrade [35])
Cosmos	Hybrid	Tendermint consensus	Interoperability between blockchains	Inter-blockchain communication (IBC), modular architecture, scalability	ATOM	Account-based	Yes	Variable per chain [36]
Kaspa	Public, permissionless	GhostDAG	Designed for microtransactions	DAG-based, parallel block validation	Kaspacoin (KSP)	UTXO	Yes (via Avalanche)	High (3,000 TPS [37])
IOTA	Public, permissionless	Tangle	IoT, Machine-to-Machine transactions	DAG-based, feeless, lightweight	IOTA (MIOTA)	Directed Acyclic Graph (DAG)	No	Very high (10,000 TPS, Pollen update v0.2.2 [38])
EOS	Public, permissioned	Delegated Proof of Stake (DPoS)	Decentralized applications, Smart contracts	High throughput, fast block times	EOS (EOS)	Account-based	Yes (via WebAssembly)	Very high (10,000 TPS, [39])
Cardano	Public, permissionless	Ouroboros (Proof of Stake)	Smart contracts, Cryptocurrency	Proof of Stake, Sustainability	ADA (ADA)	Account-based	Yes (Plutus, Marlowe)	Very high (1,000 TPS with Layer-2 Hydra [40])
Multichain	Hybrid	Multi-Peers	Permissioned ledgers, Private blockchains	Customizable, enterprise-focused	Customizable (Tokenizable)	UTXO/Account-based	Yes (via Smart Filters)	Medium (500 - 1,000 TPS)
Tendermint	Hybrid	Tendermint Byzantine Fault Tolerance (BFT)	General purpose, Smart contracts	Fast finality, BFT consensus	Atoms (ATOM)	Account-based	Yes (Cosmos SDK)	High (4,000 - 16,000 TPS [41])
Quorum	Private, permissioned	Majority Voting (Raft)	Enterprise Ethereum, Smart contracts	Privacy, permissioning	Ether (ETH)	Account-based	Yes (Solidity)	Medium-High (200 - 2000 TPS depending on the source [42], [43])
Ripple	Public, permissioned	XRP Ledger Consensus Protocol	Cross-border payments, Financial transactions	Fast and low-cost transactions	XRP (XRP)	UTXO/Account-based	Yes (Rippled)	High (1,500 - 3,400 TPS) [44]
Swirlds	Hybrid	Hashgraph	Distributed ledger technology	High throughput, fairness	None (Hedera token)	Hashgraph-based	Yes (Solidity)	Very high (10000 TPS [45])
Exonum	Private, permissioned	Byzantine fault tolerance	Oriented towards creating permissioned blockchains	Service-oriented architecture	No	An anchoring service periodically stores a snapshot of the Exonum network to Bitcoin	Yes (Rust and Java)	Very high (7,000 TPS [46])

faster than in a public blockchain and to increase transaction security, is usually delegated to a selected subgroup of nodes. Such a way of operating is usually interesting for industrial companies [116] and financial institutions [117], since different business partners and stakeholders can watch the transactions of the whole system, validate them and decide which of them will be eventually added to the blockchain. For example, one of the most popular solutions for developing federated blockchains is Hyperledger Fabric [118].

Besides the four main types of blockchains according to their user access, different authors have proposed specific variants that are based on such types. One variant consists in building hybrid blockchains, which combine public and private blockchain modules to harness the benefits of both types.

With respect to permissioned and permissionless blockchains, they differ primarily in their access control and governance structures (i.e., what can be done), leading to distinct use cases and capabilities. Besides the type of DLT, a blockchain technology is defined by other key characteristics that determine its functionality and applications. For instance, the consensus mechanism is crucial for ensuring agreement

among distributed nodes on the validity of transactions, with mechanisms like Proof of Work (PoW), Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT) that address various needs for security and efficiency. Regarding the purpose of a blockchain, it can vary widely, from enabling decentralized financial transactions to providing transparent supply chain management or supporting digital currencies. Other essential features include scalability, decentralization, high throughput and robust security, which together contribute to the system overall usability. Moreover, cryptocurrencies play a crucial role in blockchain ecosystems, serving as mediums of exchange, for storing value or as incentive mechanisms within the network.

Regarding the data model of a blockchain, it can be either account-based or UTXO-based. The account-based model, used by blockchains like Ethereum, tracks account balances directly. Each account has a unique address and associated balance, updated with each transaction. The UTXO (Unspent Transaction Output) model, employed by Bitcoin, treats each transaction output as an individual entity. Instead of tracking balances directly, it keeps track of unspent transaction outputs, consuming existing UTXOs and creating new ones with each transaction. This approach enhances privacy and scalability, as transactions can be verified independently without knowing the entire balance of an address.

Blockchain technologies are usually associated with smart contracts, which were first proposed by Nick Szabo in the early 90s. Nonetheless, it was not until the creation of the blockchain that smart contracts took off. Such contracts can be defined as self-enforcing and self-executing programs stored on a blockchain that can perform sophisticated tasks without intermediaries. The inner workings of smart contracts are out of the scope of this article, but the interested reader can find useful information in [71], [72]. In addition, it is worth mentioning the research efforts that have been devoted to unknown threat detection methods of smart contracts [73], as well as to their security, from the perspective of the software lifecycle [74], by using AI for privacy protection [75] or source code obfuscation [76]. Furthermore, systematic reviews on different topics related to smart contracts can be found in [71] and [77].

Among the characteristics compared in Table 3, it is worth pointing out that the transactions per second (TPS) is the most common metric to understand how some design aspects (e.g., cryptographic algorithms, block size, consensus mechanisms, block time, network architecture (sharding, L2 solutions)) impact transaction speed. An interactive dashboard that compares the TPS of the most popular DLTs can be found in [25]. However, despite its prevalence, TPS has its limitations [26] and blockchain industry leaders argue that transaction bundling complicates the benchmark. In fact, TPS can be adjusted, changing the consensus protocol [27], leading to discrepancies between theoretical and actual performance. In summary, while TPS remains a widely used and valuable benchmark, it is essential to consider other factors (e.g., latency, security, scalability) when evaluating blockchain performance. In addition, there is a lack of a standard framework to assess the scalability and performance of DLT platforms, making such exhaustive evaluations a complex development.

III. BLOCKCHAIN FOR INDUSTRY 5.0 ENVIRONMENTS

Blockchain systems have proven in the past that they can provide many benefits to different fields, especially in industrial scenarios. This is analyzed in the next subsections, which focus on the revision of the state of the art on the application of blockchain to industrial applications, indicating the main benefits and challenges that will be faced when implementing Industry 5.0 applications. Specifically, the last subsection of this section enumerates the design factors that impact Industry 5.0 application development.

A. PREVIOUS REVIEWS ON THE USE OF BLOCKCHAIN FOR DEVELOPING INDUSTRIAL APPLICATIONS

Despite being initially focused on acting as a ledger that stores financial transactions, blockchain can be applied to many fields [78], [79], [80], including those related to Industry 5.0.

There is currently not much information on blockchain-based Industry 5.0 applications [47], but in the last few years, several authors have analyzed how to apply blockchain to fields related to industrial applications. Existing works focus on exploring the state-of-the-art of blockchain in different industrial verticals. An extensive survey on the integration of blockchain in Industry 5.0 verticals is presented in [47]. However, such an article does not devote effort to reviewing the three main pillars: human-centricity, resilience and sustainability. The aforementioned article presents applications based on a descriptive survey methodology and research questions, and propose a taxonomy of blockchain applications in Industry 5.0 verticals (e.g., smart cities, healthcare, cloud computing, smart agriculture, digital data management).

For example, the use of blockchain and smart contracts in IoT systems is analyzed in [81], [82], and [83]. Previous literature is also focused on tackling certain aspects of IIoT deployments, (i.e., the interconnection of industrial devices with computer-based systems and software through Internet allowing for data collection, exchange and analysis). For instance, in [84] the authors propose the use of blockchain to control IIoT data gathering and dissemination. In particular, data exchange is used to prevent the forging of device or sensor information. In [85] the authors propose a blockchain-enabled architecture for IIoT that considers the generation of a unique digital identity, anonymous access identification and trusted resource provisioning. Other authors studied how to make use of blockchains together with different technologies that can be applied to a smart Industry 5.0 factory [86], [87], [88] or to certain industrial sectors, like the automotive [89], manufacturing [90], [91], [92], oil and gas [93], [94], electricity [95], [96] or the health industry [97], [98], [99], [100], [101].

The literature also includes systematic reviews on the topics that the articles about blockchain have dealt with [102], [103]. Other authors conducted a systematic analysis on the literature on engineering and manufacturing activities to investigate the use of blockchain to ensure data validity, to improve inter- and intra-organizational communications and to increase the efficiency of manufacturing processes [104]. A similar work is presented in [105], but concerning supply chain management.

Also, an initiative to develop an EU strategy on blockchain has been set by the European Commission and the European Blockchain Partnership. This public-driven blockchain initiative, the European Blockchain Services Infrastructure (EBSI) [106], intends to develop a blockchain infrastructure that takes advantage of the tamper-proof, immutable and decentralized properties of blockchain to support better public services in Europe. EBSI's architecture is composed of three main elements: (1) Application Programming Interfaces (APIs), exposed to the public, that allow third-party applications to connect (each API has a specific function, associated with one or several use cases); (2) Smart Contracts, which perform the relevant operations and record transactions on the ledger; (3) EBSI's ledger, a decentralized database that keeps a record of all transactions written on it and that can be accessed by actors looking to complete a business process. Early adopters of EBSI have already tested different pilots in real-life environments. Several frameworks have been developed on the EBSI's ledger to solve business problems that may be relevant to multiple industries/domains (e.g., ''Track & Trace'' for traceability or ''verifiable credentials'' for verification). One of such solutions is aimed at verifying education credentials on a cross-border use case between Belgium and Italy [107]. The goal is that, as EBSI comes online, it will contribute to more efficient and accessible cross-border government services in Europe. In the future, all public services that can benefit from blockchain technology will use this pan-European public infrastructure to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, to the benefit of citizens, public services and companies.

B. MAIN BENEFITS OF USING BLOCKCHAIN WITH INDUSTRY 5.0 TECHNOLOGIES

Industry 5.0 can benefit from using blockchain due to its inherent nature: modern industries have built production chains that involve multiple entities (e.g., suppliers, service providers, end clients, industrial workers, or Internet-connected machinery) that need to interact with each other in a trustworthy way.

To achieve such a purpose, blockchain can help Industry 5.0 factories by providing human-centricity to the production processes. This is because an Industry 5.0 company needs to connect humans among them and with factory-deployed machines. Blockchain allows for integrating all of them, thus creating vertical connections between entities that participate in the production value chain. As a consequence, the automation of such connections enables the optimization of company data exchanges throughout the value chain. Therefore, a direct, traceable and trusted communications channel is established among designers, developers or plant workers.

In addition, blockchain technologies allow for connecting entities that collaborate horizontally, as it occurs during manufacturing, when suppliers, manufacturers and clients exchange information and requests. To be efficient, such communications need to make use of flexible and fast networks, which can be implemented through smart contracts. Thus, smart contracts can act as a horizontal integration mechanism that allows for carrying out payments or information exchanges.

Blockchain technologies can even be integrated into event-driven architectures, which can already be found in factory plants, such as Unified Namespace (UNS). A UNS architecture is based on a software component or repository, which collects all the data obtained from factory-deployed machines, such as sensors, IIoT devices and other components, giving them context [108]. A typical UNS system comprises a data repository, where all the data are stored, an API that enables any authorized software application and system to access the data, and a set of agents, which are a combination of software and hardware systems used to collect and transform the data from the network components and deliver them to the UNS in a standard and contextualized form. UNS typically records and presents only the current state of every entity/device. To access the historical time series data, another component is needed. In a typical UNS system, such as a Hub-and-spoke network, the data repository is centralized, and for the historical data, a data lake is required. UNS's typically centralized repository may be substituted by a decentralized technology, such as the blockchain. Blockchain can be used as a distributed database for gathering the data collected from sensors and other devices, ensuring also reliable historical data. If performance can be an issue, blockchain can still be used as a secure data reliability validator for both the current state and the historical data, stored elsewhere, by storing the hash codes of the data records gathered from sensors and other entities.

Blockchain technologies also help sustainability by reducing the inefficiencies that arise when integrating the multiple technologies required by the Industry 4.0 and 5.0 paradigms. Thus, a blockchain can act as a data exchange hub that is accessed by different entities that only have to implement the functionality required to act as a blockchain client. Therefore, each hardware device or software component does not need to implement specific connectors to communicate with every entity.

Finally, it is worth noting that blockchain can help to improve the resilience of the value chain by allowing the integration of the design, engineering, manufacturing, selling or maintenance stages. Such an integration enables analysis and detection of production bottlenecks and, therefore, weak

links that may become critical for the value chain. Moreover, the rapid response of the involved entities and the acceleration of the bureaucratic processes required by the value chain can be enhanced and automated through smart contracts.

C. INDUSTRY 5.0 CHALLENGES TO BE FACED WITH BLOCKCHAIN

Once it is decided that blockchain is an appropriate technology for implementing an Industry 5.0 application, a developer should be aware of the main challenges that will be faced when deploying it in a real environment:

- Data and application decentralization. Traditional cloud-centric approaches rely on centralized servers that involve several problems:
  - Server deployment and maintenance is usually expensive [109], [110].
  - Centralized approaches usually collect and manage information from a specific server or server farm, thus easing data gathering and Denial of Service (DoS) attacks from cybercriminals.
  - Centralized servers can be difficult and expensive to scale when having to deal with medium to high computational loads.
  - Many industrial companies outsource IT services, so they have to pay middlemen for their cloud-based services. In certain cases (e.g., for industrial companies that manage critical assets), outsourcing is not possible when the remote servers are located in foreign countries due to national security policies.
- Many Industry 5.0 systems need to be updated periodically due to security patches or software enhancements. This updating process is usually straightforward for network-connected computers. Still, OT updates (e.g., IIoT devices, SCADA or more traditional Programmable Logic Controllers (PLCs)) are required to carry out such a process manually and involve many devices that are scattered throughout large areas of an industrial plant. In addition, due to the critical nature of the environments in which these systems operate and some type of devices (e.g., certain PLCs), some companies are transitioning to offline updating methods to minimize potential disruptions. Thus, the future Industry 5.0 factory needs to automate such inefficient processes and to deliver online software/firmware updates to as many IIoT devices as possible in a secure manner.
- Collected data authenticity is essential for every industry, especially when dealing with transactions that involve external suppliers, service providers, and public institutions that may audit certain aspects of an industrial plant. Therefore, it is necessary to make use of technology that can provide accountability and trust. However, it is worth noting that, since middle-men removal requires trust in the collected data [111], new security measures should be taken, especially at a hardware level [112].
- Certain data and transactions with third parties should be secured since the competitiveness of many industries relies on the privacy of such information. Moreover, the data from critical IIoT devices also needs to be protected from unauthorized parties to avoid potential attacks and data leakages [113].
- Close-source solutions can be a source of problems since the way they work is not transparent. As a consequence, open-source software like the vast majority of blockchains is a better alternative to provide trust between parties, although it can also suffer from vulnerabilities and bugs.
- Incorporating a trusted source of external information is critical. For instance, oracles serve as an external component or service that delivers real-world data to a blockchain. They gather, verify and transmit external information to smart contracts. The integrity and reliability of the data supplied by an oracle are vital for the security and proper operation of smart contracts. Oracles can be implemented in a variety of ways, each with its own advantages and disadvantages in terms of security, reliability, and scalability. Typically, a smart contract accesses an oracle through an API provided by the oracle provider. Oracles can be classified based on the origin of the data into software-based or hardware-based. Moreover, they can be categorized as centralized, decentralized or federated.

As a summary, Figure 4 outlines the main benefits and challenges previously described in Sections III-B and III-C.

D. BLOCKCHAIN DESIGN FACTORS THAT IMPACT INDUSTRY 5.0 APPLICATION DEVELOPMENT

1) HUMAN CENTRICITY: USER ACCESS AND PERMISSIONS

Industry 5.0 applications can make use of different types of blockchains, depending on how the workers of a company (or set of companies) perform transactions and how data are shared among them [82]. Moreover, different factors need to be considered due to their impact on the core of an Industry 5.0 application. Specifically, such factors impact human-centric Industry 5.0 applications, since they affect how users access the blockchain.

For example, in [119] the authors propose a resource-trading system that makes use of a consortium blockchain to build a decentralized auction platform and a public blockchain for cryptocurrency payments. A similar approach is presented in [121] for implementing a blockchain-based pharmaceutical supply chain. Another interesting example is the use of blockchain technology for implementing a COVID-19 vaccination certificate management system [120].

Once an entity has access to the blockchain, its actions are restricted according to a permission policy. Thus, there are permissionless blockchains where every user has the same permissions, so additional management is not necessary. This

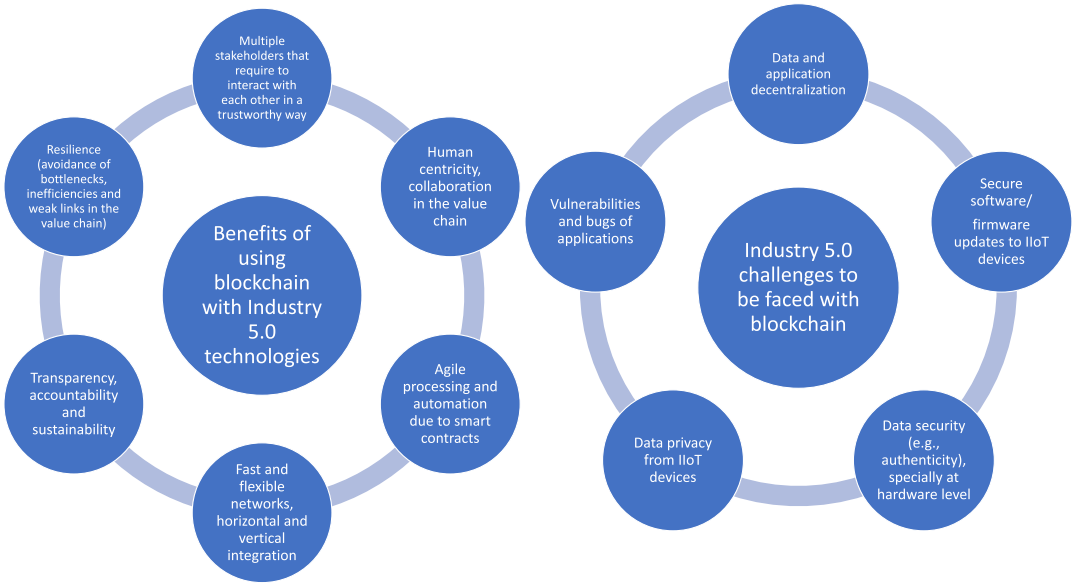

FIGURE 4. Main benefits of using blockchain with Industry 5.0 technologies and Industry 5.0 challenges to be faced with blockchain.

is the case of public blockchains like Ethereum, Bitcoin, Monero [122] or Litecoin [123]. In contrast, there are permissioned blockchains, which can set limits on the actions that a user can perform. For instance, blockchains like Multichain [124] can implement permission policies.

2) SUSTAINABILITY

The development of sustainable Industry 5.0 applications is directly associated with their integration efficiency, which should allow for fast and secure interactions among the different industrial stakeholders. Due to this reason, vertical and horizontal integration systems are key.

In the last years, solutions like Manufacturing-Execution System (MES), Product Lifecycle Management (PLM) or Enterprise Resource Planning (ERP) systems have become popular in Industry, but the demands of the Industry 4.0 and 5.0 paradigms go higher: data should not only be shared internally but also with third parties like suppliers, industrial partners, clients, or government agencies. The problem is that such a level of integration and transparency requires expensive developments and a high level of data security. Blockchain can provide a good trade-off between functionality and efficiency and, as a consequence, sustainability.

For instance, blockchain has already been used for integrating the different entities involved in the development of a power supply [125]. Thus, a manufacturer first announces that wants to develop a power supply by publishing it in a blockchain, and then engineers compete among them to earn the established reward. Another example of collaborative development is described in [126], where the authors make use of a blockchain to build a trans-regional, trans-enterprise, and trans-department industrial production service system.

Supply chain inefficiencies have also been addressed by different researchers, since such an area requires keeping track of ownership and of the performed transactions in a transparent way. For instance, in [90], a blockchain-based solution for keeping traceability of the supply chain of a company in the composite material industry was evaluated. Similar concerns about supply chains are presented in [127]. The authors focused their attention on manufacturing in the fashion industry, which is currently undergoing significant changes to create a sustainable fashion supply chain. Specifically, they devote efforts to supply chain optimization (e.g., minimizing overproduction and surplus stock) and manufacturing with environmentally friendly materials. Note that the fashion industry accounts for about 10% of global carbon emissions and is the second-largest consumer of the world's water supply [128]. Thus, the work analyzes the use of blockchain to determine the impact of information asymmetry and information disclosure. For instance, due to the limited traceability information, consumers may be concerned about the trustworthiness of a product's eco-label, so blockchain-based solutions can enhance consumers' overall willingness to pay for sustainable fashion products.

