# A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0

Sidi Boubacar Elmamy, Hichem Mrabet, Hassen Gharbi, Abderrazak Jemai, Damien Trentesaux

*sustainability*

MDPI

*Review*

# A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0

**Sidi Boubacar ElMamy [1], Hichem Mrabet [2], Hassen Gharbi [3], Abderrazak Jemai [4] and Damien Trentesaux [5,*]**

1 Department of Computer Science, Faculty of Sciences of Tunis, University of Tunis El Manar, Tunis 2092, Tunisia; elmamy.sidiboubecar@etudiant-fst.utm.tn
2 SERCOM-Laboratory, Tunisia Polytechnic School, Carthage University, Tunis 1054, Tunisia; hichem.mrabet@gmail.com
3 National School of Computer Science (ENSI), Manouba University, Manouba 2010, Tunisia; hassen.gharbi@ensi-uma.tn
4 INSAT, SERCOM-Laboratory, Tunisia Polytechnic School, Carthage University, Tunis 1080, Tunisia; abderrazak.jemai@insat.rnu.tn
5 LAMIH-UMR CNRS, Université Polytechnique Hauts-de-France, 59313 Valenciennes, France
* Correspondence: damien.trentesaux@uphf.fr

Received: 28 September 2020; Accepted: 24 October 2020; Published: 4 November 2020


**Abstract:** A systematic review of the literature is presented related to the usage of blockchain technology (BCT) for cyber-threats in the context of Industry 4.0. BCT plays a crucial role in creating smart factories and it is recognized as a core technology that triggers a disruptive revolution in Industry 4.0. Beyond security, authentication, asset tracking and the exchange of smart contracts, BCTs allow terminals to exchange information according to mutually agreed rules within a secured manner. Consequently, BCT can play a crucial role in industrial sustainability by preserving the assets and the environment and by enhancing the quality of life of citizens. In this work, a classification of the most important cyber-attacks that occurred in the last decade in Industry 4.0 is proposed based on four classes. The latter classes cover scanning, local to remote, power of root and denial of service (DoS). BCT is also defined and various types belong to BCT are introduced and highlighted. Likewise, BCT protocols and implementations are discussed as well. BCT implementation includes linear structure and directed acyclic graph (DAG) technology. Then, a comparative study of the most relevant works based on BCT in Industry 4.0 is conducted in terms of confidentiality, integrity, availability, privacy and multifactor authentication features. Our review shows that the integration of BCT in industry can ensure data confidentiality and integrity and should be enforced to preserve data availability and privacy. Future research directions towards enforcing BCT in the industrial field by considering machine learning, 5G/6G mobile systems and new emergent technologies are presented.

**Keywords:** Industry 4.0; blockchain; industrial internet of things (IIoT); cyber-security; cyber physical system (CPS); cloud computing; edge computing; smart manufacturing; sustainability

## 1. Introduction

The term blockchain technology (BCT) appeared in 2008 with Bitcoin [1–4]; it is part of a set of disruptive technologies that promise to be the key to revolutionizing and changing the future of our industry, created so that smart and digitally connected factories perform more autonomous, efficient, fast and secure processes without the need for a third party to control operations [1,2]. BCT provides data immutability, provenance, consistency and failure tolerance and is verifiable and data auditable using built-in cryptographic mechanisms. These features match the low-trust environment

of a manufacturing system involving humans and merged in the society. Combining BCTs with smart contracts will enable automated enforcement of some conditions in real-life contracts [1–4]. Using BCT in Industry 4.0 contributes to a sustainable development by providing strong, secure and safe communication mechanisms such as the usage of a public and private key to ensure authentication, an access control list (ACL) to ensure the access control management and X.509 digital certificates to ensure authenticity, nonrepudiation and integrity.

Various review papers have been published regarding the usage of BCTs in different application fields. Observing a number of surveys and journals published on BCT applications in IoT, smart cities and industry, Table 1 contains a number of existing literature reviews and surveys. For example, the authors of [3,4] examined the BCT applications for IoT and discussed the benefits and limitations of using BCT in such applications. According to our knowledge that there is no review or investigation that focuses on the use of BCT for cyber-threats in Industry 4.0. Therefore, this motivates this research. The purpose of this survey paper is to provide a detailed analysis of BCT for Industry 4.0 and what it can bring to the key technologies of Industry 4.0; then, a classification of the most important cyber-attacks for the last decade in the Industry 4.0 field is detailed, and likewise, a comparison of the proposed related works based on BCT for Industry 4.0 in terms of security features that have never been proposed in previous review papers. After, an explanation and review of the state-of-the-art in Industry 4.0 is given with regard to the underlying industries and technologies, by focusing on the most relevant proposed framework based on BCT in the context of Industry 4.0, as well as their main challenges. Section 2 presents the main aspects of the systematic review methodology used. In Section 3, the key enabling technologies and the cyber-threats in Industry 4.0 are exhibited. Likewise, the related emerging technology associated with industry 4.0 are discussed such as IoT, cyber-physical systems and cloud and edge computing.

**Table 1.** Related literature reviews in the usage of blockchain technology (BCT).

| Years | Authors | Focus |
|---|---|---|
| 2016 | Christidis and al. [5] | Blockchain and smart contract for Internet-of-Things |
| 2018 | Fernandez-Carames and al. [6] | Challenges and recommendations for developing blockchain-based IoT applications |
| 2018 | Ferrag and al. [7] | Blockchain-based security and privacy solutions for IoT |
| 2018 | Salman et al. [3] | Blockchain solutions to achieve distributed network security |
| 2018 | Shen and al. [8] | Review of blockchain use cases for cities |
| 2019 | Fraga and al. [9] | Review of blockchain in automotive industry |
| 2019 | Lu and al. [10] | Review of blockchain in oil and gas industry |
| 2019 | Yang and al. [11] | Integration of blockchain and edge computing technologies |
| 2019 | Xie and al. [12] | Blockchain applicability to smart cities |
| 2020 | Madhusudan Singh [13] | Blockchain technology for data management in Industry 4.0 |

On the other hand, security threats in Industry 4.0 are studied by proposing a classification of the most important cyber-threats in Industry 4.0 that happened in the last decade. In Section 4, blockchain technology is introduced by presenting the various protocols and implementation models that belong to blockchain technology. In Section 5, the most pertinent related works based on BCT in Industry 4.0 are presented, discussed and compared in term of confidentiality, integrity, availability and privacy security features. Then, open issues and future directions are discussed in Section 6. Finally, Section 5, presents a synthesis of the survey and a conclusion is suggested.

## 2. Methodology

A review methodology has been applied to rigorously locate relevant research and to guarantee the quality and veracity of the articles ultimately selected. The process for this approach is illustrated in Figure 1.