Concerning energy efficiency, different aspects should be considered by Industry 5.0 developers:

- Technologies like ICPSs need to address the limitations of IIoT devices in terms of energy efficiency: since ICPSs often collect information and interact with IIoT devices that rely on batteries, it is necessary to conduct further research on how to adapt blockchain (e.g., communications protocols, consensus mechanisms) to such resource-constraint devices. These issues are even more critical when the selected IIoT architecture depends on blockchain [82], since their protocols and

inner workings tend to be power hungry. Such issues are essentially related to three typical blockchain features:

- Consensus and mining. This feature has traditionally involved a relatively high amount of computing to validate transactions, so blockchains like Bitcoin are said to consume a massive amount of energy [129]. Such a high energy consumption is essentially due to the used consensus algorithm (Proof-of-Work (PoW) in the case of Bitcoin), which has gone greener in the last few years. For example, Proof-of-Space (PoS) (also known as Proof-of-Capacity (PoC)) was proposed as a green alternative to PoW by basing the consensus not on performing a computational task, but on allocating a certain amount of memory or disk [130]. There are other consensus mechanisms aimed at reducing PoW energy consumption, like Proof-of-Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT). Excellent compilations of consensus mechanisms that future researchers will have to analyze in terms of energy consumption can be found in [131] and [132].
- P2P communications. This kind of communication usually needs nodes to be powered continuously, so energy consumption is usually high [133], [134], [135]. Nonetheless, recent developments have derived into greener P2P protocols [136], [137], [138], which still require being further optimized for blockchain-based architectures and IIoT device hardware [139]. For instance, a wireless power transfer solution for green IoT is presented in [140], where the authors make use of a blockchain to defend against energy attacks from malicious devices. It is worth noting that, in blockchain architecture, most P2P communications are related to updating nodes on the state of the blockchain, so the higher the number of updates, the higher the energy consumption of the system. To tackle such an issue and reduce the number of blockchain updates, researchers have proposed alternatives in the past that may fit into different energy-efficient architectures, like mini-blockchains [141], which only store the latest transactions, thus lowering memory and computational requirements to operate.
- Security. Blockchains make use of high-security mechanisms to protect communications and data integrity. Thus, asymmetric cryptosystems, digital signatures, and hashing algorithms are commonly employed and are continuously evolving [142]. The energy consumption of many of such algorithms has been previously analyzed [143], [144], but further research is needed to develop energy-efficient blockchain-based solutions.

- New computing paradigms can be more energy efficient. Traditional Cloud Computing-based systems have proven to be useful and enable multiple stakeholders to collaborate remotely, but their energy efficiency is not always optimal for Industry 5.0 scenarios. There are other architectures, like the ones based on Edge or Mist Computing that, in certain scenarios, can be more appropriate in terms of energy consumption [146], [147]. For such architectures, blockchain can be a good complement to decentralize transaction storage and provide trustworthiness and transparency.
- Blockchain energy efficiency. Despite the multiple benefits of blockchain, the use of inefficient consensus mechanisms results in significant energy consumption [129], so it is necessary to adapt the different parameters of the selected blockchain to optimize energy consumption.
- Energy efficiency of supply chain logistics. Supply chain traceability can be accomplished through blockchain, so the used materials can be tracked throughout the value chain, and therefore their use can be optimized in conjunction with the involved logistics. For instance, blockchain-based applications have already been proposed for optimizing the COVID-19 medical equipment supply chain [148] or for the agriculture and food supply chain [149]. Moreover, it is worth indicating that future sustainable logistics may involve creating a network of distributed additive manufacturing workshops, which would avoid the shipment of goods over long distances (thus decreasing energy waste on transportation). In such a scenario, sellers would send digital files to the 3D printing workshop that is closest to the buyer to minimize the transportation impact on the environment. For instance, several authors have proposed the use of blockchain for minimizing part delivery time and improving stock management for 3D printing manufacturers [150], [151], [152]. Some companies are already implementing Just-in-Time models for 3D printing with the help of blockchain [153] and some manufacturers have also proposed to distribute additive manufacturing orders in industries as complex as defense [154]. Moreover, blockchain can also help to track and to integrate 3D printing files to avoid manufacturing mistakes, to provide trustworthiness [155], [156], and to protect and to manage intellectual property [157].

3) RESILIENCE: INCENTIVES AND ACTION AUTOMATION

Blockchain access and permissions not only condition the human-centricity of an application, but also influence industrial resilience due to their impact on security. Moreover, two other factors can help to enhance the robustness of an Industry 5.0 value chain:

- Incentives: they are essential to keep a blockchain-based solution 'alive', since they motivate the different stakeholders to carry out their tasks. Such incentives are usually set as rewards given in the form of virtual tokens. Thus, there exist tokenized and non-tokenized blockchains. The former reward actions, like transaction

processing with cryptocurrencies (this is the case of Bitcoin with bitcoins or Ethereum with Ether). The latter blockchains do not rely on specific tokens, as occurs with Hyperledger Fabric.

- Process automation: it increases resilience by enabling to react quickly to events that impact the value chain. To implement such automation mechanisms, logic-oriented blockchains provide the ability to run code, usually in the form of smart contracts, but they can also execute other applications. For instance, Ethereum, Hyperledger Fabric, NXT [158], and Counterparty [159] can be considered logic-oriented blockchains. Some blockchains are not aimed at the execution of logic but at performing transactions, like in the case of Bitcoin, Monero or Ripple.

The concept of smart contracts is especially important for relieving industrial workers from tedious tasks and improving resilience by carrying out fast and automated responses to events that impact the value chain. A smart contract can be regarded as a computer program that encodes agreements established by the involved parties and that are executed when certain conditions are met. Thus, the traditional legal terms of a contract are coded to manage virtual or real assets.

To determine when the conditions of a smart contract are met, it is often necessary to check external information sources that are called oracles. For instance, an oracle can be a service that indicates when a warehouse inventory of a specific item is running low to trigger the execution of a smart contract responsible for purchasing more stock. There are three main types of oracles that can be useful in an Industry 5.0 factory: software oracles (they extract data from online sources like websites or intranet information repositories), hardware oracles (they obtain data from physical sources like sensors or industrial machinery), and consensus-based oracles (they fuse the information received from multiple oracles to decide how the system should respond to an event). Moreover, oracles can be classified into two types: inbound oracles (they can push information from external sources (independent of the blockchain) into the blockchain) and outbound oracles (they allow smart contracts to send data to external parties that do not interact directly with the blockchain). A detailed description of the types of oracles and how they work can be found in [160].

Figure 5 summarizes the most relevant blockchain design factors that impact Industry 5.0 application development previously described in Sections III-D1, III-D2 and III-D3.

IV. BLOCKCHAIN-BASED INDUSTRY 5.0 APPLICATIONS

In this section, the intersection of blockchain technology and Industry 5.0 will be analyzed by exploring the various ways in which blockchain can transform industry.

A. BLOCKCHAIN-BASED HUMAN-CENTRIC APPLICATIONS

The concept of blockchain-based human-centric applications aims to empower individuals, protect their privacy and provide them with greater control over their data and interactions. This subsection analyzes blockchain technology's potential to reshape traceability in application domains such as logistics, manufacturing and other human-related activities, highlighting its ability to foster collaboration, transparency and inclusivity in the digital age.

1) WORKER PERSONAL DEVELOPMENT TRACKING

The Industry 5.0 paradigm considers workers as 'investments' rather than as a 'cost', so companies should foster industrial operator personal development. Thus, skill tracking and progress can be tracked through blockchain-based applications [161], which can also be gamified and incentivized through rewards or social recognition [162]. Similarly, the worker's well-being can be monitored and tracked to take the necessary mitigation measures [163].

The case of operator training is of special interest since the demand for new skills has increased rapidly in the last few years. In this aspect, technologies can help by improving their User Experience (UX) so that operators do not need specific skills to use them. For instance, AR and Mixed Reality (MR) can show virtual objects in a real-world environment, thus providing a level of immersion that cannot be achieved with other mobile device technologies like smartphones or tablets [164]. Virtual Reality (VR) is also frequently used for training [165], but it immerses trainees completely in a virtual world, so it is not appropriate in scenarios where they have to interact with real objects and specific virtual entities.

AR, MR and VR have been evaluated in the past years and showed that they can increase assembly line operator productivity [166], to improve different industrial processes (from design [167], [168] to manufacturing [12], [13], [169], [170]) or maintenance [171], [172]. Blockchain can benefit such applications by:

- Easing content sharing and access. To provide a smooth visual experience, most AR/MR/VR content is downloaded and stored locally before use. However, since in an industrial scenario part of the content changes dynamically (e.g., CAD designs are polished, design errors are fixed) and due to the memory limitations of the majority of AR/MR/VR devices, there is a need for using remote servers for storing content. In such scenarios, blockchain can help to securely share the exchanged content (e.g., to prevent downloading fake content [173] and to trace its use, especially for classified data or for content whose intellectual property is protected [174]).
- Content availability. AR/MR/VR content servers may become overloaded when multiple users request large files simultaneously. Blockchain can prevent this issue by easing server decentralization. For example, some companies offer distributed Graphical Processing Unit (GPU) rendering based on a blockchain [175]. Moreover, developers can also benefit from the availability of online marketplaces that ease content acquisition and download through blockchain-based ecosystems like Decentraland [176] or VIBEHub [177]. Furthermore,

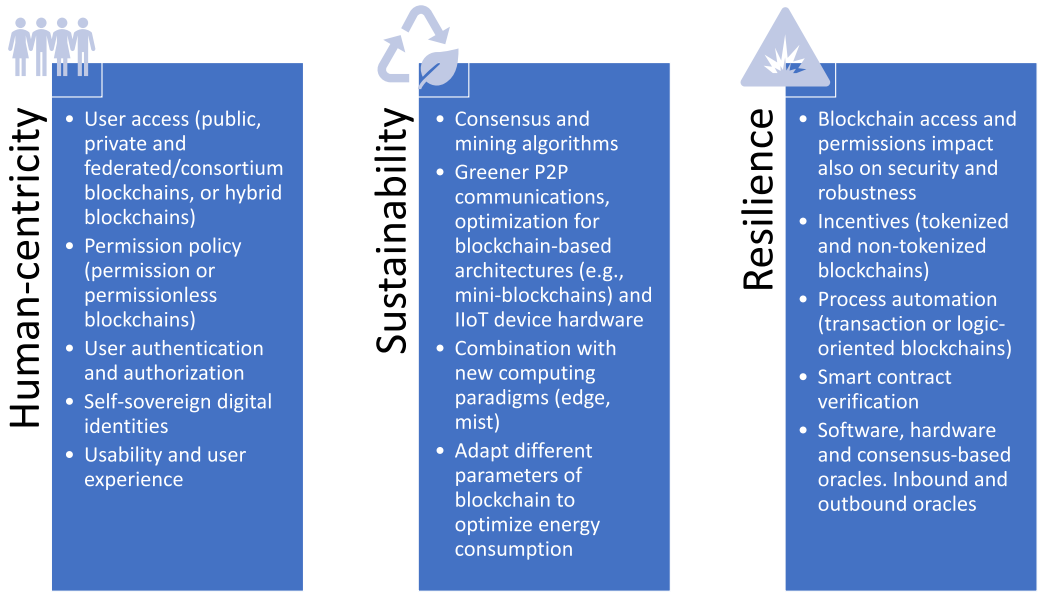

FIGURE 5. Blockchain design factors that impact Industry 5.0 application development.

industrial AR/MR/VR solutions may need to perform online payments, which can be carried out by using cryptocurrencies that use the AR/MR/VR devices as hardware wallets [178].

- Enhanced user experience through collaborative environments. Operation, training, and skill learning are often carried out in groups, which also makes the experience more entertaining [164]. Different companies realized that such a collaborative experience can be improved thanks to blockchain technologies, which make digital asset and space sharing easier and more secure [179], [180].

2) DEVELOPING HUMAN-CENTRIC PRODUCTION SYSTEMS

One of the most important guidelines of Industry 5.0 is the fact that technology is used to serve people, not the other way around. As a consequence, the blockchain technologies that are used by the different industrial processes have to be adapted to the needs and diversity of the workers, instead of forcing workers to adapt to them. Thus, ideally, blockchain-based applications should 'hide' the underlying complexity of the used technologies and mechanisms (e.g., consensus mechanisms, reward policies, mining) from the plant operators, so they can focus on their daily tasks rather than on the issues that may arise from the implemented software and the used hardware.

An example of human-centric systems is Industrial Cyber-Physical Systems (ICPS), which automate the collection, processing, storage, and visualization of information and events that enable workers to monitor and control physical processes. The subsystems that compose an ICPS are usually deployed throughout industrial plants, but can connect to other systems on the Internet, thus decentralizing data processing while making decisions fast [181], [182], [183]. Since ICPSs are commonly decentralized, blockchain technologies can be easily adapted to them. That is the reason why several authors have already proposed blockchain-based ICPSs [184], [185], [186], the use of rewards as incentives for the entities that collaborate in such a kind of systems [187] or the coordination of the local manufacturing processes monitored by an ICPS through a blockchain [188]. However, it is important to note that the development of human-centric ICPSs needs to solve two relevant problems. First, it should be noted that many blockchains have low throughput and high latency (mainly due to their transaction processing speed), which prevent ICPSs from responding fast. Second, the number of transactions to be stored by an ICPS may be high, so Industry 5.0 developers will need to devise ways to handle blockchain storage in the memory-constraint devices that interact with the ICPS.

3) CREATING A SAFE WORKPLACE

Unfortunately, accidents are common in industrial environments, especially in certain industries where workers carry out dangerous and strenuous tasks. In such environments, technologies like blockchain can help by automating and monitoring the performed tasks. For example, in [189] the authors present a blockchain-based safety supervision system. They aim to ease the supervision of equipment that may involve potential dangers (e.g., pressure pipelines, lifting machinery). The authors use Hyperledger Fabric to update the supervision information to get responsibility tracing, more transparency and accountability, more efficient data sharing, and the integration of additional functionality such as an analysis engine. However, the authors acknowledge

that additional data standardization and improvements in the design of the processes are still needed.

A broader view of safety is provided by [190]. In such a work, the researchers describe a Safety-as-a-Service (Safe-aaS) infrastructure integrated with a permissioned blockchain to protect the privacy of the information provided by operators, manage the decision parameters requested by the operators, and restrict unauthorized access to sensor data. In addition, the proposed solution facilitates secure user-level agreements and optimizes service-level quality through smart contracts.

The COVID-19 pandemic also imposed limitations on physical distancing to ensure the safety of operators. For instance, in [191] an IoT system is proposed to enable real-time estimations of the occupancy level of public spaces. In addition, certain critical physical and mental health parameters can be quantified through software and wearables to create a safer work environment. For example, in [192] the design, development, and evaluation of a system that provides a near real-time decentralized system for monitoring, reacting and tracing events that affect the safety and health of industrial operators. Such a system collects data from sensors embedded into IoT wearables that measure both personal and environmental key indicators. The collected information is sent to a LoRaWAN gateway, which then transmits it to a pool of nodes where data is stored in a distributed manner. Such a decentralized system allows for providing resilience (e.g., information redundancy and availability, as long as there is an operative node) and uses smart contracts to store and process the collected data.

4) DESIGNING INCLUSIVE INDUSTRIAL WORK ENVIRONMENTS

One of the issues raised by the practical implementation of the Industry 4.0 paradigm is the fact that jobs will be lost due to the use of new technologies. One way to minimize such an impact is to create collaborative approaches, often known as bringing the human-into-the loop. An example is provided in [193], where the authors propose a blockchain-based transportation control tower for fostering collaboration between stakeholders, especially shippers and carriers while eliminating unnecessary intermediaries (e.g., freight brokers) to create a long-term sustainable freight transportation system.

Collaborative approaches are especially important for Industry 5.0 when it comes to AI technologies (e.g., collaborative or federated learning). For instance, in [88] the authors identify three barriers to the adoption of Cognitive Computing for better decision-making in industrial scenarios. The first barrier is low efficiency, due to the massive volume of data generated by industrial devices; the second one is the possibility of data leakage; and the third barrier is the lack of incentives to contribute with data. Moreover, such a work indicates that all three barriers pose significant challenges to the accuracy of the results. As the article points out, blockchain can help with two of these issues: preventing data leakage through a decentralized model with a privacy-preserving mechanism and providing incentives for users to participate in the learning process and get rewards for their knowledge according to their contribution. In addition, the developed approach also provides robustness against poisoning attacks.

The work described in [194] goes one step further by proposing a large-scale blockchain approach to take advantage of collaborative production paradigms like distributed and social manufacturing. Such a framework aims to address current challenges of collaborative production, such as interoperability, resource allocation and tracking, security, supervision and audits, intellectual property protection, marketing and intermediaries, democratic organization, and global value chain governance. To achieve that, the proposed framework is divided into five layers: resource service, network interconnection, market agreement, collaborative management and value interconnection.

Another key aspect is long-life training in the involved technologies. For example, the industry has been increasingly vulnerable to cyber-attacks, so cybersecurity training is a current need for Industry 5.0, especially in the IIoT domain. To engage professionals in cybersecurity and vulnerability assessment, learning through case-based approaches has been proposed [113], [195]. In addition, it is also particularly relevant to also augment competencies in blockchain technology. For instance, in [196] the authors propose a gamified approach that uses an adversarial sandbox adaptive serious game to address potential barriers in the uptake of blockchain.

5) COLLABORATING WITH ROBOTS AND AUTONOMOUS VEHICLES

Robots, exoskeletons, cobots (collaborative robots), UAVs (Unmanned Aerial Vehicles) or AGVs (Autonomous Ground Vehicles) can be really useful for reducing worker task load and safety by performing repetitive and dangerous tasks [197]. For instance, cobots can help humans when performing different tasks in an assembly line [198], [199]; AGVs are useful for searching or carrying items in large warehouses and factories [200], [201], [203]; digital ergonomics can be used to assess and track the operator posture in industrial cyber-physical-human systems [202]; and UAVs can perform tasks like painting [204], transportation [205] or inspections [206].

Blockchain is a good complement to robots and autonomous vehicles since it allows multiple human and non-human entities to interact with them, either through the blockchain or through smart contracts. For instance, UAVs air routes can be coordinated through a blockchain-based solution [207]. Moreover, blockchain-based UAVs can help in tedious item inventory management tasks by embedding Auto-ID technologies, which also reduce the time required to complete the inventory [16]. A different approach is proposed in [208], where the authors present a new business model

for the use of UAVs in the industry. Their work describes a novel architecture that facilitates virtual UAVs-as-a-Service. Thus, the blockchain-based platform enables end-user access to on-demand UAV services without having to own them.

Regarding autonomous vehicles, recent literature has shown that it is possible to provide workers with blockchain-based ride-sharing services [209], [210]. Moreover, typical industrial vehicle tasks like refueling, charging, parking, and repairing can be tracked and automated for both autonomous and semi-autonomous vehicles [211], [212], [213]. Such vehicles and the operators that operate them can be incentivized through a reward system that can be based on the use of blockchain [214], [215].

6) DEVELOPING AI-ENABLED APPLICATIONS

AI can help workers while performing multiple tasks, easing the work of operators or improving their training. Among the different disciplines of AI, Big Data and Data Analytics are two of the most useful in industrial environments. This is because the ideal Industry 5.0 factory will collect enormous amounts of information from multiple sources of the value chain (e.g., plant IIoT nodes, operators, suppliers or service providers), which needs to be processed to extract valuable conclusions. In such cases, blockchain is a good complement for Big Data and Data Analytics during the information collection stage [216], [217], when verifying the trustworthiness of such information [218] or when it is necessary to automate data circulation reliably [86], [219]. This latter aspect refers to the need for authorizations throughout the value chain when data are moved through it, which can be automated by implementing smart contracts.

In addition, it must be noted that blockchain is especially well suited to overcome some of the limitations of implementing different AI techniques (e.g., deep learning [220], federated learning [221], federated transfer learning [222]) in IIoT devices like maintaining privacy, uploading training or updating model tasks. Furthermore, Cognitive Computing, which was previously mentioned in Section IV-A4, is a way to redesign industrial work environments, which can bring substantial benefits to personalized mass production with so-called cognitive manufacturing. For instance, in [224] the authors combine a mining-based cognitive manufacturing process with blockchain to ensure end-to-end traceability. Another recent example is presented by Cotta et al. in [223]. In the work, the authors discuss the convergence of intelligent spaces and Industry 5.0 concepts and present a laboratory replica of a cognitive factory cell.

7) ENSURING WORKER PRIVACY

The improvement in operation well-being envisioned by Industry 5.0 cannot be implemented at the expense of worker privacy. As a consequence, the Industry 5.0 solutions need to be protected against potential cyberattacks [225], [226], [227], [228].

Regarding data communications security, it must be first indicated that the vast majority of blockchain technologies make use of highly secure public-key cryptosystems and hash algorithms [142]. Nonetheless, it must be noted that quantum computing poses a threat to such systems, so post-quantum schemes need to be selected and put in place to avoid quantum attacks [142]. IIoT devices and the solutions that use them (e.g., ICPSs) are especially affected by the implementation of certain cryptosystems due to their computational resource constraints [143], [144].

Concerning blockchain access and permissions, as it was previously described in Section III-D1, private and federated blockchain can decide which users can interact with the blockchain, so this sole measure can decrease the number of attacks significantly. In addition, since the collected data are stored in a distributed fashion, if one of the storing entities is under attack (e.g., under a DoS/DDoS attack), the rest of the blockchain nodes can provide such information, thus guaranteeing data availability.

8) FOSTERING SUPPLY CHAIN AND LOGISTICS TRACEABILITY

Global trade depends on efficient logistics operations. Current logistic handling systems are still typically centralized, offering limited support for collaboration among supply chain stakeholders, and lacking support for traceability of logistics operations [229]. Blockchain-based logistics platforms can, also in this scope, provide transparency, security, and immutability of data exchanged during various operational processes, offering capabilities of traceability and auditability through immutable on-chain trusted transactions, in a decentralized manner without intermediaries or trusted third parties.

The study in [230] shows that blockchain technology can improve multi-organizational businesses such as supply chain and logistics, turning them into secure, agile, trusted and transparent functions. An example in the scope of aircraft spare parts inventory management shows that blockchain can provide traceability and trackability of data to ensure the compliance of airworthiness requirements [231]. The authors conclude that the enhanced blockchain-based inventory management system enables the building of digital twins for aviation.

Another growing logistics problem that may benefit from blockchain use is reverse logistics. According to the Association of Supply Chain Management [232], reverse logistics is the process of returning products from end users to the retailer or manufacturer, through the supply chain, in a reverse direction. The return of goods is the most important activity in Green reverse logistics. To ensure that the goods return to the manufacturer and have a good end-of-life treatment, it is necessary to record all the information of the goods processed from the factory to the customer. For such a purpose, the authors of [233] propose a sustainable development strategy of green reverse logistics based on blockchain.

In the proposed traceability scheme, a Merkel tree is used to implement a license chain to store traceability information, forming a ''double chain'' structure of the commodity traceability system. This double chain structure has a larger throughput than the traditional blockchain and can trace the source of the product to the manufacturer, ensuring that goods can be returned to the manufacturer for further processing, reducing the generation of waste in logistics, and providing a guarantee for promoting the sustainable development of green reverse logistics. In addition, considering the limited resources of Small and Medium-sized enterprises (SMEs), the authors of [234] implemented a blockchain-enabled supplier cooperation network for Industry 5.0.