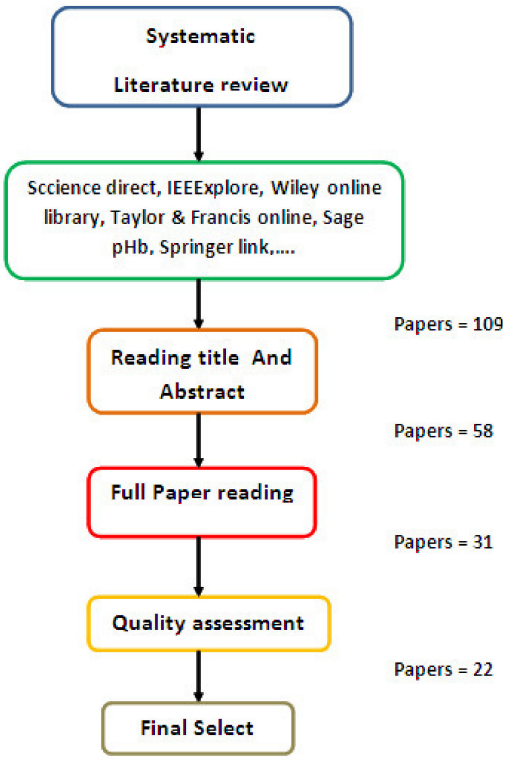


**Figure 1.** Schematic representation of the systematic review process.

First, "Blockchain," and "Industry 4.0" were chosen as keywords to search for articles (journal paper, conference, book chapter) published from 2018 to 2020 (recent works) collected from ScienceDirect, Emerald Insight, Wiley Online Library, Taylor & Francis Online, Sage Publications, IEEE Xplore and Springer Link. The research yielded 109 results, which indicates that Industry 4.0 and blockchain technology are emerging research topics. In the second step, these 109 articles were carefully reviewed, and inefficiently related articles were dropped (unclassified conference, unindexed journal, etc.). At the end, 58 documents were tabled. The 58 articles were then examined in depth, which led to 22 articles as a final selection.

## 3. Industry 4.0

### *3.1. Definition*

The concept of Industry 4.0 was originally proposed to develop the German economy in 2011. Industry 4.0 is the subset of the fourth industrial revolution that concerns industry [14].

Industry 4.0 encompasses many paradigms, including enterprise resource planning (ERP), big data, cloud manufacturing, logistics and social product development [13–15]. Particularly, Industry 4.0 is based on the smart contract concept. A smart contract is broader than a service level agreement (SLA) and can be a guarantor of protecting a SLA specification between a provider and consumers from violation while providing the security services required by the blockchain by enforcing data integrity and trustability [16]. The stakeholders in Industry 4.0 will refer to the smart contract for satisfaction of the SLA specification. SLA is a service that can be integrated with a smart contract between different participants. Therefore, BCT with the smart contract component is the ideal location to implement SLA by taking advantage of blockchain integrity and traceability.

### 3.2. Related Technology

Various technologies or techniques can be used to implement Industry 4.0. These technologies include IoT and radio frequency identification (RFID), cyber-physical systems (CPS), cloud computing, edge computing and other related technologies [17–19].

#### 3.2.1. Internet of Things (IoT)

Several architectures have been proposed in recent years and the most basic architecture is composed of four layers including the perception layer, network layer, middleware layer (service layer) and application layer, as shown in Figure 2 [20]. The perception layer is also called as 'Sensing Layer'. It is composed of physical objects and sensing devices such as various forms of sensory technologies, such as RFID sensors. The network layer is the infrastructure to support wireless or wired connections between sensor devices and the information processing system.

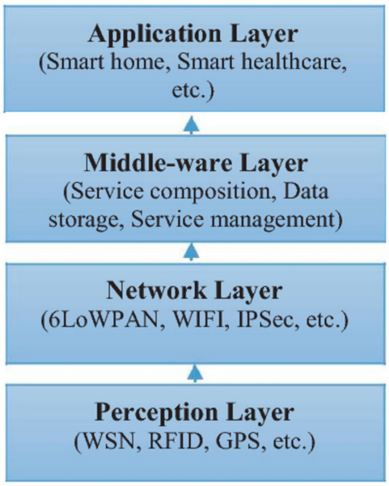


**Figure 2.** Example of internet-of-things (IoT) architecture based on four layers [20].

The middleware layer is responsible for ensuring and managing services required by users or applications. When the term IoT first appeared, it referred to uniquely identifiable interoperable connected objects using radio RFID technology. By connecting the RFID reader to the internet, readers can automatically and uniquely identify and track objects attached with labels in real time. Figure 3 illustrates technologies and devices used to support the IoT. The key technologies include RFID and a wireless sensor network (WSN) and other relevant technologies such as barcodes, smart-phones, cloud computing, location-based service, service-oriented architecture (SOA), near field communication and social networks.

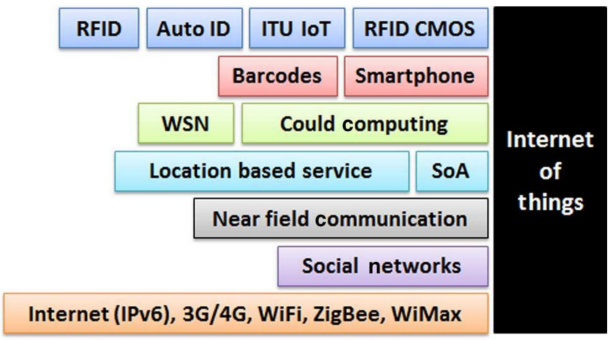


**Figure 3.** Technologies associated with the IoT [21].

Industry 4.0 combines intelligent sensors, artificial intelligence and data analysis to optimize real-time manufacturing. With advances in sensor network technologies, wireless communication and other emerging technologies, more and more networked objects, or intelligent objects, are involved in the IoT. At the same time, these IoT-related technologies have also had a significant impact on new information and communication technologies.

#### 3.2.2. Cyber-Physical-System (CPS)

CPS [22] is an autonomous system that integrates electronics and software, sensors and actuators and has communication capability. A CPS interacts with its environment in which it takes data, processes it through a control feedback loop or influences the process with which it is associated. CPSs are used to control and drive physical processes and thus "augment" these new feature processes. Because of its communication capabilities, a CPS can collaborate with other systems and exchange data with remote systems. When a CPS uses internet communication technologies, it becomes a basic building block of the IoT. A CPS [22–24] is characterized by a high degree of complexity that is partly intrinsic and especially because of interconnection and dynamic interactions with other systems. The networked use allows us to play with distributed intelligence on different CPSs as well as their individual specificities. The smart factory relies on CPSs that autonomously exchange information, control processes and trigger actions according to "circumstances". Such a system acquires a capacity of self-adaptability and agility according to the analysis of key parameters. A CPS can also trigger a preventive maintenance alert because the set of monitored parameters shows a high probability of failure. This is obtained both by correlation of the parameters with fault scenarios but also by correlation with the history of the stored data.

#### 3.2.3. Cloud Computing

In the area of industrial infrastructures dominated by physical systems, a large amount of data is collected in real time by a large number of networked sensors that must be analyzed in real time. Big data and real-time analytics applied to big data in cloud systems enable the implementation of these techniques to extract new information from the data. Several industrial applications already use cloud architectures and services [25]. The trend towards virtualization of resources and critical aspects of real-world processes addresses the needs of many organizations for scalability, more efficient use of resources and lower total cost of ownership, to name just a few each. Cloud computing has been widely adopted by the industry as it captures the benefits of virtualization, SOA and consumer computing. CPS [22] services are accessible via the internet but nevertheless offer the application the feeling of being installed locally. Vast computing and storage resources available in the cloud, which can scale or meet the needs of the specific application, are a motivating factor for using cloud computing in industrial scenarios.

Most modern industrial enterprises already rely on applications deployed on local or remote cloud computing systems, allowing multiple industry 4.0 participants to easily collaborate with each other. However, such a system suffers from a major limitation [25,26]: if the cloud is affected in one way or another by software problems, high workloads or attacks, the entire system can be blocked for all users.

### *3.3. Cyber-Threats in Industry 4.0*

As authors in [27] note in 2017, the transformation from Industry 3.0 to Industry 4.0 has been associated with technological changes and subsequent increased cyber-threats. For example, Industry 3.0 relied on serial and relay logic systems that depended on local area network (LAN), TCP/IP and programmable logic controller (PLC), which is a special computer device used for industrial control systems, and the scripting language of vendors who exposed systems to threats such as system failure due to a malfunction of the packages, the man in the middle (MIM) analyzing false information for the operators and mainly denial of service (DoS). In Table 2, a layer-based attack in IIoT systems is exhibited according to IoT architecture based on four layers [20,28].