9) FOSTERING MANUFACTURING TRACEABILITY

Within an industrial facility, shop floor activities make their way toward producing what has been planned to produce. Manufacturing traceability has its advantages, both for improving production management efficiency and for increasing production safety. As an example of the first case, the article in [235] presents the tracking of product components throughout the manufacturing shop floor in the shipbuilding industry. In heavy metallurgical industries, such as automotive, shipbuilding or aerospace, assembly customization and manufacturing in batches of a single unit lead to continuously changing product configurations, therefore generating different historical data unique to each product [236]. Tracking specific product components in such industries enables the identification of the parts of a product or a batch when a defect is detected, streamlining its quick replacement [235]. Additionally, process traceability adds value to the final product, as all traceable information may be transferred to the end customer, who becomes empowered with information on any material, component, part and block of the metalworking final product, as well as all the certificates and documents necessary for any process [235].

Also, in the case of food value chains, manufacturing traceability increases food safety, as any batch of product components can be quickly traced and, in the event of a threat to public health, the products that depend on that batch can quickly be tracked and retrieved [237], [238].

10) FOSTERING CONSUMER-IN-THE-LOOP AND CIRCULAR ECONOMY TRACEABILITY

Circular economy value chains, contrary to traditional linear value chains, require the participation of the final consumer/customer, who is responsible for postponing the end-of-life of any product, as well as delivering it for recovery or recycling when this end-of-life arrives. Of course, making the end customer responsible for the full circularization of the circular economy process is an exaggeration and a mistake, as the main role lies with industries and product brands, which must guarantee maintenance services that allow for extending the lifespan of products in question, as well as guaranteeing the recollection, sorting and recovery/recycling of these products when their end of life arrives. Thus, traceability for the circular economy enables informing the final consumer that their closing-the-loop actions are worth the effort and also eases the tasks of waste sorting and separation while informing the recycling companies about the composition of products being sorted and separated for recycling [239].

11) FOSTERING TRUSTWORTHY KNOWLEDGE

Blockchain-enabled traceability provides benefits to consumers/customers/users in terms of reliable information. An example is the tracking and certification of products with a protected designation of origin, a protected geographic indication or a traditional specialty guaranteed (PDO/PGI/TSG) [240], [241].

Another type of traceability made possible by blockchain is the distributed and decentralized tracing of political contacts, which can be used to detect evidence of corruption and ensure a more transparent way of political action [242]. The traceability of news sources also helps to build a more transparent news communication environment, therefore minimizing counterfeit reality (e.g., fake news, deepfakes) and seeking to guarantee a healthier democratic society [56], [243].

B. BLOCKCHAIN APPLICATIONS FOR SUSTAINABILITY

Given the crucial necessity of adopting sustainable practices for business development, a greater emphasis is being placed on using emerging technologies to address global environmental and social sustainability challenges. Through boosting transparency, traceability and trust, blockchain technology has emerged as a powerful instrument for advancing sustainability across a wide range of enterprises and industries. This subsection looks into blockchain applications as a means to enhance sustainable practices in Industry 5.0-related domains, such as the traceability of sustainability indicators along a value chain, green energy traceability, carbon credits exchange, circular economy and responsible resource management. By enabling immutable and decentralized systems, blockchain has the potential to promote beneficial environmental outcomes, encourage collaboration and enable informed decision-making for a greener and more sustainable industry.

1) FOSTERING VALUE CHAIN ENVIRONMENTAL AND SOCIAL TRACEABILITY

Industrial value chains are typically horizontal chains or networks that involve several cooperating companies. Some of these companies produce raw materials, others produce product designs for manufacturing, others manufacture products according to designs produced by third parties and purchase raw materials from suppliers, and others carry out a combination of these and other activities towards producing intermediate products or components and final products. Along these potentially global value chains, companies have different ways of expressing their respect for the

environment, equity and social well-being. The traceability of social and environmental aspects of every activity along the entire value chain allows any involved organization to be aware of the environmental impact of a product batch produced by a potential supplier [244]. It also allows for knowing the environmental impact of batches of raw materials or components used by that producer to produce that product's batch. Moreover, it allows for assessing the aggregate environmental impact of the company's batch of products produced from those batches of raw materials and intermediate products. This is also true for social indicators of how companies treat their employees.

These types of traceability platforms must cross all value chain business partners with maximum transparency and without trust issues [245], [246].

2) FOSTERING CIRCULAR ECONOMY

A value chain consists of a sequence of activities that build intermediate products/components, or final products, adding value to these products, up to an end client. Traditional value chains are bound to a linear economic model take-make-use-dispose (gathering/extraction of raw materials - product production - product use - waste) [239].

A circular economy model requires the implementation of activities in the value chain to extend the useful lifespan of products, such as maintenance services, in addition to product recovery/recycling activities, which allow for obtaining recycled raw materials that can re-enter the value chain, completing the cycle. In this context, a traceability platform can help by providing information about the material constitution of products, facilitating their future recycling.

The closing of the cycle in a circular economy model also demands greater involvement from the end client. Platforms are needed for engaging clients into buying products with less social and environmental impact, using their products for a longer time, maintaining and recovering their products, measuring their own activities' environmental impact, and delivering them for recycling when the time comes. These platforms may use gamification features to better engage clients and may also be based on a blockchain [247].

Another example can be seen in [248], where the authors present a review on adopting blockchain and IoT technologies to foster a circular economy in the Electric and Electronic Equipment (EEE) value chain. This involves recovering and reintegrating components, which leads to more sustainable practices and less environmental impact.

3) FOSTERING CARBON CREDITS EXCHANGE

Climate change poses one of the most significant challenges of our time, with an urgent need for reducing greenhouse gas emissions, which has brought global attention to carbon offset mechanisms [249]. Carbon credits, a key tool in the fight against climate change, have gained attention as a market-based approach to promote emission reductions and sustainable practices [250]. Traditional carbon credit systems, however, often face issues of transparency, accountability, and operational efficiency [251].

Blockchain holds the potential to transform the carbon credits market, facilitating a fair, efficient and secure exchange of carbon offsets [252].

Huckle et al. [253] explore IoT and blockchain in the context of shared economy scenarios. While not directly focused on carbon credits, the paper lays the groundwork for understanding how blockchain could be integrated into various sectors, including carbon trading. The use of blockchain for carbon credit exchange has been addressed by Patel et al. [254] by improving transparency and efficiency in carbon credit transactions. Kim and Huh in [255] introduce the concept of a blockchain-based carbon trading platform to support the United Nations Sustainable Development Goals (SDGs) while leveraging blockchain capabilities to promote sustainable practices through carbon credit trading among users. With a lot of characteristics in common, two studies [256], [257] explore carbon emission monitoring and credit trading systems using blockchain, emphasizing the potential of creating a more accurate and accountable carbon credit marketplace. Moreover, such papers discuss the benefits and challenges associated with the integration of blockchain into existing carbon credit infrastructures. Another interesting perspective is presented in [258], where a specific carbon-trading model for urban public transport based on blockchain is presented.

4) FOSTERING GREEN ENERGY TRACEABILITY

The energy sector is largely responsible for the production of greenhouse gases. Increased consumer awareness about greenhouse gas emissions from energy production has increased interest in the consumption of greener and less polluting energy. This greater awareness, combined with the definition, by several European governments, of 100% renewable energy targets by 2030 [259], makes it imperative to increase transparency regarding the origin of the electrical energy that each one consumes. There are power generation plants from renewable sources (e.g., hydroelectric, wind, and photovoltaic) and non-renewable sources (e.g., natural gas, fuel oil, coal, and nuclear), and a consumer who wants to consume only renewable energy and therefore pays a tariff that allegedly guarantees the supply of renewable sources need to be sure that the consumed energy comes from renewable sources. Efforts to establish this link between the energy produced and its use, seeking to create a link between energy production and consumption, have been carried out, and these are typically based on the creation of a Renewable Energy Certificate (REC), which is an Energy Attribute Certificate (EAC) for energy from renewable sources, which certificates the origin of energy, and is then delivered to the consumer or the energy distribution company [260] and can be used for energy traceability purposes.

These efforts to certify the production and consumption of renewable energy have some problems, such as that it

is possible for consumers to buy certificates for energy produced in a network other than their own or to buy photovoltaic solar energy certificates and consume that amount of energy during the night.

The reduction of the certified period from annual to hourly, or even shorter periods, makes it possible to match the production of renewable energy with its actual consumption, promoting the effective elimination of CO2 production instead of a mere exchange of carbon credits [261], [262]. These certificates may be blockchain-based. In [263], Andoni et al., present a systematic review of the opportunities, challenges and limitations of using blockchain for peer-to-peer (P2P) energy trading or its use in decentralized markets, electric vehicle charging and other use cases. The authors conclude that blockchain can benefit energy markets and consumers by offering disintermediation, transparency and tamper-proof transactions, and by empowering consumers and small renewable generators to have a more active role in the energy market.

5) FOSTERING RESPONSIBLE RESOURCE MANAGEMENT

Industrial resource management deals with planning and allocating physical resources, such as materials, technology and people, to a production process or project. The availability of resources when they are needed is of utmost importance for increasing productivity and leveraging the value of the organization. Blockchain can be an enabler of improved resource management. For instance, in [264] a blockchain-based digital twin-sharing platform is proposed as a solution to enable the sharing and protection of digital twins of resources in a decentralized and distributed environment. In this case, the resources are Socialized Manufacturing Resources (SMRs) and the information related to copyright and usage or sharing conditions for using and integrating SMR resources in a Universal Plug-and-Play (UPnP) network. The massive demands for specialized manufacturing services have given rise to SMRs. These resources may be clustered as a community to provide specialized manufacturing services for producers/consumers, established via social media and decentralized platforms. Communities of SMRs are formed as dynamic, autonomous systems to co-create mass-individualized products and services. These decentralized SMRs need to be organized and managed in a distributed, collaborative manner [265].

In [266] the authors propose a blockchain-based cross-domain authorization platform that enables a distributed and transparent User-Managed Access (UMA) to citizen's data for smart city operation and optimization. In conventional UMA systems, authorization mechanisms are centralized and resource owners centrally manage access rights for different resources in different domains. This raises transparency problems in the authorization mechanism and the architecture proposed aims to solve such issues by basing the authorization mechanism on blockchain.

Finally, in [267] the authors present a study on the use of blockchain for managing human resources, where employees could share sensitive information with their managers or during a hiring process through blockchain. Qualifications, achievements or recommendations could be easily validated.

C. BLOCKCHAIN-BASED RESILIENT APPLICATIONS

Resilience is critical for organizations in an increasingly interconnected and ever-changing digital economy. Blockchain has emerged as a possible option for improving resilience in systems, processes and applications by increasing its trust, security and adaptability. This subsection investigates the concept of resilient blockchain applications, focusing on their capacity to resist interruptions, to retain data integrity and to allow for decentralized decision-making. Thus, it is investigated the potential of blockchain to improve resilience in supply chain management, calamity response (e.g., COVID-19 pandemic, supply chain disruption) and cybersecurity. Thus, the adoption of blockchain can provide a solid mechanism for tackling complex difficulties in an ever-changing environment.

1) SUPPLY CHAIN MANAGEMENT

Increasing resilience and helping to prevent fraudulent activities and data tampering is another reason why companies are turning to blockchain. In [268] a literature review on the advancements made in using blockchain for developing a cyber-secure and resilient supply chain is presented.

The COVID-19 pandemic has also impacted business environments around the world. Supply chains, especially those that cross multiple countries, have suffered multiple disruptions [269]. Many of these disruptive events (e.g., shortages of personal protective equipment, empty shelves in supermarkets) were related to supply chain management, especially regarding single-sourcing strategies, the lack of adequate risk management, delivery failures by suppliers and lack of transparency and visibility [270].

In [271], after analyzing COVID-19 disruptions, the authors propose that resilient supply chains should consider a strategy driven by disruptive technologies. The authors concluded that embracing disruptive technologies, particularly those rooted in data, information and knowledge (such as cloud computing, big data analytics, artificial intelligence or blockchain), is vital for enabling the manipulation of data, facilitating the generation and utilization of information and knowledge and fostering self-executed and controlled supply chain processes through cyber-physical technologies like IoT, robotics, additive manufacturing and augmented reality. The authors emphasize the importance of interoperability among these technologies to drive enhancements in key performance attributes such as efficiency, responsiveness, flexibility, reliability, transparency, visibility and traceability.

2) FOSTERING VALUE CHAIN RESILIENCE

The factories that have already implemented the Industry 4.0 paradigm can be considered competitive, but they compete in a global economy and are exposed to rapid

geopolitical changes. As a consequence, an Industry 4.0 smart factory can be efficient and produce goods at a reduced cost, but it is vulnerable to disruptions in its value chains. The value chain problems that arose due to the COVID-19 pandemic and the Russia-Ukraine war highlighted the mentioned problems and forced companies to analyze how to address the detected vulnerabilities.

To tackle the previous issues, blockchain could be used, since it is a technology characterized by its robustness and resilience in relation to data collection and automatic transactions. Thus, information disruptions can be prevented in cases where there are technical problems or cyberattacks. To prevent them and thus monitor the state of the value chain, transparent and tamper-proof traceability is essential, so that its data can be trusted by the involved parties. Such traceability can be kept by making use of blockchain, as different authors have already demonstrated. For instance, in [272] originChain is presented: a blockchain that uses smart contracts to maintain traceability in industrial settings. Such a work examines the main current disadvantages of deploying a blockchain-based traceability system for an industrial company, including high integration costs and large amounts of time required to understand business processes and to implement smart contracts, which must be defined precisely due to the consequences of their malfunction. However, once the blockchain-based traceability system is working, a company benefits from having a trustworthy transaction log on the product value chain events. It is possible to identify every product unambiguously to avoid counterfeiting and to demonstrate ownership. Tendering can be automated through smart contracts, and responsible consumption can be promoted by providing the whole manufacturing trace [273].

To keep traceability of the products and manufacturing processes, IIoT sensors and nodes are essential. Such nodes adapt traditional IoT developments [274], [275], [276], [277], [278] to Industry 5.0 requirements, so sensors, actuators and machines can embed remote control and management capabilities [279], [280], [281], [282] to create context-aware scenarios [283]. Due to such a dependency, IIoT systems need to be robust against cyberattacks that may disrupt the value chain.

Blockchain is a technology able to provide IIoT with decentralized and secure transactions through a common ledger [284]. Thus, a blockchain can guarantee that the shared information is not forged or has been altered; external access can be given to the collected data for the sake of transparency; and, at the same time, it provides a mechanism that allows multiple entities to communicate in an automatic or non-automatic way [81]. Thanks to the previous benefits, different authors have proposed practical applications for fields like energy trading, which can use blockchain-based sensors to carry out fair payments [285]. An example of a blockchain-based energy trading system is described in [286], where the authors propose a distributed management approach to energy trading in which IoT devices participate autonomously in energy markets, with the key advantages of resilience and availability. Such work also draws attention to a novel type of attack that can be used to delay, change, or discard trading bids. Such attacks do not target the trading system, but the gateways that connect market participants to the system. Thus, the article analyzes the potential impact of such attacks by introducing mitigation techniques.

Value chain resilience can be tested through simulation software. Such software models the behavior of the stakeholders and entities involved in the different processes and estimates the current and future state of a product value chain. Thus, simulation and predictive analytics software can anticipate future problems and determine potential mitigation measures. Moreover, simulation software can be complemented by a Digital Twin [287], which enables visualizing in an integrated and user-friendly way relevant parameters of the entities involved in the value chain.

Blockchain technologies can help simulation software in different aspects:

- Data collection. Blockchain enables the collection of information from diverse sources in a homogeneous and distributed way, thus easing integration and improving data availability and sharing.
- Data authenticity. Blockchain includes mechanisms to provide trustworthy information, which is essential for obtaining accurate simulation software predictions.
- Data processing task distribution. The use of blockchain technologies enables to distribute computational tasks among multiple peers, which can be rewarded for their collaboration [288].

3) PREPARING A CALAMITY RESPONSE

The concept of leveraging blockchain-based solutions to improve disaster preparedness, response, and recovery efforts addresses critical societal challenges related to the safety of populations. The intrinsic qualities of blockchain technology, including decentralization, transparency, and immutability, make it a promising technology for reinforcing the resilience of applications in disaster scenarios. Blockchain has been previously applied to crowdsensing and IoT in disaster response scenarios. For instance, Sarbajna et al. [289] introduce DEIMOSBC, a blockchain-based system for crowdsensing after natural disasters, showcasing its potential for efficient data collection. Samir et al. [290] discuss blockchain-guided trustworthy interactions for distributed disaster management, emphasizing blockchain role in coordinating response efforts. Additionally, Ahmed [291] proposes a data security model for device-to-device (D2D) communication using blockchain, ensuring secure communication during crises. Wasserman et al. [292] present a blockchain-based data access environment for disaster risk reduction, enhancing data availability and sharing for risk assessment. Liu et al. [293] introduce a blockchain-based disaster recovery data storage and security auditing solution in multi-cloud environments, ensuring data resilience. Kaur et al. [294] propose a Blockchain-based IoT (BIoT) framework for

disaster management, combining blockchain and IoT technologies for efficient response. Bai et al. [295] discuss the use of blockchain-enabled IoT in insurance, focusing on calamity-based crop insurance as a disaster-related application. Moreover, Wang et al. [296] present RescueChain, a blockchain-based secure information-sharing system for UAV-aided disaster rescue operations. Badarudin et al. [297] introduce a blockchain-based assistance digital model for first responders and emergency volunteers, enhancing their coordination during disaster response. Lastly, Xing et al. [298] propose UAVs-aided delay-tolerant blockchain secure offline transactions for post-disaster vehicular networks, ensuring connectivity and secure transactions in challenging conditions.

However, it is important to note that blockchain practical implementation and seamless integration into existing disaster management systems present substantial challenges, such as the use of blockchain for Big Data [299], since issues like scalability, interoperability and regulatory considerations need to be addressed.

4) ENHANCING CYBERSECURITY

Blockchain-based solutions have gained attention for their potential to enhance resilience in several application domains, especially in cybersecurity. This subsection explores blockchain-based resilient applications and their role in strengthening cybersecurity while providing a robust foundation for secure data storage, authentication and protection against cyberthreats by recording transactions immutably and ensuring transparent, decentralized consensus mechanisms. Thus, use cases and innovations in blockchain-driven cybersecurity applications are examined (e.g., for industry, smart grids, vehicular networks, management, quantum computing, or AI), including secure data sharing, identity management, threat detection and incident response.

For example, in [300] Bansal et al., present a comprehensive survey of blockchain applications, emphasizing its decentralized nature and security attributes. The paper describes the architecture, characteristics and relevance in enhancing security, particularly in the realm of IoT, and highlights its potential in shaping the future of cybersecurity, cryptocurrency and IoT adoption. The authors identify the need for blockchain across various technical fields and its advantages over conventional systems, providing valuable insights into the transformative role of blockchain in enhancing security and trust in digital transactions and systems. Recently, Salama et al. [301] presented a comprehensive survey obtained by employing text mining techniques to analyze academic publications from digital libraries focusing on the topics of blockchain applied to cybersecurity. The authors use automated methods like topic modeling and keyword extraction to extract key topics from a vast body of literature. The article underscores the interdisciplinary nature of blockchain in the context of cybersecurity. It reveals the emerging risks and security vulnerabilities as blockchain evolves. Additionally, it identifies research gaps in computer security and proposes directions for future research aimed at establishing secure blockchain platforms.

Several specific application domains (e.g., industry, smart grids, vehicular networks, management, quantum computing) have been also using blockchain in cybersecurity-related topics. For example, the work presented by Maleh et al., [302] discusses the widespread influence of blockchain across various industries, highlighting its growing significance in cybersecurity. The paper emphasizes the versatility of blockchain, which can secure digital assets and transactions in various sectors, including healthcare and manufacturing, offering valuable insights into blockchain role in enhancing cybersecurity and privacy. The work focuses on fundamental concepts, architectural considerations and challenges associated with adopting blockchain for cybersecurity and showcases real-world applications of blockchain in areas like IoT, healthcare, e-commerce payments and digital forensics, making it a valuable resource for understanding the expanding role of blockchain in safeguarding digital assets and data privacy.

Zhuang et al. [303] discuss the growing importance of blockchain in enhancing cybersecurity for smart grids. While blockchain immutable and decentralized nature makes it appealing for securing smart grid data, there is a lack of comprehensive research in this area. To address this gap, the authors conducted a thorough survey, presenting insights, architectural ideas and implementation techniques related to blockchain use in smart grid cybersecurity. The article aims to serve as a valuable reference and guide for future research in this field.

In [304] Wang et al. explore the integration of blockchain to enhance cybersecurity in vehicular networks. While these networks have improved traffic system efficiency and safety, they also introduce new security challenges due to their dynamic topology and large scale. Traditional security solutions are not well-suited to address these issues, and centralized security mechanisms pose a single point of failure. The authors conduct a comprehensive review of existing blockchain-based cybersecurity mechanisms, along with performance analysis, to highlight the potential of blockchain in addressing these security concerns. Thus, the paper aims to provide guidance for further research in applying blockchain to enhance security in vehicular networks, offering a promising avenue for improved network protection.

In [305] Andriole discuss the critical process of evaluating emerging technologies, particularly blockchain and cryptocurrency, and their impact on cybersecurity, from a managerial perspective. It emphasizes the need for managers and executives to gain a thorough understanding of these technologies, assess their relevance to existing business models and processes, and evaluate their maturity. As a result, the authors recommend scoring these technologies based on their potential for pilot projects and emphasize the importance of finding pilot sponsors and developing comprehensive project

plans in collaboration with them. This guidance serves as a valuable resource for decision-makers looking to harness the potential of blockchain and cryptocurrency technologies within the context of cybersecurity and broader business strategies.