**Table 2.** Layer-based attacks in IIoT systems.

| Layer | Attacks | Description |
|---|---|---|
| Application | Injection | Untrusted data that is sent to an interpreter or database |
| | Brute force | An attempt to guess a password via sending various passwords |
| | Malware | A malicious code can attack mail and web services |
| Middleware | Flooding | Repeating the request of a new connection until the IIoT system reaches maximum level. |
| | De-synchronization | Disruption of an existing connection |
| Network | DoS | Attempt to stop or reduce activity of an IIoT |
| | MIM | Violating data confidentiality or integrity during transfer |
| | HELLO flood | Uses HELLO packets as weapon to launch the attack on IIoT system |
| | Sybil | A single node duplicates its node to be in multiple locations |
| Perception | Eavesdropping | Deducing data sent by IIoT devices across network |
| | RFID tracking | Modifying a content of a tag or trying to disable it |
| | Jamming | Creating radio interference and exhaustion on IIoT devices |

A denial of service (DoS) attack is an attack that targets the availability of a system or service by flooding it with requests that make the service unavailable to its legitimate users [23]. A specific type called distributed DoS (DDoS) is a type of DoS attack in which flood requests come simultaneously from multiple sources on the network. In conventional DoS attacks, the attacker bombards the target server with a huge quantity of requests forcing it to commit all available computer resources, and the input data forces the server to malfunction resulting in a crash. The technique can also be used as a listening support tool in MIM attacks.

In general, the buffer overflow that occurs within the server can result in the disabling of security systems, in particular the network intrusion detection system (NIDS) and the firewall. Industry 4.0 depends on the interconnection and integration of many systems and processes, creating environments that may be suitable for successful DoS attacks [29]. In addition, the increasing use of cloud-based techniques in manufacturing processes and intelligent factories will expose many DoS attacks if the cloud system is not well designed to defend against them [30]. As organizations move forward with applications, many other unknown vulnerabilities are emerging [31]. The consequences and impacts of DoS attacks can severely affect an organization's operations in the context of Industry 4.0 due to the use of sensors. The main challenge of DoS is that it is difficult to detect and therefore its risks cannot be easily quantified and planned for, and the constraint extends to the creation of controls within systems and processes to minimize impacts. However, it was noted that the origin of vulnerabilities in supply chains can be traced back to vendors where the potential for portal hacking, MIM attacks, DoS and lateral attacks resulting from unencrypted connections and data transmission remain. Authors in [21,32] suggest that the transition to Industry 4.0 requires plans to create security awareness and develop control mechanisms and authentication policies, including encryption technologies and behavioral analysis tools to prevent hacking of supply chains and their dependent processes.

Industry 4.0 is mainly based on the industrial IoT and relies on ad hoc connections facilitating rigorous collection and monitoring to improve product life cycles. The flow of data on the system presents innumerable points of vulnerability, and attackers can steal data at any point and without appropriate protective measures [33]. In particular, attackers can physically or logically access cyber-physical production systems (CPPS): "systems of collaborating computational entities which are in intensive connection with the surrounding physical world and its on-going processes, providing and using, at the same time, data-accessing and data-processing services available on the internet" or programmable logic controllers within the IoT [34]. A layer-based attack and the attempt by an adversary to attack through communication protocol stack is shown in Table 2. There are five levels involved where the attacker can try to compromise the objects of IoT [20].

In cloud computing, especially in the context of big data, it is becoming increasingly difficult to secure data transmission between physical and virtual assets, and authentication is even difficult when disseminating information across several vulnerable interconnected devices [35]. Some of the

threats to data are confidentiality, integrity and authentication, data availability and misconfiguration. Wide-area attack threats are associated with a single point of failure, and most reports have cited denial of service (DoS) as the primary mode of attack [36]. In the context of Industry 4.0, and given the speed at which organizations and companies in all sectors are adopting certain concepts and technologies, the threats related to espionage and theft of confidential information are much greater due to the interaction of partners and devices within the network. Moreover, the theft of sensitive information, in particular intellectual property of products and production processes, compromises the competitive ability of the undertaking concerned on the market. Collaborative theft and industrial espionage continue to increase as many companies seek more technologies to achieve intelligent factory configuration [37,38]. Therefore, establishing security techniques and control mechanisms to ensure transparency and trust within all types of Industry 4.0 platforms is crucial, and these measures should focus on protecting confidential information [30,39]. It would be prudent for individual organizations to pursue some of the modern and advanced data protection and encryption technologies, including the possibility of implementing quantum cryptography at the production, manufacturing and distribution levels. On the other hand, according to a survey conducted in the Swedish manufacturing industry, the effective implemented cyber security measures in Industry 4.0 by order of merit are technical solutions, rules and processes, strategy, annual review, continuity plan, cyber insurance, training, exercise and certification [25].

Table 3 presents a classification of the most important cyber-attacks in Industry 4.0 based on the four classes proposed by authors in [33] involving scanning, remote to local, user to root and DoS for class 1, class 2, class 3 and class 4 attacks, respectively.

**Table 3.** Classification of the most important cyber-threats in Industry 4.0.

| Cyber-Attack | Description | Class 1 (Scan) | Class 2 (Remote to local) | Class 3 (Power of root) | Class 4 (DoS) |
|---|---|---|---|---|---|
| Cyber-attack'2009 | A group of cyberattacks took on major government's financial websites and news agencies, both United States and South Korea, with releasing of botnet. | | | | ✓ |
| Stuxnet'2010 | It was designed to target and disrupt industrial control systems based on the supervisory control and data acquisition (SCADA) system. | | | | ✓ |
| Spamhaus'2013 | It is considered as the biggest cyber-attack in history, it is a filtering service used to extract spam e-mails. | ✓ | | | |
| Steel mill'2014 | The hackers attacked a steel mill in Germany. By manipulating or disrupting the control systems, it caused major damages in the foundry. | | | | ✓ |
| Black Energy malware'2015 | The malware exploited the macros in Microsoft Excel documents. The bug was planted into a company's network using spam emails. | | ✓ | | |
| Norsk Hydro Aluminum'2019 | Norsk Hydro, a global aluminium and renewable energy company based in Norway, was hit by a ransomware called LockerGoga. | | | ✓ | |

In fact, blockchain technology is based on the implementation of the consensus algorithm via a smart contract between participants. Therefore, smart contracts are linked blocks using a hash function to ensure blockchain integrity. In addition, using a hash function between the different smart contract blocks can preserve the data integrity and can be useful to detect any malicious modifications. On the other hand, using a Mongo database with blockchain implementation can also enforce the security mechanism, adding more cryptography proofs against various confidentiality threats and attacks. Finally, a hash function and cryptography proofs are effective solutions against various attacks to IIoT systems such as injection and malware attacks targeting the data confidentiality and integrity related to databases and blockchain as well.

## 4. Blockchain Technology

In this section a definition of blockchain technology (BCT) is provided, exhibiting various types that belong to BCT. The BCT protocols and implementation models are discussed at the end of this section.

BCT is defined as a secured agreement among users via a consensus algorithm leading to a new transaction (i.e., new block) added in the ledger [40]. Likewise, transaction validation requested by a node in the network in BCT is based on a validation algorithm like a public key. BCT is seen as a promising and emerging technology to benefit the cyber security domain. BCT is made up of different components working together in a distributed decentralized network. The technology aims to ensure trust in a completely untrusted network with unknown parties [19]. A very significant added value of BCT is that it solves two of the most dreaded problems of currency-based transactions, which have so long necessitated the validation of a third party [41]. These problems are popularly known as the Byzantine generals' problem and the double spend problem. The original idea of BCT implementation propounded by Nakamoto [1,42] was that of a publicly distributed ledger. In theory, based on who can access the BCT network and how the permissions to write to the BCT network are assigned, four types of BCTs can be defined including permission less (i.e., anyone with computing power can join), permissioned (i.e., approved users only), public (i.e., all who access can modify) and private (i.e., only specific users can write/modify).

Public BCTs are open for everyone to participate. Anyone can join them to perform transactions and to participate in the mining and consensus process to add new blocks of transactions to the BCT [18]. These BCTs usually use proof of work (PoW) or proof of stake (PoS) for the consensus mechanism.

Permissioned BCTs are built usually by organizations for their specific business need. Such BCTs are likely to have interfaces with existing applications of the organization. Organizations may opt for consortium BCTs where limited trusted members mandatorily need to sign off a transaction. In fully private BCTs, the write permission over the BCT is given to a central organization. The former are referred to as partially decentralized according to authors in [43]. Much value is seen in private BCTs due to the flexibility offered by increased control over the rules of transaction, which may be altered by overall consensus. This becomes easier in a private or consortium BCT than a public one. There is also increased accountability as all the nodes are named.