In [306] El-Latif et al. highlight the critical role of blockchain in cybersecurity, especially in the face of potential threats from large-scale quantum computers. Recognizing the vulnerability of current cryptographic mechanisms to hacking, the paper introduces a quantum-inspired approach to designing blockchain frameworks. It presents a novel authentication and encryption protocol based on quantum-inspired quantum walks (QIQW), which is applied to establish a secure blockchain system for data transmission among IoT devices. Instead of conventional cryptographic hash functions, quantum hash functions rooted in QIQW are used to link blocks within the blockchain. The framework offers advantages, such as enabling effective data sharing among IoT nodes and ensuring complete control over their records. Security analysis demonstrates the protocol capability to defend against message attacks and impersonation, ensuring the secure transmission of data among IoT devices in the context of smart edge utilities within IoT-based smart cities.

Another relevant topic that needs to be considered is related to the convergence of communication technologies with AI and blockchain. On the one hand, authors like Aiden et al. [307] discuss the growing convergence of communication networks in devices and systems, particularly in Cyber-Physical Systems (CPS), with applications ranging from industrial control systems to healthcare and electricity production. As these CPS integrate with Internet networks, security vulnerabilities become a concern. The authors highlight the rapid expansion of both blockchain and AI in various domains by emphasizing the bottleneck caused by centralized systems in handling real-time data across information systems, such as in healthcare. The authors propose blockchain decentralized database management as a solution to this problem, ensuring secure data storage, interchange and authentication, and suggest that AI can leverage collective data to provide insights for future predictions. As a conclusion, the authors underline the role of blockchain as a cutting-edge security technology and how it creates chronological chains through node agreements. With the increasing adoption of digital technologies and services across industries like banking, finance, cybersecurity and healthcare, the paper underscores the rising threat of cyberattacks. It explores the collaboration between AI and blockchain in enhancing cybersecurity, particularly in safeguarding cyber-physical systems.

On the other hand, researchers like Muheidat et al. [308] explore the rapidly evolving convergence of AI and blockchain technologies, particularly in everyday applications and various industries. The paper addresses the challenges of real-time data access and processing in centralized systems like healthcare and suggests that blockchain decentralized architecture, secure storage and authentication can provide solutions. Moreover, the paper highlights how AI, when integrated with blockchain, can generate valuable insights from shared data for predictive purposes. Thus, blockchain is recognized as a high-level cybersecurity technology, forming chains of secure blocks through mutual agreements between nodes. This technology convergence has the potential to boost various industries, including banking, insurance, cybersecurity, forecasting, medical services and cryptocurrency. Given the increasing adoption of digital systems and services, the paper underscores the significance of combining blockchain and AI to fortify defenses against cyberattacks and security threats, particularly in the context of securing cyber-physical systems.

5) PRIVACY AND CYBER RESILIENCE

In the current evolving context of Industry 5.0, the synergy of blockchain with principles of privacy and cyber-resilience has emerged as a central focus in academic research with several applications for the real world.

Blockchain is revolutionizing the domain of cyber-resilience, providing innovative solutions, and reshaping the landscape of cybersecurity and how blockchain-based cyber resilience frameworks can make a difference. For instance, Kelli et al. in [309] present a Cyber-Resilience Framework for Next-Generation Internet of Things (NG-IoT), which addresses the challenges posed by IoT in healthcare, where smart hospitals and remote assistance have become prevalent. Ensuring the security of eHealth networks and patient data against cyber threats is a complex task, particularly with the susceptibility of eHealth devices. The authors propose a solution that involves intelligent monitoring and robust access controls. Achieving interoperability among various healthcare organizations while complying with data protection regulations is emphasized. The framework incorporates blockchain-based access control to enhance cyber resilience in eHealth.

Secondly, in [310], Sharma et al., address the increasing IoT data volume driven by 5G adoption. The authors propose a secure IoT architecture that leverages blockchain and federated learning to address real-time application requirements while mitigating security concerns. The proposed architecture introduces lightweight authentication, model training, and a reward system, supporting cyber-resilience. Moreover, the authors put forward an experimental evaluation and analysis that substantiates the model effectiveness.

Thirdly, Gajek et al., in [311], discuss the relevance of blockchain in IIoT and cyber-resilience. To safeguard society's interests, robust cybersecurity measures are indispensable. Thus, blockchain is presented as an enhancement to security in industrial networks, as demonstrated through a USB-device use case, particularly relevant in incidents like Stuxnet.

Lastly, Harman et al. [312] emphasize the importance of protecting organizational assets for business continuity. While many organizations have invested in security

strategies, the authors have identified a rising trend of cyber incidents and the evolving threat landscape. Moreover, they advocate shifting the focus towards rapid response and recovery, recognizing the challenge of preventing all cyberattacks. The authors also identify common pitfalls in existing processes and propose a blockchain-based approach to enhance security and recovery, addressing these limitations. Cyber-resilience, in this context, should continuously adapt to the latest threats. Thus, the role of blockchain in applications that demand heightened cyber-resilience is introduced, which includes contributions to the energy sector, Vehicle-to-Everything (V2X) communications, railroad customs clearance, firms and organizations, and Digital Twin environments.

The energy sector, represented by the microgrid control and energy trading use case examples, shows a high potential for blockchain technology. For instance, Mahmud and Seo [313] presents a pioneering approach for distributed energy resource control. Leveraging a consensus algorithm and blockchain as a secure communication medium, this framework fosters cyber-resilience within distributed energy resources. In the described system each distributed energy resource communicates with a local blockchain server, ensuring secure data sharing for global control objectives like voltage and frequency regulation, and power sharing.

On the other hand, the escalating demand for electricity, driven by modernization, has elevated the significance of the power market in terms of fairness and security. In [314] Alam et al. acknowledge the unidirectional nature of traditional power markets and the emergence of prosumers in bidirectional energy supply microgrids. The authors propose a blockchain-based solution featuring a dual-chain model to facilitate peer-to-peer trading among prosumers. This innovative approach is complemented by smart contract deployment, coalition formation, and negotiation of electricity trades, offering efficient resolutions to contemporary energy management challenges.

The advancement of cellular technology has propelled the V2X market, necessitating robust cybersecurity measures. In [315] Sharma et al. discuss the implications of 5th Generation and Beyond (5G&B) networks on V2X, which entail vast data generation and local model learning for real-time tasks. This paradigm shift raises concerns about security and privacy, particularly concerning local nodes such as vehicles. The study seeks to address these concerns by identifying research questions, requirements and potential solutions to fortify cyber-resilience in V2X communications. In [316] Kim and Kim address the challenges posed by current railroad customs clearance systems, which result in train movement restrictions and resource inefficiency. Their solution introduces a cross-border blockchain-based non-stop customs clearance system, emphasizing integrity, stability and resource optimization. This system integrates diverse trade agreements into a single blockchain network. The empirical results highlight the system time and cost efficiency, along with its superior attack resilience compared to existing customs clearance systems.

In addition, cyberresilience transcends various societal actors, spanning organizations, individuals, governments, insurers and more. Hausken et al., in [317], conduct an extensive survey of literature, elucidating the foundational components of cyber resilience. Distinguishing between non-threat and threat actors, the study recognizes their roles and influences within the cyber resilience landscape. Moreover, it explores the intersections between cyber-resilience, cyber-insurance and IoT, highlighting the intricate relationships and potential benefits and vulnerabilities in this evolving digital landscape.

Lastly, Kanak et al. [318] advocate for the blockchain transformative potential beyond cryptocurrencies. Their work introduces a blockchain-based model tailored for collaborative digital twin environments. This model incorporates a public or private authority responsible for ensuring transaction non-repudiation, security and privacy. This innovative approach enhances security and integrity within decentralized mechanisms, as exemplified through insightful case studies.

To further clarify the reader the issues discussed throughout Section IV, the following Tables outline the main described applications in each of the pillars: Human-centricity (Table 4), Sustainability (Table 5) and Resilience (Table 6).

6) COMMUNICATIONS ARCHITECTURE RESILIENCE

As it was previously mentioned, blockchain technologies allow for implementing tamper-proof, redundant and high-security communications ledgers. Such features can be extrapolated to complete blockchain-based architectures to provide a better alternative to traditional communications architectures. For instance, Cloud Computing architectures have been widely used, but they have a significant limitation in terms of cybersecurity [319]: the cloud is a centralized point-of-failure that can be impacted by cyberattacks (e.g., DoS/DDoS attacks), traffic overload or software/hardware problems that may render the whole system useless. These are common problems for systems that have not been scaled appropriately or that have not implemented appropriate security policies. Moreover, most cloud-based solutions were not devised for distributing workload among peers, so the implementation of P2P systems may overload the system when a large number of entities exchange information with the cloud simultaneously. In contrast, blockchain-based architectures are inherently distributed, thus being able to support Cloud Computing systems. For example, researchers have proposed the use of blockchain for implementing a decentralized cloud storage that consists of secure data blocks that are distributed among peers that provide storage space [320].

As an example, Figure 6 depicts a decentralized IIoT architecture based on blockchain that is composed of four main components:

TABLE 4. Most relevant blockchain solutions in each Industry 5.0 dimension: Human-centricity.

Addressed Topic	Operational Focus	References
Worker personal development tracking	Training, skills development, gamification (incentives), well-being monitoring, fake content prevention, tracing intellectual property, decentralized AR/MR/VR ecosystems, and enhanced collaborative environments.	[161], [162], [163], [173], [174], [176], [177], [178], [179], [180]
Human-centric production systems	Blockchain-based ICPSs, fair payment with a reputation for reliable ICPSs, coordination of local manufacturing processes	[181], [182], [183], [184], [185], [186], [187], [188]
Creating a safe workplace	Safety supervision system, Safety as a Service (Safe-aaS) infrastructure, Physical and mental health data monitoring	[189], [190], [191], [192]
Designing inclusive industrial work environments	Collaborative and human-into-the loop approaches while eliminating unnecessary intermediaries, collaborative production and long-life training	[193], [194], [88], [196]
Robots and autonomous vehicles	Enabling human or machine interaction (e.g., UAVs, AGVs, robots, cobots, exoskeletons) through blockchain or smart contracts Novel incentivized services or business models (e.g., ride-sharing, UAVs-as-a-Service Tracking of typical industrial tasks for autonomous and semi-autonomous vehicles (e.g., refueling, charging, parking, repairing), reward systems for vehicular networks	[207], [16], [208], [211], [212], [213], [214], [215]
Development of AI-enabled applications	Data collection, trustworthiness verification, automate reliable data circulation, use of deep learning, federated learning, and federated transfer learning techniques cognitive manufacturing with end-to-end traceability	[216], [217], [218], [86], [219], [220], [221], [222], [224]
Worker privacy	Protection against cyber-attacks (access control, data availability, DoS/DDoS attack protection, post-quantum solutions, cryptosystems adequate for IIoT devices, privacy-preserving solutions)	[142]
Supply chain and Logistics traceability	Creation of transparent, efficient, and secure systems that track and enhance the visibility of goods and services throughout the supply chain, ensuring accountability and trust while optimizing logistics processes.	[229], [230], [231], [233]
Manufacturing and safety traceability	Establish transparent and secure systems for tracking and verifying the production and safety compliance of goods, enhancing consumer trust, and promoting responsible manufacturing practices.	[235], [236], [237], [238]
Consumer-in-the-loop and CE traceability	Focus on the creation of systems that actively involve consumers in CE initiatives, enabling them to trace product lifecycles, make sustainable choices, and contribute to a more eco-conscious and responsible consumer culture.	[239]
Other human-related activities traceability	Transparently trace and verify a wide range of human-related activities, fostering accountability, trust, and efficiency in areas beyond supply chain and manufacturing, ultimately enhancing various aspects of human-centric processes and interactions	[241], [242], [243]

- IIoT Device Layer: it is conformed by the IIoT devices deployed in the Industry 5.0 factory. Such devices receive commands from the blockchain subsystem (usually in relation to actions triggered by smart contracts). The system stores data in the decentralized storage subsystem and transactions on the blockchain.
- Blockchain subsystem: it is composed by all the elements that make up the blockchain, as well as by the logic that runs on it (i.e., the smart contracts).
- Decentralized storage: instead of centralizing the data on a single central server or in a server cluster that conforms a cloud, they are scattered throughout multiple servers over the Internet so as to provide redundancy and to avoid DoS attacks.
- Blockchain IIoT applications: they provide high-level applications to remote users by interacting with the transactions stored on the blockchain and can retrieve data from the decentralized storage subsystem.

V. MAIN CHALLENGES OF THE IMPLEMENTATION OF BLOCKCHAIN-BASED INDUSTRY 5.0 APPLICATIONS

Despite all the benefits and media hype on the use of blockchain for a myriad of applications, it is not always the best solution for every Industry 5.0 scenario. For instance, on many occasions, a traditional database and an ERP are

TABLE 5. Most relevant blockchain solutions in each Industry 5.0 dimension: Sustainability.

Addressed Topic	Operational Focus	References
Value Chain Environmental and Social Traceability	Enable organizations to monitor and improve their environmental and social impact throughout the product or service value chain, fostering responsible and eco-friendly practices	[244], [245], [246], [90], [127], [148], [149]
Circular Economy	Focus on the creation of transparent, efficient, and eco-conscious systems that enable the traceability, optimization, and promotion of resource recycling and sustainable practices, ultimately contributing to a more environmentally responsible and economically viable world.	[239], [247]
Carbon Credits Exchange	Facilitate transparent, secure, and efficient trading of carbon credits, enabling organizations to mitigate their carbon footprint and accelerate the transition to a more sustainable and environmentally-conscious future.	[252], [253], [254], [255], [256], [257]
Green Energy Traceability	Focus on the establishment of transparent, verifiable systems that trace the production, distribution, and consumption of renewable energy, promoting accountability, reducing carbon emissions, and advancing the transition to a more sustainable energy ecosystem.	[261], [262, [263], [140]
Responsible Resource Management	Enhance transparency and accountability in resource allocation and consumption, enabling organizations and individuals to make environmentally-conscious decisions and contribute to the responsible adoption of finite resources for a more sustainable future.	[264], [265], [266], [267], [125], [126]
Development of additive manufacturing enabled applications.	Minimizing part delivery time and improving stock management of 3D printing manufacturers, Just-in-Time models for 3D printing, distribute additive manufacturing in Defense, Track and integrate 3D printing files to avoid manufacturing mistakes and provide trustworthiness, protection of intellectual property	[150] [151], [152], [153], [154], [155], [156], [157]

TABLE 6. Most relevant blockchain solutions in each Industry 5.0 dimension: Resilience.

Addressed Topic	Operational Focus	References
Supply chain management	Perform robust and adaptable systems that enhance transparency, efficiency, and resilience in supply chain operations, ensuring continuity and reliability in the face of disruptions and challenges	[268], [269], [270], [271], [272], [273], [284], [285]
Calamity response	Create agile and transparent systems for disaster management, facilitating real-time coordination, resource allocation, and data sharing to enhance the effectiveness of response efforts during emergencies and natural disasters.	[289], [298], [297], [296], [295], [294], [293], [292], [291]
Cybersecurity	Strengthen digital defenses, providing secure, decentralized solutions for safeguarding sensitive data and critical infrastructure, reinforcing resilience against cyber threats and ensuring the integrity of digital ecosystems.	[300], [301], [302], [303], [304], [305], [306], [308], [307], [286], [288]
Privacy and cyber resilience	Establish robust, privacy-preserving solutions that enhance data protection, identity management, and overall cyber resilience, providing individuals and organizations with secure, decentralized tools to withstand evolving digital threats.	[310], [311], [312], [313], [314], [315], [316], [318]

enough to store the information shared by an industrial organization. Therefore, an Industry 5.0 application developer must first determine whether blockchain is the most appropriate technology. For such a purpose, the following subsections discuss the main questions that Industry 5.0 developers should answer in order to determine whether the use of blockchain is appropriate. Nonetheless, it is worth noting that the literature contains examples of frameworks aimed at determining the necessity of using blockchain, either generic [321], for Industry 4.0 applications [322], or for specific industries like construction [323] or logistics [324].

A. DOES THE APPLICATION NEED TO BE SCALED EASILY?

Bottlenecks caused by excessive traffic load may be a problem in traditional cloud computing-based architectures, although in the last years, they have evolved towards new paradigms that decrease the communications with the cloud

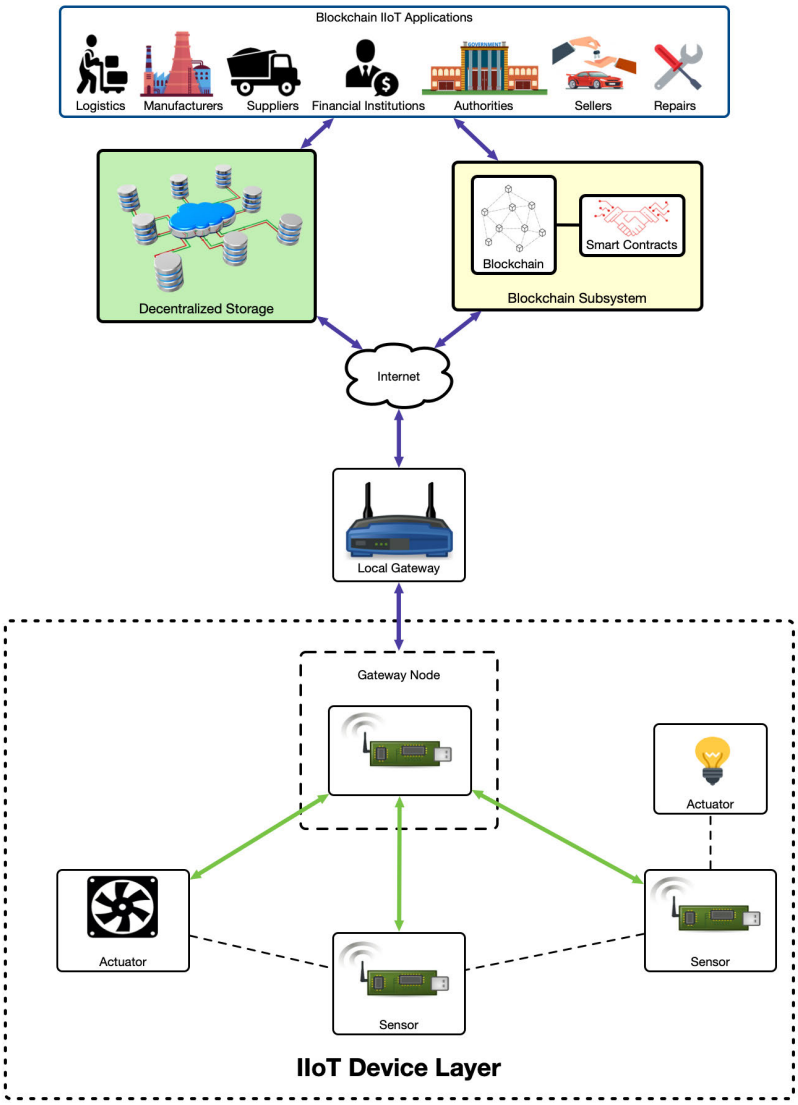

FIGURE 6. Example of blockchain-based IIoT architecture.

by providing services close to the edge of the network, where IIoT nodes and the rest of industrial devices operate. Thus, Edge and Mist Computing [20], [21], [325], [326], [327] allow for offloading the cloud from a significant part of the requests and data exchanges required by the deployed network devices. Blockchain can also be useful for such a kind of architecture. For instance, in [328] it is presented a blockchain design for Edge Computing environments. Such an article studies the optimal resource allocation strategy to store metadata and blocks, as well as the consensus protocol (e.g., Proof of Stake) to make use of less storage and energy consumption than traditional blockchain systems.

It is also worth mentioning that many blockchains make use of dedicated hardware (e.g., mining hardware), so scaling a blockchain-based Industry 5.0 application should consider the fact that the required blockchain-specific infrastructure will need to be extended. In addition, storage will also have to be scaled as the blockchain grows with the number of stored transactions. Furthermore, communications infrastructure will have to be able to handle the increasing number of peers that will carry out P2P exchanges.

Finally, scalable blockchain-based solutions may have to balance tradeoffs between privacy, speed and decentralization. One solution is to consider the use of off-chain operations and state channels. Off-chain operations are carried out outside of the blockchain and later added to it, while state channels allow users to transfer their state on a blockchain outside of such a network (i.e., off-chain), where it can be manipulated without the limitations of the blockchain [329].

This solution poses additional challenges on how to ensure the verifiability and reliability of off-chain operation results. To tackle such an issue, in [329] the authors propose a new state channel solution for the Ethereum blockchain network in

the form of a State Channel as a Service, which incorporates a secure distributed and decentralized network, although off-chain. This tries to mitigate scalability problems while also responding to the transparency and traceability challenges. The proposed solution performs operations off-chain, giving users the confidence that only the valid last off-chain state is transferred back on the blockchain network.

Other solutions to the blockchain scalability problem may involve storing most of the data off-chain and creating and storing a hash code of that data on the blockchain, in order to guarantee the reliability of the original data stored off-chain [330].

B. DOES THE BLOCKCHAIN NEED TO BE OPTIMIZED IN TERMS OF ENERGY CONSUMPTION?

Blockchains are usually power-hungry due to their need for continuous communications [133], [136] and the use of energy-expensive consensus mechanisms and high-security cryptosystems. These power needs are especially relevant for devices that depend on batteries, which currently cannot make direct use of some of the most power-hungry consensus mechanisms (e.g., PoW), so they have to rely on an intermediate entity to interact with the blockchain. Less energy-intensive consensus mechanisms still need to be analyzed in terms of energy consumption, like the ones previously mentioned in Section III-D2. Moreover, other green alternatives have been proposed to decrease blockchain data updates, like mini-blokchains [141].

Security mechanisms also consume a significant amount of energy. Specifically, the majority of blockchains use Elliptic Curve Cryptography (ECC) cryptosystems, which are usually more efficient in terms of energy than algorithms like Rivest-Shamir Addleman (RSA) [143], but they can still be considered as power hungry [144]. ECC is recognized for its effectiveness in securing communications within European industrial protocols, particularly due to its suitability for low-memory devices [145]. Hash algorithm execution is not as demanding in terms of energy as public-key cryptography, but algorithms used traditionally by blockchains like SHA-256 are slower than other recent alternatives (e.g., Scrypt [331], Equihash [332], X11 [333], RandomX [122]), so energy consumption may be reduced during their execution.

C. DOES THE APPLICATION NEED TO BE HIGHLY SECURE FOR IIOT DEVICES?

As it was previously mentioned, the security of the exchanged information is essential for human-centric applications to preserve worker privacy. For instance, it is possible to deploy IIoT camera-based sensors in an industrial facility to prevent accidents [334], but the captured images need to be stored (either in files or their hash) and transmitted securely.

IIoT nodes like sensors, actuators or certain industrial machinery are usually constrained in terms of computational power, memory and energy consumption, so it is difficult to implement on them high-security cryptosystems like the public-key algorithms commonly used by blockchain [335]. Moreover, the implementation of energy-efficient post-quantum cryptosystems for low-power devices needs to be further analyzed for the industrial systems that will operate in the next ten to twenty years [142], [336], [337].

Moreover, IIoT nodes have additional limitations that need to be considered in applications when they need to interact with a blockchain. First, it is important to note that such nodes are not anonymous: they are identified by an identifier, so, in certain scenarios, industrial competitors may be able to obtain critical business information from such nodes. This fact has to be especially considered in blockchain-based systems, which can use mixing techniques to enhance privacy, but which, in some cases, have been de-anonymized [338]. In addition, Industry 5.0 developers should consider the use of permissioned blockchains or multichains in cases when it is essential to certificate the identity of the IIoT devices that interact with the blockchain or where only a reduced group of participants should be able to monitor the blockchain [124], [339].

Finally, IIoT node data integrity should be verified to avoid the use of malicious or corrupted information that may threaten the blockchain resilience. Besides the high-security mechanisms used by blockchains, some authors have suggested the use of integrity services to not rely on third-party verification [340].

D. DOES THE APPLICATION NEED TO CONSIDER OTHER IIOT NODE LIMITATIONS?

In addition to the different aspects mentioned in the previous subsections, it is worth considering other aspects of IIoT nodes that impact the sustainability of Industry 5.0 applications:

- Latency and throughput limitations. ICPSs and the underlying IIoT systems often have to handle large amounts of transactions per second, which is a problem for many blockchains due to their transaction latency and throughput. For instance, initially, Bitcoin was only able to process a maximum of 7 transactions per second [341], although later it was possible to increase such a throughput by adjusting block size [342]. Moreover, such an initial version of Bitcoin proposed to use a transaction latency that followed a Poisson distribution with a mean of 10 minutes [23], which is a long time in comparison to the transaction processing speed of most modern databases. Other blockchains like Ethereum have evolved significantly in the last years in terms of transaction speed and latency. Initially, each blockchain node is required to process every transaction sent through the network [343], but the latest developments allow for decreasing dramatically such a transaction load. For instance, sharding [344] enables to splitting of nodes and transactions into small groups called shards, so that the selected nodes only process transactions for a specific shard, thus increasing network throughput.

Another interesting solution is Raiden [345], which makes use of bi-directional channels between groups of nodes, which avoid performing direct transactions with the Ethereum blockchain. There is a simplified version of Raiden called μRaiden [346] and a similar solution for Bitcoin called Lightning Network [347]. Between the layer-2 solutions [348], it is also worth mentioning Plasma [349], which proposes the use of a tree hierarchy of blockchains where parent blockchains can enforce the execution of smart contracts to their child blockchains. Finally, it is important to consider the limitations for the efficient execution of smart contracts, which can in part be mitigated by making use of highly parallel solutions [350].

- Growth sustainability. A blockchain grows continuously, as more transaction blocks are added, so it is necessary to reduce its storage space by making use of compression techniques or smaller versions of the blockchain [141], [351], [352]. This is especially important for devices that are constrained in terms of memory, like most IIoT low-power devices. In addition, it should be considered that the growth of the blockchain and its members will derive from requiring a larger storage and mining infrastructure. Such an infrastructure can be implemented with commercial hardware, which has evolved significantly in the last few years [353].

E. IS IT NECESSARY TO IMPLEMENT SOPHISTICATED CONSENSUS ALGORITHMS?

It must be noted that the use of sophisticated consensus algorithms is not necessary for applications based on private or federated blockchains, so power consumption and computational needs can be significantly reduced in such systems. In other Industry 5.0 blockchain-based applications, the selection of consensus algorithms needs to provide a trade-off between performance, sustainability, and resilience. For instance, some PoW consensus algorithms like the one used by Bitcoin have been proven to be energy inefficient [129], but there are others whose performance and power consumption need to be assessed, such as Proof-of-Stake, Proof-of-Space, Delegated Proof-of-Stake (DPoS) with downgrade [354], Proof-of-Quality-Factor (PoQF) [355], Proof-of-Activity, Practical Byzantine Fault Tolerance (PBFT) [356], Sieve [357], Proof-of-Burn, Proof-of-Personhood [358] and others that can be found in [132].

F. DOES THE APPLICATION NEED TO BE INTEGRATED WITH DIFFERENT BLOCKCHAINS OR DLTS?

It is possible that an Industry 5.0 company needs to provide support for several blockchains within its internal software ecosystem. For example, a company may decide to accept payments through Bitcoin but deploy smart contracts on Ethereum or Hyperledger Fabric. As a consequence, it is necessary to design and implement interoperable and standardized solutions.

In this regard, entities like IEEE are working on standardization initiatives related to the health industry for the development of consensus mechanisms for clinical trials and the pharmaceutical industry [359] or for supply chain finance [360]. Moreover, IEEE has also defined the key general aspects of blockchain systems, like data format requirements [361], IoT data management [362] or even a blockchain-based reference architecture for the electronic invoice (e-invoice) business process [363]. Additional standardization activities include ISO/TC 307 [364], CEN-CLC/JTC 19 [365], ETSI ISG Permission Distributed Ledgers (PDL) [366] or ITU-T Focus Group on DLTs [367].

It is also worth noting that the World Economic Forum and the Global Blockchain Business Council presented a report that maps standardization efforts as of August 2020 [368]. In addition to IEEE, the mentioned organizations consider more than thirty formal organizations like W3C, IRTF, IEC or IETF. They conclude that there are both gaps and overlaps in the current standardization landscape. Moreover, they remark that there are technical aspects of blockchain that are not yet mature enough for standardization and that rushing to standardization could hinder innovation or lead to harmful incentives. Even though some time has elapsed since such an initial assessment, the conclusions drawn remain relevant and applicable.

G. DOES YOUR INDUSTRY HAVE TO COMPLY WITH REGULATORY AND LEGAL ASPECTS RELATED TO THE USE OF BLOCKCHAIN?

Industry 5.0 companies need to fulfill the requirements imposed by the law and regulatory agencies, especially the aspects related to sustainability. Different countries have imposed restrictions and laws on the use of cryptocurrencies [369], while others like the European Union have launched initiatives to monitor the development of blockchain within its territories [370].

VI. CONCLUSION

Industry 5.0 is a novel concept derived from the Industry 4.0 paradigm that is going to transform the way smart factories operate by redefining their mission and vision to be more sustainable, human-centric and resilient. Industry 5.0 relies on technologies previously developed by Industry 4.0 as well as on new, promising technologies. Among them, blockchain is one of the most compelling technologies that can help implement communications architectures for Industry 5.0 applications, thanks to its ability to bring security, trust, immutability, disintermediation, decentralization and a high degree of automation through smart contracts. This article provided a detailed review of the benefits that blockchain can bring to Industry 5.0, as well as an analysis on the impact of blockchain on the main Industry 5.0 foundations. Moreover, this article examined the benefits and challenges that may arise when developing blockchain-based Industry 5.0 applications.

Furthermore, a thorough review of the most recent and relevant blockchain-based Industry 5.0 applications was presented. As a result, this article provides a comprehensive and extensive list of recommendations for future Industry 5.0 developers to guide them in the implementation of the next-generation Industry 5.0 applications.

VII. AUTHOR CONTRIBUTIONS

Conceptualization, Paula Fraga-Lamas and Tiago M. Fernández-Caramés; methodology, Paula Fraga-Lamas, Sergio Ivan Lopes, António M. Rosado da Cruz, and Tiago M. Fernández-Caramés; investigation, Paula Fraga-Lamas and Tiago M. Fernández-Caramés; writing—original draft preparation, Paula Fraga-Lamas, Sergio Ivan Lopes, António M. Rosado da Cruz, and Tiago M. Fernández-Caramés; writing—review and editing, Tiago M. Fernández-Caramés; supervision, Tiago M. Fernández-Caramés; project administration, Paula Fraga-Lamas, Sergio Ivan Lopes, and Tiago M. Fernández-Caramés; and funding acquisition, Tiago M. Fernández-Caramés. All authors read and agreed to the published version of the manuscript.

REFERENCES

[1] *Industry 5.0 Towards a Sustainable, Human-Centric and Resilient European Industry*, European Commission, Brussels, Belgium, Jan. 2021.

[2] H. Kagermann, *Securing the Future of German Manufacturing Industry: Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0*, Final Report of the Industrie 4.0 Working Group, Acatech National Academy of Sciences and Engineering, Munich, Germany, Apr. 2013.

[3] E. Munera, J. L. Poza-Lujan, J. L. Posadas-Yagüe, J. Simo, J. F. Blanes, and P. Albertos, "Control kernel in smart factory environments: Smart resources integration," in *Proc. IEEE Int. Conf. Cyber Technol. Autom., Control, Intell. Syst. (CYBER)*, Shenyang, China, Jun. 2015, pp. 2002–2005.

[4] *Announcement of the Industrie 4.0 Project in the 2011 Hannover Fair*. Accessed: Jun. 21, 2023. [Online]. Available: https://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-Dinge-Weg-4-industriellen-Revolution

[5] *Industrie 4.0 Project Official Web Page*. Accessed: Jul. 13, 2023. [Online]. Available: https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html

[6] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[7] Z. Wang, C. Chen, B. Guo, Z. Yu, and X. Zhou, "Internet plus in China," *IT Prof.*, vol. 18, no. 3, pp. 5–8, May 2016.

[8] Center for Strategic and International Studies. *Made in China 2025: Critical Questions*. Accessed: Jul. 13, 2023. [Online]. Available: https://www.csis.org/analysis/made-china-2025

[9] J. Leng, W. Sha, B. Wang, P. Zheng, C. Zhuang, Q. Liu, T. Wuest, D. Mourtzis, and L. Wang, "Industry 5.0: Prospect and retrospect," *J. Manuf. Syst.*, vol. 65, pp. 279–295, Jan. 2022.

[10] *100 Radical Innovation Breakthroughs for the Future*, European Commission Report, Brussels, Belgium, Nov. 2019.

[11] *Enabling Technologies for Industry 5.0 Results of a Workshop With Europe's Technology Leaders*, European Commission Report, Brussels, Belgium, Sep. 2020.

[12] Ó. Blanco-Novoa, T. M. Fernndez-Carams, P. Fraga-Lamas, and M. A. Vilar-Montesinos, "A practical evaluation of commercial industrial augmented reality systems in an Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 8201–8218, 2018.

[13] P. Fraga-Lamas, T. M. FernáNdez-CaraméS, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, "A review on industrial augmented reality systems for the Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13358–13375, 2018.

[14] H. R. Chi, C. K. Wu, N.-F. Huang, K.-F. Tsang, and A. Radwan, "A survey of network automation for industrial Internet-of-Things toward Industry 5.0," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 2065–2077, Feb. 2023, doi: 10.1109/TII.2022.3215231.

[15] D. K. Jain, Y. Li, M. J. Er, Q. Xin, D. Gupta, and K. Shankar, "Enabling unmanned aerial vehicle borne secure communication with classification framework for Industry 5.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5477–5484, Aug. 2022, doi: 10.1109/TII.2021.3125732.

[16] T. Fernández-Caramés, O. Blanco-Novoa, M. Suárez-Albela, and P. Fraga-Lamas, "A UAV and blockchain-based system for Industry 4.0 inventory and traceability applications," in *Proc. 5th Int. Electron. Conf. Sensors Appl.*, vol. 6, Nov. 2018, p. 26.

[17] S. K. Jagatheesaperumal and M. Rahouti, "Building digital twins of cyber physical systems with metaverse for Industry 5.0 and beyond," *IT Prof.*, vol. 24, no. 6, pp. 34–40, Nov. 2022, doi: 10.1109/MITP.2022.3225064.

[18] A. Du, Y. Shen, Q. Zhang, L. Tseng, and M. Aloqaily, "CRACAU: Byzantine machine learning meets industrial edge computing in Industry 5.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5435–5445, Aug. 2022, doi: 10.1109/TII.2021.3097072.

[19] I. Ahmad, S. Abdullah, and A. Ahmed, "IoT-fog-based healthcare 4.0 system using blockchain technology," *J. Supercomput.*, vol. 79, no. 4, pp. 3999–4020, Mar. 2023.

[20] T. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. Vilar-Montesinos, "A fog computing and cloudlet based augmented reality system for the Industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1798, Jun. 2018.

[21] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. A. Díaz-Bouza, "A fog computing based cyber-physical system for the automation of pipe-related tasks in the Industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1961, Jun. 2018.

[22] B. Bajic, A. Rikalovic, N. Suzic, and V. Piuri, "Industry 4.0 implementation challenges and opportunities: A managerial perspective," *IEEE Syst. J.*, vol. 15, no. 1, pp. 546–559, Mar. 2021, doi: 10.1109/JSYST.2020.3023041.

[23] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jun. 21, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[24] C. Ebert, P. Louridas, T. M. Fernández-Caramés, and P. Fraga-Lamas, "Blockchain technologies in practice," *IEEE Softw.*, vol. 37, no. 4, pp. 17–25, Jul. 2020.

[25] *Chainspect Official Webpage*. Accessed: Mar. 15, 2024. [Online]. Available: https://chainspect.app/dashboard

[26] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927–126950, 2020.

[27] S. Kruglik, K. Nazirkhanova, and Y. Yanovich, "Challenges beyond blockchain: Scaling, oracles and privacy preserving," in *Proc. 16th Int. Symp. Problems Redundancy Inf. Control Syst. (REDUNDANCY)*, Oct. 2019, pp. 155–158.

[28] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. S. M. Kayes, M. Alazab, and P. Watters, "A comparative analysis of distributed ledger technology platforms," *IEEE Access*, vol. 7, pp. 167930–167943, 2019, doi: 10.1109/ACCESS.2019.2953729.

[29] M. Belotti, N. Božic, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3796–3838, 4th Quart., 2019, doi: 10.1109/COMST.2019.2928178.

[30] (Feb. 2023). *Benchmarking Hyperledger Fabric 2.5 Performance*. Accessed: Mar. 15, 2024. [Online]. Available: https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance

[31] *Polkadot FAQs Official Webpage*. Accessed: Mar. 15, 2024. [Online]. Available: https://wiki.polkadot.network/docs/faq

[32] *Corda Performance Benchmarking Result Official Webpage*. Accessed: Mar. 15, 2024. [Online]. Available: https://docs.r3.com/en/platform/corda/4.8/enterprise/performance-testing/performance-results.html

[33] (Jan. 2022). *Are ZK-Rollups The Last Piece of Blockchain's Scaling Solution Puzzle? Forbes Article*. Accessed: Mar. 15, 2024. [Online]. Available: https://www.forbes.com/sites/lawrencewintermeyer/2022/01/20/are-zk-rollups-the-last-piece-of-blockchains-scaling-solution-puzzle/

[34] (Sep. 16, 2021). *What do You Prefer—Maximum Security or Cheaper Transactions? Polygon Labs*. Accessed: Mar. 15, 2024. [Online]. Available: https://polygon.technology/blog/what-do-you-prefer-maximum-security-or-cheaper-transactions

[35] (Sep. 2023). *Avalanche's HyperSDK Blockchain Upgrade Hits 143K TPS on Testnet. Cointelegraph*. Accessed: Mar. 15, 2024. [Online]. Available: https://cointelegraph.com/news/avalanche-hyper-sdk-blockchain-upgrade-hits-143000-tps-on-testnet

[36] *Analyzing Cosmos TPS: Performance, Comparisons, and Alternatives*. Accessed: Mar. 15, 2024. [Online]. Available: https://webisoft.com/articles/cosmos-tps/

[37] *Kaspa on Rust: Evolving Testnet 11*. Accessed: Mar. 15, 2024. [Online]. Available: https://kaspa.org/kaspa-on-rust-evolving-testnet-11/

[38] *What is IOTA*. Accessed: Mar. 15, 2024. [Online]. Available: https://www.iota-services.com/what-is-iota/

[39] *Understanding EOS & EOSIO*. Accessed: Mar. 15, 2024. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/eos-eosio/

[40] *Cardano Hydra: How Cardano's Scaling Solution Liberates ADA*. Accessed: Mar. 15, 2024. [Online]. Available: https://dailycoin.com/cardano-hydra-scaling-solution-liberates-ada/

[41] *Gemini Ignite (Tendermint) and The Cosmos Network*. Accessed: Mar. 15, 2024. [Online]. Available: https://www.gemini.com/cryptopedia/cosmos-ignite-crypto-consensus-tendermint-ecosystem#section-the-cosmos-network-and-ignite-core

[42] M. Mazzoni, A. Corradi, and V. Di Nicola, "Performance evaluation of permissioned blockchains for financial applications: The ConsenSys quorum case study," *Blockchain: Res. Appl.*, vol. 3, no. 1, Mar. 2022, Art. no. 100026.

[43] C. Slager, "Security evaluation of GoQuorum-based smart contracts: A case study of malfunctioning access control and double-spending," Tech. Rep., 2021. [Online]. Available: https://cse3000-research-project.github.io/static/0ae72b924e52ac9c732ca441a730d4da/poster.pdf

[44] I. Amores-Sesar, C. Cachin, and J. Mi, "Security analysis of ripple consensus," in *Proc. 24th Int. Conf. Princ. Distrib. Syst. (OPODIS)*, vol. 184, 2021, pp. 10:1–10:16.

[45] L. Baird and A. Luykx, "The hashgraph protocol: Efficient asynchronous BFT for high-throughput distributed ledgers," in *Proc. Int. Conf. Omni-layer Intell. Syst. (COINS)*, Barcelona, Spain, Aug. 2020, pp. 1–7.

[46] *Exonum Official Webpage*. Accessed: Mar. 15, 2024. [Online]. Available: https://exonum.com/doc/version/latest/get-started/what-is-exonum/

[47] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for Industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, pp. 69160–69199, 2022, doi: 10.1109/ACCESS.2022.3186892.

[48] S. Nahavandi, "Industry 5.0—A human-centric solution," *Sustainability*, vol. 11, no. 16, p. 4371, Aug. 2019.

[49] D. Paschek, A. Mocan, and A. Draghici, "Industry 5.0 The expected impact of next industrial revolution," in *Proc. MakeLearn & TIIM Conf.*, May 2019, pp. 125–132.

[50] A. Beniiche, S. Rostami, and M. Maier, "Society 5.0: Internet as if people mattered," *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 160–168, Dec. 2022, doi: 10.1109/MWC.009.2100570.

[51] Council for Science, Technology and Innovation, Government of Japan. (Dec. 18, 2015). *Report on The 5th Science and Technology Basic Plan*. Accessed: Jul. 13, 2023. [Online]. Available: https://www8.cao.go.jp/cstp/kihonkeikaku/5basicplan_en.pdf

[52] Keidanren. (Nov. 2018). *Soc. 5.0: Co-Creating Future*. Accessed: Jul. 13, 2023. [Online]. Available: https://www.keidanren.or.jp/en/policy/2018/095.html

[53] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2019). *The European Green Deal*. Accessed: Jul. 13, 2023. [Online]. Available: https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_en.pdf

[54] *European Commission, Industry 5.0: A Transformative Vision for Europe, ESIR Policy Brief No.3*. Accessed: Mar. 6, 2024. [Online]. Available: https://www.horizon-europe.gouv.fr/sites/default/files/2022-01/industry-5-0-pdf-5324.pdf

[55] P. Fraga-Lamas, S. I. Lopes, and T. M. Fernández-Caramés, "Green IoT and edge AI as key technological enablers for a sustainable digital transition towards a smart circular economy: An Industry 5.0 use case," *Sensors*, vol. 21, no. 17, p. 5745, Aug. 2021.

[56] P. Fraga-Lamas and T. M. Fernández-Caramés, "Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality," *IT Prof.*, vol. 22, no. 2, pp. 53–59, Mar. 2020.

[57] L. Lebastard and R. Serafini. *Understanding the Impact of COVID-19 Supply Disruptions on Exporters in Global Value Chains*. Accessed: Apr. 10, 2024. [Online]. Available: https://www.ecb.europa.eu/press/research-publications/resbull/2023/html/ecb.rb230322 5c08629152.en.html

[58] *How is the War in Ukraine Impacting the Global Supply Chain*? Accessed: Apr. 10, 2024. [Online]. Available: https://www.weforum.org/agenda/2022/07/ripple-effects-from-russia-ukraine-war-test-global-economies/

[59] S. Lee and M. Lee, "The Israel-Hamas War, oil price volatility, and anticipated impacts: Implications for Korean industries," Korea Inst. Ind. Econ. Trade, Res. Paper 23/MER/10/2, 2023, vol. 301. [Online]. Available: https://ssrn.com/abstract=4733510

[60] G. Gereffi, H.-C. Lim, and J. Lee, "Trade policies, firm strategies, and adaptive reconfigurations of global value chains," *J. Int. Bus. Policy*, vol. 4, no. 4, pp. 506–522, Dec. 2021.

[61] M. Ghobakhloo, M. Iranmanesh, M. F. Mubarak, M. Mubarik, A. Rejeb, and M. Nilashi, "Identifying Industry 5.0 contributions to sustainable development: A strategy roadmap for delivering sustainability values," *Sustain. Prod. Consumption*, vol. 33, pp. 716–737, Sep. 2022.

[62] T. van Erp, N. G. P. Carvalho, M. C. Gerolamo, R. Gonçalves, N. G. M. Rytter, and B. Gladysz, "Industry 5.0: A new strategy framework for sustainability management and beyond," *J. Cleaner Prod.*, vol. 461, Jul. 2024, Art. no. 142271.

[63] I. Askoxylakis, "A framework for pairing circular economy and the Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[64] J. Leng, Y. Zhong, Z. Lin, K. Xu, D. Mourtzis, X. Zhou, P. Zheng, Q. Liu, J. L. Zhao, and W. Shen, "Towards resilience in Industry 5.0: A decentralized autonomous manufacturing paradigm," *J. Manuf. Syst.*, vol. 71, pp. 95–114, Dec. 2023.