BCT protocols fall into three categories covering proof of work (PoW), proof of stake (PoS) and practical Byzantine fault tolerance (PBFT).

On the one hand, PoW protocol requires cryptographic puzzles to be solved using brute force [19,44] in order to create a new block. This process of creating a new block is called mining. Miners represent the nodes in the network that mean new blocks. Every miner will create a new block individually by solving the cryptographic puzzle. The winning miner is the first one who solves the puzzle and creates the block. They are rewarded with an amount of cryptocurrency which varies from one BCT platform to another. Furthermore, the PoW behaves like a lottery system. The more processing power the node detains, the more its chance increases to be the winning miner. PoW has a property that anyone can easily prove that a certain amount of work was done to produce a block. However, it is an expansive process that expands significant computational resources.

On the other hand, PoS is an alternative to the PoW consensus protocol [45–48]. It does not rely on the mining process, but performs a validating one. Peers who perform block validation are called validators. Each validator owns a stake in the network, which is a security deposit also called a bond.

Finally, an approach dealing with the Byzantine general's problem is the federated Byzantine agreement (FBA) [19,44]. In this approach, it is assumed that the participants of the network know each other and can distinguish which ones are important and which ones are not. PBFT is a replication algorithm, which utilizes this principle. Hyperledger utilizes the PBFT as its consensus algorithm [48,49].

In the decade since its inception, the BCT model has faced growing difficulties. Two of the largest challenges facing BCT are its inability to handle a large volume of transactions simultaneously and its high transaction fees. In order to resolve these drawbacks, a more recent solution is to use a directed acyclic graph (DAG) to implement a distributed ledger [45,46] instead of the BCT linear structure as shown in Figure 4. In mathematics, DAG is a graph that travels in one direction without cycles connecting to other edges. An example of DAG-based distributed ledger technology is the tangle implemented by IOTA [47,48].

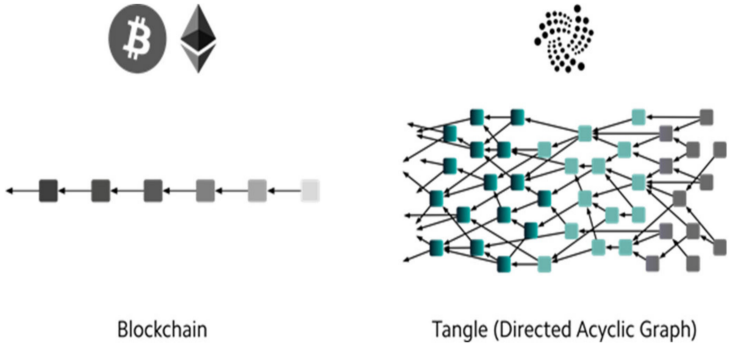


**Figure 4.** Blockchain versus tangle (directed acyclic graph) [44].

The tangle is a DAG composed of a network with a number of different nodes confirming transactions. Every new transaction that is submitted requires the confirmation of at least two earlier transactions before it is successfully recorded on the network [44]. Unlike the BCT model, tangle requires no miners to confirm each transaction as being authentic. Having two parent transactions confirms the validity of a subsequent transaction.

## 5. Related Works Based on BCT for Industry 4.0

In this section, we select the five most pertinent proposals on BCT for Industry 4.0 among 22 papers provided by the result of the systematic review process. The latter selected works cover the implementation of the Hydro Raindrop multifactor authentication solution on a WordPress page (named 2FA) [50], a sample system data exchange between sample participants using smart contracts (called FabRec) [51], a middleware approach for utilizing BCT services by integrating IIoT embedded in a robot, manufacturing CPS, cloud and fog manufacturing for a smart manufacturing solution (called Man4Ware) [52], BSeIn [53] and FAR-EDGE [43]. The author in [50] presents how the usage of a BCT two-factor authentication solution (2FA) on a page developed on WordPress can contribute to information security regarding user authentication. The research method employed is characterized as exploratory research, since all the analysis is based on the theoretical reference data available on the subject. Field research was carried out in relation to the implementation of the multi-factor authentication plugin Hydro Raindrop MFA (i.e., MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows a user to present two pieces of evidence or credentials when logging into an account). Additionally, user credentials must come from two different categories to enhance security according to the National Institute of Standards and Technology (NIST) recommendation, which uses BCT technology [1] offered by the Hydrogen Technology Corporation and the Project Hydro platform over the Ethereum