[65] *Millennials at Work Reshaping Workplace*, PriceWaterhouseCoopers, London, U.K., 2011.

[66] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[67] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[68] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[69] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[70] Y. Liu, Z. Fang, M. H. Cheung, W. Cai, and J. Huang, "Mechanisms design for blockchain storage sustainability," *IEEE Commun. Mag.*, vol. 61, no. 8, pp. 102–107, Aug. 2023, doi: 10.1109/MCOM.001.2200809.

[71] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019.

[72] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on blockchain-based smart contracts: Technical aspects and future research," *IEEE Access*, vol. 9, pp. 87643–87662, 2021.

[73] D. He, K. Ding, S. Chan, and M. Guizani, "Unknown threats detection methods of smart contracts," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4430–4441, Feb. 2024, doi: 10.1109/jiot.2023.3299492.

[74] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart contract security: A software lifecycle perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019.

[75] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.

[76] P. Zhang, Q. Yu, Y. Xiao, H. Dong, X. Luo, X. Wang, and M. Zhang, "BiAn: Smart contract source code obfuscation," *IEEE Trans. Softw. Eng.*, vol. 49, no. 9, pp. 4456–4476, Sep. 2023, doi: 10.1109/tse.2023.3298609.

[77] N. Sánchez-Gómez, J. Torres-Valderrama, J. A. García-García, J. J. Gutiérrez, and M. J. Escalona, "Model-based software design and testing in blockchain smart contracts: A systematic literature review," *IEEE Access*, vol. 8, pp. 164556–164569, 2020.
[78] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain for intelligent transportation systems: Applications, challenges, and opportunities," *IEEE Internet Things J.*, vol. 10, no. 21, pp. 18961–18970, Nov. 2023, doi: 10.1109/JIOT.2023.3277923.
[79] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed., Newton, MA, USA: O'Reilly Media, Jan. 2015.
[80] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Blockchain applications for Industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019.
[81] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[82] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[83] Y. Jiang, Y. Zhong, and X. Ge, "Smart contract-based data commodity transactions for industrial Internet of Things," *IEEE Access*, vol. 7, pp. 180856–180866, 2019.
[84] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, "Blockchain assisted secure data sharing model for Internet of Things based smart industries," *IEEE Trans. Rel.*, vol. 71, no. 1, pp. 348–358, Mar. 2022, doi: 10.1109/TR.2020.3047833.
[85] H. Yang, B. Bao, C. Li, Q. Yao, A. Yu, J. Zhang, and Y. Ji, "Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2419–2431, Feb. 2022, doi: 10.1109/JIOT.2021.3097440.
[86] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE EUROCON 17th Int. Conf. Smart Technol.*, Ohrid, Macedonia, Jul. 2017, pp. 763–768.
[87] N. Mohamed, J. Al-Jaroodi, and S. Lazarova-Molnar, "Leveraging the capabilities of Industry 4.0 for improving energy efficiency in smart factories," *IEEE Access*, vol. 7, pp. 18008–18020, 2019.
[88] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in Industry 4.0 networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2964–2973, Apr. 2021.
[89] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.
[90] A. E. C. Mondragon, C. E. C. Mondragon, and E. S. Coronado, "Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry," in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Chiba, Japan, Apr. 2018, pp. 1300–1303.
[91] C. Zhang, G. Zhou, H. Li, and Y. Cao, "Manufacturing blockchain of things for the configuration of a Data- and knowledge-driven digital twin manufacturing cell," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11884–11894, Dec. 2020, doi: 10.1109/JIOT.2020.3005729.
[92] J. Leng, S. Ye, M. Zhou, J. L. Zhao, Q. Liu, W. Guo, W. Cao, and L. Fu, "Blockchain-secured smart manufacturing in Industry 4.0: A survey," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 1, pp. 237–252, Jan. 2021, doi: 10.1109/tsmc.2020.3040789.
[93] H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," *IEEE Access*, vol. 7, pp. 41426–41444, 2019.
[94] Y. Zuo and Z. Qi, "A blockchain-based IoT framework for oil field remote monitoring and control," *IEEE Access*, vol. 10, pp. 2497–2514, 2022, doi: 10.1109/ACCESS.2021.3139582.
[95] A. de Villiers and P. Cuffe, "A three-tier framework for understanding disruption trajectories for blockchain in the electricity industry," *IEEE Access*, vol. 8, pp. 65670–65682, 2020.
[96] O. Alao and P. Cuffe, "Implementing contract-for-difference arrangements for hedging electricity price risks of renewable generators on a blockchain marketplace," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5679–5688, Apr. 2023, doi: 10.1109/TII.2022.3185661.
[97] T. Fernández-Caramés and P. Fraga-Lamas, "Design of a fog computing, blockchain and IoT-based continuous glucose monitoring system for crowdsourcing mHealth," in *Proc. 5th Int. Electron. Conf. Sensors Appl.*, vol. 55, Nov. 2018, p. 37.
[98] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar, and R. A. Khan, "A systematic analysis on blockchain integration with healthcare domain: Scope and challenges," *IEEE Access*, vol. 9, pp. 84666–84687, 2021.
[99] S. Liu, L. Chen, G. Wu, H. Wang, and H. Yu, "Blockchain-backed searchable proxy signcryption for cloud personal health records," *IEEE Trans. Services Comput.*, vol. 16, no. 5, pp. 3210–3223, Oct. 2023, doi: 10.1109/TSC.2023.3272770.
[100] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-enabled fine-grained searchable encryption with cloud–edge computing for electronic health records sharing," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 18414–18425, Oct. 2023, doi: 10.1109/jiot.2023.3279893.
[101] R. Gupta, P. Bhattacharya, S. Tanwar, N. Kumar, and S. Zeadally, "GaRuDa: A blockchain-based delivery scheme using drones for healthcare 5.0 applications," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 60–66, Dec. 2021, doi: 10.1109/IOTM.001.2100045.
[102] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov./Dec. 2016, pp. 1–6.
[103] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," *PLoS ONE*, vol. 11, no. 10, pp. 1–27, 2016.
[104] J. E. Kasten, "Engineering and manufacturing on the blockchain: A systematic review," *IEEE Eng. Manag. Rev.*, vol. 48, no. 1, pp. 31–47, 1st Quart., 2020.
[105] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020.
[106] *European Blockchain Services Infrastructure (EBSI)*. Accessed: Apr. 23, 2024. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home
[107] E. Tan, E. Lerouge, J. Du Caju, and D. Du Seuil, "Verification of education credentials on European blockchain services infrastructure (EBSI): Action research in a cross-border use case between Belgium and Italy," *Big Data Cognit. Comput.*, vol. 7, no. 2, p. 79, Apr. 2023, doi: 10.3390/bdcc7020079.
[108] *United Manufacturing Hub*. Accessed: Apr. 24, 2024. [Online]. Available: https://learn.umh.app/course/the-unified-namespace-as-the-strongest-architectural-proposal-for-industry-4-0/
[109] J. Koomey, K. Brill, P. Turner, J. Stanley, and B. Taylor, "A simple model for determining true total cost of ownership for data centers," Uptime Inst., New York, NY, USA, White Paper, Jan. 2007, vol. 2. [Online]. Available: https://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/(TUI3011B)SimpleModelDeterminingTrueTCO.pdf
[110] S. G. Middleton and M. Marden, "Deploying an effective server life-cycle strategy will minimize costs: Leasing is a valuable tool," IDC, Framingham, MA, USA, White Paper, Jan. 2015. [Online]. Available: https://i.dell.com/sites/csdocuments/Learn_Docs/pl/idc-whitepaper-server-leasing.pdf
[111] T. Locher, S. Obermeier, and Y. A. Pignolet, "When can a distributed ledger replace a trusted third party?" in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1069–1077.
[112] Y. Jin, "Introduction to hardware security," *Electronics*, vol. 4, no. 4, pp. 763–784, Oct. 2015.
[113] T. M. Fernández-Caramés and P. Fraga-Lamas, "Use case based blended teaching of IIoT cybersecurity in the Industry 4.0 era," *Appl. Sci.*, vol. 10, no. 16, p. 5607, Aug. 2020.
[114] *Ethereum Official Web Page*. Accessed: Sep. 13, 2023. [Online]. Available: https://www.ethereum.org
[115] *Ripple's Official Web Page* Accessed: Sep. 13, 2023. [Online]. Available: https://www.ripple.com
[116] *EWF's Official Web Page*. Accessed: Sep. 13, 2023. [Online]. Available: http://energyweb.org
[117] *Corda's Official Web Page*. Accessed: Sep. 13, 2023. [Online]. Available: https://www.corda.net
[118] *Hyperledger Fabric Official Web Page* Accessed: Sep. 13, 2023. [Online]. Available: https://www.hyperledger.org/projects/fabric
[119] S. Fan, H. Zhang, Y. Zeng, and W. Cai, "Hybrid blockchain-based resource trading system for federated learning in edge computing," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2252–2264, Feb. 2021.
[120] S. S. Nabil, M. S. A. Pran, A. A. Al Haque, N. R. Chakraborty, M. J. M. Chowdhury, and M. S. Ferdous, "Blockchain-based COVID vaccination registration and monitoring," *Blockchain: Res. Appl.*, vol. 3, no. 4, Dec. 2022, Art. no. 100092, doi: 10.1016/j.bcra.2022.100092.

[121] G. Subramanian, A. S. Thampy, N. V. Ugwuoke, and B. Ramnani, "Crypto pharmacy—Digital medicine: A mobile application integrated with hybrid blockchain to tackle the issues in pharma supply chain," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 26–37, 2021.

[122] *Monero's Official Web Page*. Accessed: Jul. 13, 2023. [Online]. Available: https://getmonero.org

[123] *Litecoin Official Web Page*. Accessed: Jul. 13, 2023. [Online]. Available: https://litecoin.com

[124] *Multichain White Paper*. Accessed: Jul. 13, 2023. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[125] Y. Yan, B. Duan, Y. Zhong, and X. Qu, "Blockchain technology in the Internet plus: The collaborative development of power electronic devices," in *Proc. IECON 43rd Annu. Conf. IEEE Ind. Electron. Soc.*, Beijing, China, Oct. 2017, pp. 922–927.

[126] F. Zhang, M. Liu, and W. Shen, "Operation modes of smart factory for high-end equipment manufacturing in the Internet and big data era," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Banff, AB, Canada, Oct. 2017, pp. 152–157.

[127] S. Guo, X. Sun, and H. K. S. Lam, "Applications of blockchain technology in sustainable fashion supply chains: Operational transparency and environmental efforts," *IEEE Trans. Eng. Manag.*, vol. 70, no. 4, pp. 1312–1328, Apr. 2023.

[128] World Economic Forum. *These Facts Show How Unsustainable the Fashion Industry IS*. Accessed: Jul. 13, 2023. [Online]. Available: https://www.weforum.org/agenda/2020/01/fashion-industry-carbon-unsustainable-environment-pollution/

[129] C. Stoll, L. Klaaßen, and U. Gallersdörfer, "The carbon footprint of Bitcoin," *Joule*, vol. 3, no. 7, pp. 1647–1661, Jul. 2019.

[130] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. 35th Annu. Cryptol. Conf.*, Aug. 2015, pp. 585–605.

[131] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[132] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[133] Z. Zhou, M. Xie, T. Zhu, W. Xu, P. Yi, Z. Huang, Q. Zhang, and S. Xiao, "EEP2P: An energy-efficient and economy-efficient P2P network protocol," in *Proc. Int. Green Comput. Conf.*, Dallas, TX, USA, Nov. 2014, pp. 1–6.

[134] L. Sharifi, N. Rameshan, F. Freitag, and L. Veiga, "Energy efficiency dilemma: P2P-cloud vs. datacenter," in *Proc. IEEE 6th Int. Conf. Cloud Comput. Technol. Sci.*, Singapore, Dec. 2014, pp. 611–619.

[135] I. Froiz-Míguez, P. Fraga-Lamas, and T. M. Fernández-Caramés, "Decentralized P2P Broker for M2M and IoT Applications," *Proceedings*, vol. 54, no. 24, p. 24, 2020.

[136] P. Zhang and B. E. Helvik, "Towards green P2P: Analysis of energy consumption in P2P and approaches to control," in *Proc. Int. Conf. High Perform. Comput. Simul. (HPCS)*, Madrid, Spain, Jul. 2012, pp. 336–342.

[137] S. Miyake and M. Bandai, "Energy-efficient mobile P2P communications based on context awareness," in *Proc. IEEE 27th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Barcelona, Spain, Mar. 2013, pp. 918–923.

[138] C.-C. Liao, S.-M. Cheng, and M. Domb, "On designing energy efficient Wi-Fi P2P connections for Internet of Things," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.

[139] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain technology toward green IoT: Opportunities and challenges," *IEEE Netw.*, vol. 34, no. 4, pp. 263–269, Jul. 2020.

[140] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Blockchain empowered wireless power transfer for green and secure Internet of Things," *IEEE Netw.*, vol. 33, no. 6, pp. 164–171, Nov. 2019.

[141] J. D. Bruce. *The Mini-Blockchain Scheme*. Accessed: Oct. 11, 2022. [Online]. Available: https://cryptonite.info/files/mbc-scheme-rev3.pdf

[142] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[143] M. Suárez-Albela, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, no. 9, p. 1978, Aug. 2017.

[144] M. Suárez-Albela, P. Fraga-Lamas, L. Castedo, and T. M. Fernández-Caramés, "Clock frequency impact on the performance of high-security cryptographic cipher suites for energy-efficient resource-constrained IoT devices," *Sensors*, vol. 19, no. 1, p. 15, Dec. 2018.

[145] A. Tidrea, A. Korodi, and I. Silea, "Elliptic curve cryptography considerations for securing automation and SCADA systems," *Sensors*, vol. 23, no. 5, p. 2686, Mar. 2023.

[146] S. K. Mishra, D. Puthal, B. Sahoo, S. Sharma, Z. Xue, and A. Y. Zomaya, "Energy-efficient deployment of edge dataenters for mobile clouds in sustainable IoT," *IEEE Access*, vol. 6, pp. 56587–56597, 2018.

[147] M. Guo, L. Li, and Q. Guan, "Energy-efficient and delay-guaranteed workload allocation in IoT-edge-cloud computing systems," *IEEE Access*, vol. 7, pp. 78685–78697, 2019.

[148] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based forward supply chain and waste management for COVID-19 medical equipment and supplies," *IEEE Access*, vol. 9, pp. 44905–44927, 2021.

[149] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020.

[150] R. Rahmani, J. Karimi, P. R. Resende, J. C. C. Abrantes, and S. I. Lopes, "Overview of selective laser melting for Industry 5.0: Toward customizable, sustainable, and human-centric technologies," *Machines*, vol. 11, no. 5, p. 522, May 2023.

[151] R. Winkler-Goldstein, F. Imbault, T. Usländer, and H. de la Gastine, "Fractal production reprogramming 'Industrie 4.,' around resource and energy efficiency?" in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I&CPS Europe)*, Palermo, Italy, Jun. 2018, pp. 1–5.

[152] S. Trouton, M. Vitale, and J. Killmeyer. (Nov. 2016). *3D Opportunity for Blockchain*. Deloitte Insights. Accessed: Oct. 11, 2022. [Online]. Available: https://www2.deloitte.com/insights/us/en/focus/3d-opportunity/3d-printing-blockchain-in-manufacturing.html

[153] *3D-TOKEN Official Web Site*. Accessed: Oct. 11, 2022. [Online]. Available: https://3d-token.com

[154] J. McCarter, U. S. Department of Navy (DON). (Jun. 2017). *DON Innovator Embraces a New Disruptive Technology: Blockchain*. Accessed: Oct. 11, 2022. [Online]. Available: http://www.secnav.navy.mil/innovation/Pages/2017/06/BlockChain.aspx

[155] J. J. Freer, R. P. Messmer, A. Rangaranjan, and D. R. Safford, "Methods and systems for implementing distributed ledger manufacturing history," U.S. Patent 0 713 203, Jun. 21, 2018.

[156] *LINK3D Official Web Site*. Accessed: Oct. 11, 2022. [Online]. Available: https://solution.link3d.co

[157] M. Holland, J. Stjepandić, and C. Nigischer, "Intellectual property protection of 3D print supply chain with blockchain technology," in *Proc. IEEE Int. Conf. Eng., Technol. Innov.*, Jun. 2018, pp. 1–8.

[158] *NXT's Official Web Page*. Accessed: Sep. 13, 2023. [Online]. Available: https://nxtplatform.org

[159] *Counterparty Official Web Page*. Accessed: Sep. 13, 2023. [Online]. Available: wwww.counterparty.io

[160] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy blockchain oracles: Review, comparison, and open research challenges," *IEEE Access*, vol. 8, pp. 85675–85685, 2020.

[161] L. Liyuan, H. Meng, Z. Yiyun, and P. Reza, "E^2C-chain: A two-stage incentive education employment and skill certification blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 140–147.

[162] N. Nair, A. K. Dalal, A. Chhabra, and N. Giri, "Edu-coin: A proof of stake implementation of a decentralized skill validation application," in *Proc. Int. Conf. Nascent Technol. Eng. (ICNTE)*, Jan. 2019, pp. 1–4.

[163] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020.

[164] A. Vidal-Balea, O. Blanco-Novoa, P. Fraga-Lamas, M. Vilar-Montesinos, and T. M. Fernández-Caramés, "Creating collaborative augmented reality experiences for Industry 4.0 training and assistance applications: Performance evaluation in the shipyard of the future," *Appl. Sci.*, vol. 10, no. 24, p. 9073, Dec. 2020.

[165] P. Zawadzki, K. Zywicki, P. Bun, and F. Górski, "Employee training in an intelligent factory using virtual reality," *IEEE Access*, vol. 8, pp. 135110–135117, 2020.

[166] F. Loch, F. Quint, and I. Brishtel, "Comparing video and augmented reality assistance in manual assembly," in *Proc. 12th Int. Conf. Intell. Environments (IE)*, London, U.K., Sep. 2016, pp. 147–150.
[167] H. Cave, "VR in…the factory of the future," *Eng. Technol.*, vol. 11, no. 3, p. 4447, Apr. 2016.
[168] M. Schneider, J. Rambach, and D. Stricker, "Augmented reality based on edge computing using the example of remote live support," in *Proc. 18th Annu. Int. Conf. Ind. Technol.*, Toronto, ON, Canada, Mar. 2017, pp. 121–282.
[169] A. C. Boud, C. Baber, and S. J. Steiner, "Virtual reality: A tool for assembly?" *Presence, Teleoperators Virtual Environ.*, vol. 9, no. 5, pp. 486–496, Oct. 2000.
[170] C. Shin, B.-H. Park, G.-M. Jung, and S.-H. Hong, "Mobile augmented reality mashup for furture IoT environment," in *Proc. IEEE 11th Int. Conf Ubiquitous Intell. Comput. IEEE 11th Int. Conf Autonomic Trusted Comput. IEEE 14th Int. Conf Scalable Comput. Commun. Associated Workshops*, Bali, Indonesia, Dec. 2014, pp. 888–891.
[171] Q. He, "Research and application of virtual reality technology in mechanical maintenance," in *Proc. Int. Conf. Adv. Technol. Design Manuf. (ATDM)*, Beijing, China, Nov. 2010, pp. 256–258.
[172] M. Aleksy, E. Vartiainen, V. Domova, and M. Naedele, "Augmented reality for improved service delivery," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl.*, Victoria, BC, Canada, May 2014, pp. 382–389.
[173] S. Baranski and J. Konorski, "Mitigation of fake data content poisoning attacks in NDN via blockchain," in *Proc. 30th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2020, pp. 1–6.
[174] L. Xiao, W. Huang, Y. Xie, W. Xiao, and K.-C. Li, "A blockchain-based traceable IP copyright protection algorithm," *IEEE Access*, vol. 8, pp. 49532–49542, 2020.
[175] *RNDR Official Web Site*. Accessed: Oct. 11, 2023. [Online]. Available: https://rendertoken.com
[176] *Decentraland Official Web Site*. Accessed: Oct. 11, 2023. [Online]. Available: https://decentraland.org
[177] *VibeHub Official Web Site*. Accessed: Oct. 11, 2023. [Online]. Available: https://www.vibehub.io
[178] Bitcoin Magazine New. *The Lucyd Story: Augmented Eyeware Backed The Blockchain*. Accessed: Oct. 11, 2023. [Online]. Available: https://bitcoinmagazine.com/articles/lucyd-story-augmented-eyeware-backed-blockchain/
[179] *Matryx Official Web Site*. Accessed: Oct. 11, 2023. [Online]. Available: https://nanome.ai/matryx/
[180] *Verses Official Web Site*. Accessed: Oct. 11, 2023. [Online]. Available: https://www.verses.io
[181] R. Harrison, D. Vera, and B. Ahmad, "Engineering methods and tools for CyberPhysical automation systems," *Proc. IEEE*, vol. 104, no. 5, pp. 973–985, May 2016.
[182] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and Industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.
[183] C. Klötzer, J. Weißenborn, and A. Pflaum, "The evolution of cyber-physical systems as a driving force behind digital transformation," in *Proc. IEEE Conf. Bus. Inform.*, Thessaloniki, Greece, Jul. 2017, pp. 5–14.
[184] M. Ya. Afanasev, Y. V. Fedosov, A. A. Krylova, and S. A. Shorokhov, "An application of blockchain and smart contracts for machine-to-machine communications in cyber-physical production systems," in *Proc. IEEE Ind. Cyber-Phys. Syst. (ICPS)*, St. Petersburg, Russia, May 2018, pp. 13–19.
[185] A. J. M. Milne, A. Beckmann, and P. Kumar, "Cyber-physical trust systems driven by blockchain," *IEEE Access*, vol. 8, pp. 66423–66437, 2020.
[186] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo, "Blockchain-enabled CyberPhysical systems: A review," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4023–4034, Mar. 2021.
[187] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.
[188] M. Isaja and J. Soldatos, "Distributed ledger technology for decentralization of manufacturing processes," in *Proc. IEEE Ind. Cyber-Phys. Syst. (ICPS)*, May 2018, pp. 696–701.
[189] Z. Liang, K. Zhou, R. Gao, and K. Gao, "Special equipment safety supervision system architecture based on blockchain technology," *Appl. Sci.*, vol. 10, no. 20, p. 7344, Oct. 2020.
[190] C. Roy, S. Misra, and S. Pal, "Blockchain-enabled safety-as-a-service for industrial IoT applications," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 19–23, Jun. 2020.
[191] T. M. Fernández-Caramés, I. Froiz-Míguez, and P. Fraga-Lamas, "An IoT and blockchain based system for monitoring and tracking real-time occupancy for COVID-19 public safety," *Eng. Proc.*, vol. 2, no. 67, p. 30, Nov. 2020.
[192] I. Froiz-Míguez, P. Fraga-Lamas, J. Varela-Barbeito, and T. M. Fernández-Caramés, "LoRaWAN and blockchain based safety and health monitoring system for Industry 4.0 operators," *Proceedings*, vol. 42, no. 1, p. 77, Nov. 2019.
[193] S. Alacam and A. Sencer, "Using blockchain technology to foster collaboration among shippers and carriers in the trucking industry: A design science research approach," *Logistics*, vol. 5, no. 2, p. 37, Jun. 2021.
[194] L. Ouyang, Y. Yuan, and F.-Y. Wang, "A blockchain-based framework for collaborative production in distributed and social manufacturing," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Informat. (SOLI)*, Zhengzhou, China, Nov. 2019, pp. 76–81.
[195] T. M. Fernández-Caramés and P. Fraga-Lamas, "Teaching and learning IoT cybersecurity and vulnerability assessment with shodan through practical use cases," *Sensors*, vol. 20, no. 11, p. 3048, May 2020.
[196] A. Mittal, M. P. Gupta, M. Chaturvedi, S. R. Chansarkar, and S. Gupta, "Cybersecurity enhancement through blockchain training (CEBT)—A serious game approach," *Int. J. Inf. Manage. Data Insights*, vol. 1, no. 1, Apr. 2021, Art. no. 100001.
[197] H. Andreasson, A. Bouguerra, M. Cirillo, D. N. Dimitrov, D. Driankov, L. Karlsson, A. J. Lilienthal, F. Pecora, J. P. Saarinen, A. Sherikov, and T. Stoyanov, "Autonomous transport vehicles: Where we are and what is missing," *IEEE Robot. Autom. Mag.*, vol. 22, no. 1, pp. 64–75, Mar. 2015.
[198] P. Akella, M. Peshkin, E. Colgate, W. Wannasuphoprasit, N. Nagesh, J. Wells, S. Holland, T. Pearson, and B. Peacock, "Cobots for the automobile assembly line," in *Proc. IEEE Int. Conf. Robot. Autom.*, May 1999, pp. 728–733.
[199] S. Robla-Gómez, V. M. Becerra, J. R. Llata, E. González-Sarabia, C. Torre-Ferrero, and J. Pérez-Oria, "Working together: A review on safe human-robot collaboration in industrial environments," *IEEE Access*, vol. 5, pp. 26754–26773, 2017.
[200] *Kollmorgen Official Web Page*. Accessed: Sep. 11, 2023. [Online]. Available: http://www.kollmorgen.com
[201] *Atlas Copco Official Web Page*. Accessed: Sep. 11, 2023. [Online]. Available: http://www.atlascopco.com
[202] E. Pontes, A. Moradbeikie, R. Azevedo, C. Jesus, and S. I. Lopes, "Ergonomic posture assessment and tracking for industrial cyber-physical-human systems: A case study in the heavy metalworking industry," in *Proc. Hum. Aspects Adv. Manuf. AHFE Int. Conf.*, vol. 80, W. Karwowski and S. Trzcielinski, Eds., Orlando, FL, USA: AHFE International, 2023, pp. 1–10.
[203] *Kiva Systems (Now Amazon Robotics) Official Web Page*. Accessed: Sep. 11, 2023. [Online]. Available: http://www.kivasystems.com/
[204] A. S. Vempati, M. Kamel, N. Stilinovic, Q. Zhang, D. Reusser, I. Sa, J. Nieto, R. Siegwart, and P. Beardsley, "PaintCopter: An autonomous UAV for spray painting on three-dimensional surfaces," *IEEE Robot. Autom. Lett.*, vol. 3, no. 4, pp. 2862–2869, Oct. 2018.
[205] E. H. C. Harik, F. Guérin, F. Guinand, J. F. Brethé, and H. Pelvillain, "UAV-UGV cooperation for objects transportation in an industrial area," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Seville, Spain, Mar. 2015, p. 552.
[206] J. Nikolic, M. Burri, J. Rehder, S. Leutenegger, C. Huerzeler, and R. Siegwart, "A UAV system for inspection of industrial facilities," in *Proc. Aerosp. Conf.*, Big Sky, MT, USA, Mar. 2013, pp. 1–8.
[207] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," in *Proc. Workshop Res., Educ. Develop. Unmanned Aerial Syst. (RED-UAS)*, Linkoping, Sweden, Oct. 2017, pp. 84–89.
[208] N. Pathak, A. Mukherjee, and S. Misra, "AerialBlocks: Blockchain-enabled UAV virtualization for industrial IoT," *IEEE Internet Things Mag.*, vol. 4, no. 1, pp. 72–77, Mar. 2021.
[209] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, Apr. 2021.

[210] D. Wang and X. Zhang, "Secure ride-sharing services based on a consortium blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2976–2991, Feb. 2021.

[211] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, May 2018.

[212] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[213] A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, "Blockchain based data and energy trading in Internet of electric vehicles," *IEEE Access*, vol. 9, pp. 7000–7020, 2021.

[214] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[215] X. Chen, T. Zhang, W. Ye, Z. Wang, and H. H. Iu, "Blockchain-based electric vehicle incentive system for renewable energy consumption," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 396–400, Jan. 2021.

[216] J. Chen and Y. Xue, "Bootstrapping a blockchain based ecosystem for big data exchange," in *Proc. IEEE Int. Congr. Big Data*, Honolulu, HI, USA, Jun. 2017, pp. 460–463.

[217] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4000–4015, May 2020.

[218] N. Abdullah, A. Hakansson, and E. Moradian, "Blockchain based approach to enhance big data authentication in distributed environment," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Milan, Italy, Jul. 2017, pp. 887–892.

[219] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, and M. Guo, "Making big data open in edges: A resource-efficient blockchain-based approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 870–882, Apr. 2019.

[220] Y. Wu, G. J. Mendis, and J. Wei, "DDLPF: A practical decentralized deep learning paradigm for Internet-of-Things applications," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9740–9752, Jun. 2021.

[221] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5926–5937, Apr. 2021.

[222] P. Zhang, H. Sun, J. Situ, C. Jiang, and D. Xie, "Federated transfer learning for IIoT devices with low computing power based on blockchain and edge computing," *IEEE Access*, vol. 9, pp. 98630–98638, 2021.

[223] W. A. A. Cotta, S. I. Lopes, and R. F. Vassallo, "Towards the cognitive factory in Industry 5.0: From concept to implementation," *Smart Cities*, vol. 6, no. 4, pp. 1901–1921, Aug. 2023.

[224] K. Chung, H. Yoo, D. Choe, and H. Jung, "Blockchain network based topic mining process for cognitive manufacturing," *Wireless Pers. Commun.*, vol. 105, no. 2, pp. 583–597, Mar. 2019.

[225] C. Hur, S. Kim, Y. Kim, and J. Eom, "Changes of cyber-attacks techniques and patterns after the fourth industrial revolution," in *Proc. 5th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Prague, Czech Republic, Nov. 2017, pp. 69–74.

[226] P. Fraga-Lamas and T. M. Fernández-Caramés, "Reverse engineering the communications protocol of an RFID public transportation card," in *Proc. IEEE Int. Conf. RFID (RFID)*, Phoenix, AZ, USA, May 2017, pp. 30–35.

[227] T. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "Reverse engineering and security evaluation of commercial tags for RFID-based IoT applications," *Sensors*, vol. 17, no. 1, p. 28, Dec. 2016.

[228] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "A methodology for evaluating security in commercial RFID systems, radio frequency identification," in *Radio Frequency Identification*, 1st ed., P. C. Crepaldi and T. C. Pimenta, Eds. Rijeka, Croatia: InTech, 2017.

[229] R. W. Ahmad, H. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Blockchain applications and architectures for port operations and logistics management," *Res. Transp. Bus. Manage.*, vol. 41, Dec. 2021, Art. no. 100620, doi: 10.1016/j.rtbm.2021.100620.

[230] A. Raja Santhi and P. Muthuswamy, "Influence of blockchain technology in manufacturing supply chain and logistics," *Logistics*, vol. 6, no. 1, p. 15, Feb. 2022, doi: 10.3390/logistics6010015.

[231] G. T. S. Ho, Y. M. Tang, K. Y. Tsang, V. Tang, and K. Y. Chau, "A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management," *Expert Syst. Appl.*, vol. 179, Oct. 2021, Art. no. 115101, doi: 10.1016/j.eswa.2021.115101.

[232] *Association of Supply Chain Management*. Accessed: Mar. 15, 2024. [Online]. Available: https://www.ascm.org/lp/reverse-logistics/

[233] J. Wu, "Sustainable development of green reverse logistics based on blockchain," *Energy Rep.*, vol. 8, pp. 11547–11553, Nov. 2022, doi: 10.1016/j.egyr.2022.08.219.

[234] P. W. Khan, I. Bareche, and T. Wuest, "Towards Industry 5.0: Empowering SMEs with blockchain-based supplier collaboration network," *Advances in Production Management Systems*, vol. 689, E. Alfnes, A. Romsdal, J. O. Strandhagen, G. von Cieminski, and D. Romero, Eds., Cham, Switzerland: Springer, 2023.

[235] P. Araújo, A. M. R. da Cruz, and S. I. Lopes, "IoT and blockchain technologies for process traceability in the shipbuilding industry," in *Proc. 17th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Madrid, Spain, Jun. 2022, pp. 1–6, doi: 10.23919/CISTI54924.2022.9820491.

[236] M. Kuhn, F. Funk, G. Zhang, and J. Franke, "Blockchain-based application for the traceability of complex assembly structures," *J. Manuf. Syst.*, vol. 59, pp. 617–630, Apr. 2021, doi: 10.1016/j.jmsy.2021.04.013.

[237] E. Cruz and A. Rosado da Cruz, "Using blockchain to implement traceability on fishery value chain," in *Proc. 15th Int. Conf. Softw. Technol.*, Jul. 2020, pp. 501–508.

[238] N. Chhikara, "Importance of traceability in food supply chain for brand protection and food safety systems implementation," *Ann. Biol.*, vol. 34, pp. 111–118, Jan. 2018.

[239] L. Alves, E. F. Cruz, S. I. Lopes, P. M. Faria, and A. M. R. da Cruz, "Towards circular economy in the textiles and clothing value chain through blockchain technology and IoT: A review," *Waste Manage. Res., J. Sustain. Circular Economy*, vol. 40, no. 1, pp. 3–23, Jan. 2022, doi: 10.1177/0734242x211052858.

[240] L. Alves, T. Carvalhido, E. Cruz, and A. R. da Cruz, "Using blockchain to trace PDO/PGI/TSG products," in *Proc. 23rd Int. Conf. Enterprise Inf. Syst.*, 2021, pp. 368–376, doi: 10.5220/0010482503680376.

[241] G. Varavallo, G. Caragnano, F. Bertone, L. Vernetti-Prot, and O. Terzo, "Traceability platform based on green blockchain: An application case study in dairy supply chain," *Sustainability*, vol. 14, no. 6, p. 3321, Mar. 2022, doi: 10.3390/su14063321.

[242] R. Dias, H. Cardoso, E. F. Cruz, and A. M. R. da Cruz, "A blockchain-based platform for reliably tracing political contacts," in *Proc. 16th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Chaves, Portugal, Jun. 2021, pp. 1–6, doi: 10.23919/CISTI52073.2021.9476327.

[243] W. Shang, M. Liu, W. Lin, and M. Jia, "Tracing the source of news based on blockchain," in *Proc. IEEE/ACIS 17th Int. Conf. Comput. Inf. Sci. (ICIS)*, Singapore, Jun. 2018, pp. 377–381, doi: 10.1109/ICIS.2018.8466516.

[244] M. J. Muñoz-Torres, M. Á. Fernández-Izquierdo, J. M. Rivera-Lirio, I. Ferrero-Ferrero, and E. Escrig-Olmedo, "Sustainable supply chain management in a global context: A consistency analysis in the textile industry between environmental management practices at company level and sectoral and global environmental challenges," *Environ., Develop. Sustainability*, vol. 23, no. 3, pp. 3883–3916, Mar. 2021, doi: 10.1007/s10668-020-00748-4.

[245] A. Rosado da Cruz and E. Cruz, "Blockchain-based traceability platforms as a tool for sustainability," in *Proc. 22nd Int. Conf. Enterprise Inf. Syst.*, 2020, p. 33037, doi: 10.5220/0009463803300337.

[246] L. Alves, E. F. Cruz, and A. M. R. Da Cruz, "Tracing sustainability indicators in the textile and clothing value chain using blockchain technology," in *Proc. 17th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2022, pp. 1–7, doi: 10.23919/CISTI54924.2022.9820241.

[247] I. J. Scott, M. de Castro Neto, and F. L. Pinheiro, "Bringing trust and transparency to the opaque world of waste management with blockchain: A polkadot parathread application," *Comput. Ind. Eng.*, vol. 182, Aug. 2023, Art. no. 109347, doi: 10.1016/j.cie.2023.109347.

[248] L. Fernandes, A. M. Rosado da Cruz, E. F. Cruz, and S. I. Lopes, "A review on adopting blockchain and IoT technologies for fostering the circular economy in the electrical and electronic equipment value chain," *Sustainability*, vol. 15, no. 5, p. 4574, Mar. 2023.

[249] United Nations Framework Convention on Climate Change (UNFCCC). (2021). *What is the Kyoto Protocol*. [Online]. Available: https://unfccc.int/kyotoprotocol

[250] Carbon Market Institute. (2021). *FACT SHEET 2 Carbon Markets. Carbon Markets—An Overview*. [Online]. Available: https://carbonmarketinstitute.org/app/uploads/2021/06/CMIFactSheet2Carbon-Markets-101.pdf
[251] A. Sipthorpe, S. Brink, T. Van Leeuwen, and I. Staffell, "Blockchain solutions for carbon markets are nearing maturity," *One Earth*, vol. 5, no. 7, pp. 779–791, Jul. 2022, doi: 10.1016/j.oneear.2022.06.004.
[252] A. Vilkov and G. Tian, "Blockchain's scope and purpose in carbon markets: A systematic literature review," *Sustainability*, vol. 15, no. 11, p. 8495, May 2023, doi: 10.3390/su15118495.
[253] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, blockchain and shared economy applications," *Proc. Comput. Sci.*, vol. 98, pp. 461–466, Jan. 2016.
[254] D. Patel, B. Britto, S. Sharma, K. Gaikwad, Y. Dusing, and M. Gupta, "Carbon credits on blockchain," in *Proc. Int. Conf. Innov. Trends Inf. Technol. (ICITIIT)*, Kottayam, India, Feb. 2020, pp. 1–5, doi: 10.1109/ICITIIT49094.2020.9071536.
[255] S.-K. Kim and J.-H. Huh, "Blockchain of carbon trading for UN sustainable development goals," *Sustainability*, vol. 12, no. 10, p. 4021, May 2020, doi: 10.3390/su12104021.
[256] D. Effah, B. Chunguang, F. Appiah, B. L. Y. Agbley, and M. Quayson, "Carbon emission monitoring and credit trading: The blockchain and IoT approach," in *Proc. 18th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP)*, Chengdu, China, Dec. 2021, pp. 106–109, doi: 10.1109/ICCWAMTIP53232.2021.9674144.
[257] L. Francisco, R. Bonacin, and F. De Franco Rosa, "A study on the application of blockchain in carbon trading systems," in *Proc. IEEE/ACS 19th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Abu Dhabi, United Arab Emirates, Dec. 2022, pp. 1–6, doi: 10.1109/AICCSA56895.2022.10017504.
[258] X. Yu and X. Wang, "Research on carbon-trading model of urban public transport based on blockchain technology," *Energies*, vol. 16, no. 6, p. 2606, Mar. 2023, doi: 10.3390/en16062606.
[259] *European Commission, Renewable Energy Targets, Renewable Energy Directive 2018/2001/EU*. Accessed: Mar. 15, 2024. [Online]. Available: https://energy.ec.europa.eu/topics/renewable-energy/renewable-energy-directive-targets-and-rules/renewable-energy-targetsen
[260] (Sep. 2020). *International REC Standard Foundation, Understanding EAC Schemes and Roadmaps for Their Development, Report Submitted as Per the Agreement Between the I-REC Standard Foundation and the United Nations Development Program*. [Online]. Available: https://www.irecstandard.org/what-are-recs/
[261] Q. Zhang, T. Xu, D. Wang, Z. Liu, C. Cheng, S. Zheng, and G. Wang, "Study of traceability system of renewable energy power trading based on blockchain technology," in *Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, Huaihua City, China, Jul. 2022, pp. 171–176, doi: 10.1109/ICBCTIS55569.2022.00047.
[262] C. Inês, P. L. Guilherme, M.-G. Esther, G. Swantje, H. Stephen, and H. Lars, "Regulatory challenges and opportunities for collective renewable energy prosumers in the EU," *Energy Policy*, vol. 138, Mar. 2020, Art. no. 111212, doi: 10.1016/j.enpol.2019.111212.
[263] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019, doi: 10.1016/j.rser.2018.10.014.
[264] M. Li, Z. Li, X. Huang, and T. Qu, "Blockchain-based digital twin sharing platform for reconfigurable socialized manufacturing resource integration," *Int. J. Prod. Econ.*, vol. 240, Oct. 2021, Art. no. 108223, doi: 10.1016/j.ijpe.2021.108223.
[265] J. Leng and P. Jiang, "Socialized manufacturing resources and interconnections," in *Social Manufacturing: Fundamentals and Applications* (Springer Series in Advanced Manufacturing). Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-319-72986-2_3.
[266] Y. Ezawa, S. Kakei, Y. Shiraishi, M. Mohri, and M. Morii, "Blockchain-based cross-domain authorization system for user-centric resource sharing," *Blockchain, Res. Appl.*, vol. 4, no. 2, Jun. 2023, Art. no. 100126, doi: 10.1016/j.bcra.2023.100126.
[267] E. Anaam, T. M. Ghazal, S.-C. Haw, H. M. Alzoubi, M. T. Alshurideh, and A. A. Mamun, "Utilization of blockchain technology in human resource management," in *Proc. IEEE 2nd Int. Conf. AI Cybersecurity (ICAIC)*, Houston, TX, USA, Feb. 2023, pp. 1–5, doi: 10.1109/ICAIC57335.2023.10044181.
[268] R. Kumar Singh, R. Mishra, S. Gupta, and A. A. Mukherjee, "Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda," *Comput. Ind. Eng.*, vol. 175, Jan. 2023, Art. no. 108854, doi: 10.1016/j.cie.2022.108854.
[269] P. Haren and D. Simchi-Levi. (2020). *How Coronavirus Could Impact the Global Supply Chain by Mid-March*. Harvard Bus. Review. Accessed: Feb. 2020. [Online]. Available: https://hbr.org/2020/02/how-coronavirus-could-impact-the-global-supply-chain-by-mid-march
[270] M. Kutzner and M. Rajal. (2020). *Shaping Sourcing and Procurement in a Post-COVID Environment*. Delloite. Accessed: Sep. 8, 2020. [Online]. Available: www2.deloitte.com/ch/en/pages/technology/articles/shaping-sourcing-and-procurement-in-a-post-covid-environment.html
[271] G. F. Frederico, "Towards a supply chain 4.0 on the post-COVID-19 pandemic: A conceptual and strategic discussion for more resilient supply chains," *Rajagiri Manage. J.*, vol. 15, no. 2, pp. 94–104, Sep. 2021, doi: 10.1108/ramj-08-2020-0047.
[272] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov. 2017.
[273] J. H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, p. 1923, Jul. 2017.
[274] Ó. Blanco-Novoa, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "An electricity price-aware open-source smart socket for the internet of energy," *Sensors*, vol. 17, no. 3, p. 643, Mar. 2017.
[275] T. M. Fernández-Caramés, "An intelligent power outlet system for the smart home of the Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Nov. 2015, Art. no. 214805.
[276] M. Suárez-Albela, P. Fraga-Lamas, T. Fernández-Caramés, A. Dapena, and M. González-López, "Home automation system based on intelligent transducer enablers," *Sensors*, vol. 16, no. 10, p. 1595, Sep. 2016.
[277] J. Pérez-Expósito, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "VineSens: An eco-smart decision-support viticulture system," *Sensors*, vol. 17, no. 3, p. 465, Feb. 2017.
[278] T. Fernández-Caramés and P. Fraga-Lamas, "Towards the internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected E-textiles," *Electronics*, vol. 7, no. 12, p. 405, Dec. 2018.
[279] H. Wang, O. L. Osen, G. Li, W. Li, H.-N. Dai, and W. Zeng, "Big data and industrial Internet of Things for the maritime industry in Northwestern Norway," in *Proc. TENCON IEEE Region 10 Conf.*, Nov. 2015, pp. 1–5.
[280] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, "A plug-and-play human-centered virtual TEDS architecture for the web of things," *Sensors*, vol. 18, no. 7, p. 2052, Jun. 2018.
[281] L. Shu, M. Mukherjee, M. Pecht, N. Crespi, and S. N. Han, "Challenges and research issues of data management in IoT for large-scale petrochemical plants," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2509–2523, Sep. 2018.
[282] O. Blanco-Novoa, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A cost-effective IoT system for monitoring indoor radon gas concentration," *Sensors*, vol. 18, no. 7, p. 2198, Jul. 2018.
[283] P. López-Iturri, E. Aguirre, L. Azpilicueta, J. Astrain, J. Villandangos, and F. Falcone, "Challenges in wireless system integration as enablers for indoor context aware environments," *Sensors*, vol. 17, no. 7, p. 1616, Jul. 2017.
[284] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *Proc. 21st Conf. Open Innov. Assoc. (FRUCT)*, Helsinki, Finland, Nov. 2017, pp. 321–329.
[285] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[286] C. Barreto, T. Eghtesad, S. Eisele, A. Laszka, A. Dubey, and X. Koutsoukos, "Cyber-attacks and mitigation in blockchain based transactive energy systems," in *Proc. IEEE Conf. Ind. Cyberphysical Syst. (ICPS)*, vol. 1, Tampere, Finland, Jun. 2020, pp. 129–136.
[287] Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and Industry 4.0: 360 degree comparison," *IEEE Access*, vol. 6, pp. 3585–3593, 2018.
[288] *Gridcoin Official Web Site*. Accessed: Oct. 11, 2023. [Online]. Available: https://gridcoin.us

[289] R. Sarbajna, C. F. Eick, and A. Laszka, "DEIMOSBC: A blockchain-based system for crowdsensing after natural disasters," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Paris, France, Sep. 2021, pp. 17–20, doi: 10.1109/BRAINS52497.2021.9569794.

[290] E. Samir, M. Azab, and Y. Jung, "Blockchain guided trustworthy interactions for distributed disaster management," in *Proc. IEEE 10th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Vancouver, BC, Canada, Oct. 2019, pp. 241–245, doi: 10.1109/IEMCON.2019.8936147.

[291] S. Ahmed, "A novel data security model of D2D communication using blockchain for disaster," in *Proc. Int. Conf. Comput. Sci., Inf. Technol. Eng. (ICCoSITE)*, Jakarta, Indonesia, Feb. 2023, pp. 319–324, doi: 10.1109/ICCoSITE57641.2023.10127771.

[292] N. H. Wasserman, "Blockchain-based data access environment for disaster risk Reduction," in *Proc. IEEE Global Humanitarian Technol. Conf. (GHTC)*, Santa Clara, CA, USA, Sep. 2022, pp. 273–276, doi: 10.1109/GHTC55712.2022.9910985.

[293] B. Liu, Y. Xin, and S. Dai, "Blockchain-based disaster recovery data storage and security auditing solution in multi-cloud environment," in *Proc. Int. Appl. Comput. Electromagn. Soc. Symp. (ACES-China)*, Xuzhou, China, Dec. 2022, pp. 1–4, doi: 10.1109/ACES-China56081.2022.10065296.

[294] M. Kaur, P. D. Kaur, and S. K. Sood, "BIoT (blockchain-based IoT) framework for disaster management," in *Proc. 12th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Noida, India, Jan. 2022, pp. 318–323, doi: 10.1109/Confluence52989.2022.9734193.

[295] P. Bai, S. Kumar, and K. Kumar, "Use of blockchain enabled IoT in insurance: A case study of calamity based crop insurance," in *Proc. 3rd Int. Conf. Intell. Comput. Instrum. Control Technol. (ICICICT)*, Kannur, India, Aug. 2022, pp. 1135–1141, doi: 10.1109/ICICICT54557.2022.9917659.

[296] Y. Wang, Z. Su, Q. Xu, R. Li, and T. H. Luan, "Lifesaving with RescueChain: Energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Vancouver, BC, Canada, May 2021, pp. 1–10, doi: 10.1109/INFOCOM42981.2021.9488719.

[297] P. H. A. P. Badarudin, A. T. Wan, and S. Phon-Amnuaisuk, "A blockchain-based assistance digital model for first responders and emergency volunteers in disaster response and recovery," in *Proc. 8th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Yogyakarta, Indonesia, Jun. 2020, pp. 1–5, doi: 10.1109/ICoICT49345.2020.9166389.

[298] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, and R. Li, "UAVs-aided delay-tolerant blockchain secure offline transactions in post-disaster vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12030–12043, Nov. 2022, doi: 10.1109/TVT.2022.3184965.

[299] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. Kumar R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Gener. Computer Syst.*, vol. 131, pp. 209–226, Jun. 2022, doi: 10.1016/j.future.2022.01.017.

[300] P. Bansal, R. Panchal, S. Bassi, and A. Kumar, "Blockchain for cybersecurity: A comprehensive survey," in *Proc. IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Gwalior, India, Apr. 2020, pp. 260–265, doi: 10.1109/CSNT48778.2020.9115738.

[301] R. Salama, F. Al-Turjman, C. Altrjman, S. Kumar, and P. Chaudhary, "A comprehensive survey of blockchain-powered cybersecurity—A survey," in *Proc. Int. Conf. Comput. Intell., Commun. Technol. Netw. (CICTN)*, Ghaziabad, India, Apr. 2023, pp. 774–777, doi: 10.1109/CICTN57981.2023.10141282.

[302] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani, *Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications*. Boca Raton, FL, USA: CRC Press, 2020.

[303] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021, doi: 10.1109/TII.2020.2998479.

[304] X. Wang, C. Xu, Z. Zhou, S. Yang, and L. Sun, "A survey of blockchain-based cybersecurity for vehicular networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 740–745, doi: 10.1109/IWCMC48107.2020.9148566.

[305] S. J. Andriole, "Blockchain, cryptocurrency, and cybersecurity," *IT Prof.*, vol. 22, no. 1, pp. 13–16, Jan. 2020, doi: 10.1109/MITP.2019.2949165.

[306] A. A. A. El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-based smart cities," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102549, doi: 10.1016/j.ipm.2021.102549.

[307] M. K. Aiden, S. M. Sabharwal, S. Chhabra, and M. Al-Asadi, "AI and blockchain for cyber security in cyber-physical system," in *Engineering Cyber-Physical Systems and Critical Infrastructures*, vol. 6, B. Bhushan, A. K. Sangaiah, and T. N. Nguyen, Eds., Cham, Switzerland: Springer, 2023, p. 10, doi: 10.1007/978-3-031-31952-5.

[308] F. Muheidat and L. Tawalbeh, "Artificial intelligence and blockchain for cybersecurity applications," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*. Cham, Switzerland: Springer, 2021, pp. 3–29, doi: 10.1007/978-3-030-74575-2_1.

[309] V. Kelli, P. Sarigiannidis, V. Argyriou, T. Lagkas, and V. Vitsas, "A cyber resilience framework for NG-IoT healthcare using machine learning and blockchain," in *Proc. IEEE Int. Conf. Commun.*, Montreal, QC, Canada, Jun. 2021, pp. 1–6, doi: 10.1109/ICC42927.2021.9500496.

[310] P. K. Sharma, P. Gope, and D. Puthal, "Blockchain and federated learning-enabled distributed secure and privacy-preserving computing architecture for IoT network," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Genoa, Italy, Jun. 2022, pp. 1–9, doi: 10.1109/EuroSPW55150.2022.00008.

[311] S. Gajek, M. Lees, and C. Jansen, "IIoT and cyber-resilience: Could blockchain have thwarted the stuxnet attack?" *AI Soc.*, vol. 36, no. 3, pp. 725–735, Sep. 2021, doi: 10.1007/s00146-020-01023-w.

[312] T. Harman, P. Mahadevan, K. Mukherjee, P. Chandrashekar, S. Venkiteswaran, and S. Mukherjea, "Cyber resiliency automation using blockchain," in *Proc. IEEE Int. Conf. Cloud Comput. Emerg. Markets (CCEM)*, Bengaluru, India, Sep. 2019, pp. 51–54, doi: 10.1109/CCEM48484.2019.00011.

[313] R. Mahmud and G.-S. Seo, "Blockchain-enabled cyber-secure microgrid control using consensus algorithm," in *Proc. IEEE 22nd Workshop Control Modeling Power Electron. (COMPEL)*, Cartagena, Colombia, Nov. 2021, pp. 1–7, doi: 10.1109/COMPEL52922.2021.9645973.

[314] A. Alam, M. T. Islam, and A. Ferdous, "Towards blockchain-based electricity trading system and cyber resilient microgrids," in *Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–5, doi: 10.1109/ECACE.2019.8679442.

[315] P. K. Sharma, D. Vohra, and S. Rathore, "Security and privacy in V2X communications: How can collaborative learning improve cybersecurity?" *IEEE Netw.*, vol. 36, no. 3, pp. 32–39, May 2022, doi: 10.1109/MNET.003.2100522.

[316] S. Kim and D. Kim, "Securing the cyber resilience of a blockchain-based railroad non-stop customs clearance system," *Sensors*, vol. 23, no. 6, p. 2914, Mar. 2023, doi: 10.3390/s23062914.

[317] K. Hausken, "Cyber resilience in firms, organizations and societies," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100204, doi: 10.1016/j.iot.2020.100204.

[318] A. Kanak, N. Ugur, and S. Ergun, "A visionary model on blockchain-based accountability for secure and collaborative digital twin environments," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Bari, Italy, Oct. 2019, pp. 3512–3517, doi: 10.1109/SMC.2019.8914304.

[319] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[320] J. Li, Z. Liu, L. Chen, P. Chen, and J. Wu, "Blockchain-based security architecture for distributed cloud storage," in *Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl. IEEE Int. Conf. Ubiquitous Comput. Commun. (ISPA/IUCC)*, Guangzhou, China, Dec. 2017, pp. 408–411.

[321] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, "Evaluating suitability of applying blockchain," in *Proc. 22nd Int. Conf. Eng. Complex Comput. Syst. (ICECCS)*, Fukuoka, Japan, Nov. 2017, pp. 158–161.

[322] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure Industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[323] J. J. Hunhevicz and D. M. Hall, "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options," *Adv. Eng. Informat.*, vol. 45, Aug. 2020, Art. no. 101094.

[324] I. M. Ar, I. Erol, I. Peker, A. I. Ozdemir, T. D. Medeni, and I. T. Medeni, "Evaluating the feasibility of blockchain in logistics operations: A decision framework," *Expert Syst. Appl.*, vol. 158, Nov. 2020, Art. no. 113543.
[325] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, Nov. 2018.
[326] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.
[327] J. S. Preden, K. Tammemäe, A. Jantsch, M. Leier, A. Riid, and E. Calis, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, Jul. 2015.
[328] Y. Huang, J. Zhang, J. Duan, B. Xiao, F. Ye, and Y. Yang, "Resource allocation and consensus of blockchains in pervasive edge computing environments," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3298–3311, Sep. 2022.
[329] B. Podgorelec, M. Hericko, and M. Turkanovic, "State channel as a service based on a distributed and decentralized web," *IEEE Access*, vol. 8, pp. 64678–64691, 2020.
[330] J. Yang, D. Lee, C. Baek, C. Park, B. Q. Lan, and D. Lee, "Leveraging blockchain for scaffolding work management in construction," *IEEE Access*, vol. 10, pp. 39220–39238, 2022.
[331] *Original Scrypt Function for Tarsnap*. Accessed: Jul. 26, 2023. [Online]. Available: http://www.tarsnap.com/scrypt.html
[332] A. Biryukov and D. Khovratovich, "Equihash: Asymmetric proof-of-work based on the generalized birthday problem," *Ledger*, vol. 2, pp. 1–30, Apr. 2017.
[333] *X11 Official Documentation for Dash*. Accessed: Jul. 26, 2023. [Online]. Available: https://docs.dash.org/en/stable/introduction/features.html#x11-hash-algorithm
[334] P. Fraga-Lamas, D. Barros, S. I. Lopes, and T. M. Fernández-Caramés, "Mist and edge computing cyber-physical human-centered systems for Industry 5.0: A cost-effective IoT thermal imaging safety system," *Sensors*, vol. 22, no. 21, p. 8500, Nov. 2022, doi: 10.3390/s22218500.
[335] N. Li, D. Liu, and S. Nepal, "Lightweight mutual authentication for IoT and its applications," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 4, pp. 359–370, Oct. 2017.
[336] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
[337] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.
[338] G. Danezis and A. Serjantov, "Statistical disclosure or intersection attacks on anonymity systems," in *Proc. Int. Workshop Inf. Hiding*. Toronto, ON, Canada, 2004, pp. 293–308.
[339] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, p. 16.
[340] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Honolulu, HI, USA, Jun. 2017, pp. 468–475.
[341] M. Vukolić. *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. Accessed: Jul. 26, 2023. [Online]. Available: http://www.vukolic.com/iNetSec2015.pdf
[342] N. T. Courtois, P. Emirdag, and D. A. Nagy, "Could Bitcoin transactions be 100x faster?" in *Proc. 11th Int. Conf. Secur. Cryptography*, Vienna, Austria, 2014, p. 16.
[343] D. Mohanty, "Ethereum: What lies ahead," in *Ethereum for Architects Developers*. Berkeley, CA, USA: Apress, 2018.
[344] *Sharding Official Web Page*. Accessed: Jul. 26, 2023. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-roadmap
[345] *Raiden Official Web Page*. Accessed: Jul. 26, 2023. [Online]. Available: https://raiden.network/101.html
[346] *MicroRaiden Official Web Page*. Accessed: Jul. 26, 2023. [Online]. Available: https://raiden.network/micro.html
[347] *LightningNetwork Official Web Page*. Accessed: Jul. 26, 2023. [Online]. Available:https://lightning.network/
[348] L. D. Negka and G. P. Spathoulas, "Blockchain state channels: A state of the art," *IEEE Access*, vol. 9, pp. 160277–160298, 2021, doi: 10.1109/ACCESS.2021.3131419.
[349] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," White Paper, 2017, pp. 1–47. [Online]. Available: https://www.plasma.io/plasma.pdf
[350] C. Jin, S. Pang, X. Qi, Z. Zhang, and A. Zhou, "A high performance concurrency protocol for smart contracts of permissioned blockchain," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 11, pp. 5070–5083, Nov. 2022.
[351] B. F. França. (Apr. 2015). *Homomorphic Mini-Blockchain Scheme*. Accessed: Jul. 26, 2023. [Online]. Available: http://cryptonite.info/files/HMBC.pdf
[352] T. Kim, S. Lee, Y. Kwon, J. Noh, S. Kim, and S. Cho, "SELCOM: Selective compression scheme for lightweight nodes in blockchain system," *IEEE Access*, vol. 8, pp. 225613–225626, 2020.
[353] M. B. Taylor, "The evolution of Bitcoin hardware," *Computer*, vol. 50, no. 9, pp. 58–66, 2017.
[354] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019, doi: 10.1109/ACCESS.2019.2935149.
[355] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A proof-of-quality-factor (PoQF)-based blockchain and edge computing for vehicular message dissemination," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2468–2482, Feb. 2021, doi: 10.1109/JIOT.2020.3026731.
[356] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd USENIX Symp. Operating Syst. Design Implement.*, 1999, pp. 173–186.
[357] C. Cachin, S. Schubert, and M. Vukolić, "Non-determinism in Byzantine fault-tolerant replication," in *Proc. Int. Conf. Princ. Distrib. Syst. (OPODIS)*, Madrid, Spain, Dec. 2016, p. 120.
[358] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Paris, France, Apr. 2017, pp. 23–26.
[359] *IEEE Blockchain Standards Association*. Accessed: Jul. 26, 2023. [Online]. Available: https://blockchain.ieee.org/standards
[360] *IEEE Draft Standard for the Use of Blockchain in Supply Chain Finance*, Standard IEEE P2418.7/D2.0, Mar. 2021, pp. 1–24.
[361] *IEEE Standard for Data Format for Blockchain Systems*, Standard IEEE Std 2418.2-2020, Dec. 2020, pp. 1–32.
[362] *IEEE Standard for Framework of Blockchain-Based Internet of Things (IoT) Data Management*, Standard IEEE 2144.1-2020, Jan. 2021, pp. 1–20.
[363] *IEEE Recommended Practice for E-Invoice Business Using Blockchain Technology*, Standard 2142.1-2021, Mar. 2021, pp. 1–18.
[364] *ISO/TC 307*. Accessed: Jul. 26, 2023. [Online]. Available: http://www.iso.org
[365] *CEN-CLC/JTC 19*. Accessed: Jul. 26, 2023. [Online]. Available: https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/emerging-technologies/
[366] *ETSI ISG PDL*. Accessed: Jul. 26, 2023. [Online]. Available: https://www.etsi.org/committee/1467-pdl
[367] *ITU-T Focus Group on DLTs*. Accessed: Jul. 26, 2023. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
[368] World Economic Forum. (Oct. 2020). *Global Standards Mapping Initiative: An Overview of Blockchain Technical Standards*. Accessed: Jul. 26, 2023. [Online]. Available: http://www3.weforum.org/docs/WEFGSMITechnicalStandards2020.pdf
[369] N. Borri and K. Shakhnov, "Regulation spillovers across cryptocurrency markets," *Finance Res. Lett.*, vol. 36, Oct. 2020, Art. no. 101333.
[370] *European Union Blockchain Observatory and Forum*. Accessed: Jul. 26, 2023. [Online]. Available: https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum

PAULA FRAGA-LAMAS (Senior Member, IEEE) received the M.Sc. degree in computer engineering from the University of A Coruña (UDC), in 2009, and the M.Sc. and Ph.D. degrees from five Spanish universities: The University of the Basque Country, the University of Cantabria, the University of Zaragoza, the University of Oviedo, and UDC, in 2011 and 2017, respectively, through the joint Mobile Network Information and Communication Technologies Program. She holds an M.B.A. and postgraduate studies in business innovation management (Jean Monnet Chair in European Industrial Economics, UDC), and in sustainability and social innovation (Inditex-UDC Chair of Sustainability). Since 2009, she has been with the Group of Electronic Technology and Communications (GTEC), Department of Computer Engineering, UDC. She is currently a Senior Researcher and Lecturer at UDC. She has published more than 100 contributions in indexed international journals, conferences, and book chapters. She holds four patents. Her current research interests include mission-critical scenarios, Industry 4.0/5.0, the Internet of Things (IoT), cyber-physical systems (CPS), augmented/mixed reality (AR/MR), fog and edge computing, blockchain and distributed ledger technology (DLT), and cybersecurity. She has been included, in 2019, 2020, 2021, and 2022, in the world's top 2% scientists, a study led by Stanford University that lists the 161,000 scientists worldwide with the highest impact publications. She has also been participating in over 40 research projects funded by the regional and national governments and research and development contracts with private companies. She is actively involved in many professional and editorial activities, acting as a reviewer, an advisory board member, a topic/guest editor of top-rank journals, and a TPC member of international conferences.

TIAGO M. FERNÁNDEZ-CARAMÉS (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from the University of A Coruña (UDC), Spain, in 2005 and 2011, respectively. He is currently an Associate Professor with UDC. His current research interests include the IoT/IIoT systems, RFID, wireless sensor networks, extended reality, embedded systems and blockchain, and the different technologies involved in the Industry 4.0/5.0 paradigms. In such fields, he has contributed to more than 120 papers for JCR-indexed journal articles, peer-reviewed conferences, and book chapters. Due to the impact of his publications, he has been included, since 2019, in the world's top 2% scientists, which lists the 2% scientists with the most impact according to a study led by Stanford University (only 161,000 worldwide scientists are listed in the rank). In the same study, since 2020, he has been among the 2% of scientists with the most impact throughout their entire careers. Moreover, due to his expertise in the previously mentioned fields, he has acted as a peer reviewer and a guest editor for different top-rank journals and a project reviewer for European Union and national research bodies from Austria, Croatia, Latvia, and Argentina.

ANTÓNIO M. ROSADO DA CRUZ received the B.Sc. degree in mathematics and computer science and the M.Sc. degree in computer science from the University of Minho, in 1993 and 2004, respectively, and the Ph.D. degree in informatics engineering from the University of Porto, Portugal, in 2011. He is currently an Associate Professor with the Polytechnic Institute of Viana do Castelo, Portugal, where he has coordinated the M.Sc. degree in software engineering, from 2012 to 2017, and the M.Sc. degree in informatics engineering, since 2017. He is a Researcher with the ADiT-Lab, Polytechnic Institute of Viana do Castelo, where he has participated into and managed several financed research projects. He is also an Associate Researcher with the ALGORITMI Research Centre, University of Minho, Portugal. He has 12 years of experience in the software industry plus 19 years of experience in academia. He has contributed to more than 40 Scopus-indexed articles, conference papers, and book chapters, peer-reviewed conference papers, and acted as a guest editor in several special issues of top-rank journals. His research interests include model-driven software engineering, code generation, human-centered AI, and the IIoT and traceability applications.

SERGIO IVAN LOPES (Senior Member, IEEE) received the B.Sc. degree in electronics and telecommunications engineering, the M.Sc. degree in biomedical engineering, the Ph.D. degree in electrical engineering from the University of Aveiro, and the Postgraduate Diploma degree in project management from Porto Business School, University of Porto. Since 2016, he has been a European Commission Expert and from 2019 to 2023, he was a Board Member with the Applied Digital Transformation Laboratory (ADiT-Lab). He is currently the Director General of CiTin—Centro de Interface Tecnológico Industrial, a Researcher with Instituto de Telecomunicacoes, and the Director of the graduation course in networks and Computer Systems Engineering (ERSC) of the Technology and Management School, Polytechnic Institute of Viana do Castelo (ESTG-IPVC), where he holds the position of an Assistant Professor. He is the co-inventor of two patents and has authored more than 100 scientific publications in international peer-reviewed journals and international conference proceedings. He has been a Researcher in several national and international research and development projects, five of which involved coordination activities. His research interests include cyber-physical systems, the IIoT/IoT, embedded systems, edge computing/intelligence, digital signal processing, and indoor positioning. In 2015, he was awarded the First Prize in the Fraunhofer Portugal Challenge (Ph.D. category), a distinction that rewards research of practical utility, and in 2007, he received the Texas Instruments ESPA Award (Excellence in Signal Processing Award). He has been the General-Chair of the EdgeIoT-International Conference on Intelligent Edge Processing in the IoT Era, since 2020, the Co-Chair of the WDTE-Workshop on Digital Transformation in The Enterprise, since 2019, the Co-Chair of the IEEE SCIS 2023-Conference on Smart Cities and Innovative Systems, and the Co-Chair of the Vertical Track: Energy and Power at the IEEE World Forum on Internet of Things 2022. He is the Professional Activities Coordinator of the IEEE Portuguese Section and Counselor on the Executive Committee of the IEEE IPVC Student Branch. He actively collaborates with the IEEE Communications Society and the IEEE Internet of Things (IoT) Initiative and has been a keynote speaker at international events, such as the IEEE IoT Vertical and Topical Summit at the IEEE Radio Wireless Week 2022.