network [2]. Thus, this paper sought to present and conceptualize some of the technologies used, pointing out their contribution to information security. The main results showed that the use of decentralized technology, such as BCT and the Hydro Raindrop plugin, can contribute considerably in the process of user authentication, which may strengthen the safeguarding of the information and assets of individuals and organizations by inhibiting or reducing the possibility of successful hacker attacks. This solution is at the forefront of innovation with regard to data security because it uses advanced BCT technology [23]. It might contribute in a satisfactory way to the preservation of critical data and information, which are the core value of many organizations of Industry 4.0 [6,24]. This research was limited to analyzing how the implementation of the Hydro Raindrop multifactor authentication solution on a WordPress page can be beneficial to ensuring information security. Authors in [51] proposed FabRec, which is defined as a decentralized approach to handling manufacturing information by various organizations using BCT technology. A system in which a decentralized network of manufacturing machines and computing nodes can enable automated transparency of an organization's capability based on past events and automated mechanisms to drive paperless contracts between participants using smart contracts [2]. This system decentralizes critical information about the manufacturer and makes it available on a peer to network provenance of fiduciary nodes to ensure transparency and data provenance through a verifiable audit trail. Authors in [51] present a testbed platform through a combination of machine and system-on-chip platforms computing nodes to be able to work through a consortium of disparate organizations through a decentralized network. This prototype testbed demonstrates the value of the residing computer code residing and can be divided into two groups autonomously initiated in the physical world. Middleware solutions and BCT functionality are useful methods to provide a development and execution environment to address many of these challenges. As shown in Figure 5, the designer has introduced four software components: 1) a machine's virtual twin library; 2) an Ethereum client; 3) a nodal database sentry and 4) a FabRec blockchain view manager. Each component has a specific purpose: The virtual twin library enables machine communication with the digital twin/virtual manufacturing machine built on top of a not only SQL(NoSQL) database. The Ethereum client is hosted at the client to enable interaction with the BCT. The nodal database sentry can be envisioned as a program enforcing cryptographic proofs that the data coming from the virtual machine node have not been tampered with. The BCT manager can be thought of as an indexing and visualization server to keep track of the transactions on the BCT in a human readable format (similar to etherscan.io but for machine data).

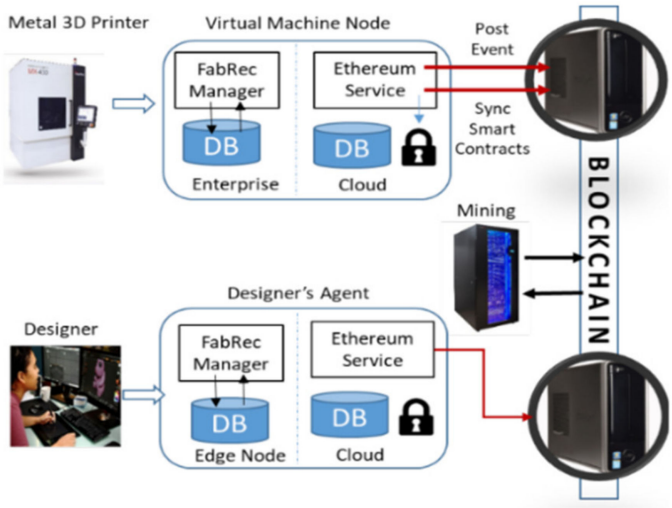


**Figure 5.** Sample system data exchange between sample participants [51].

The FabRec smart contract structure is composed of a global register contract (RC) that contains a list of participant historical event contracts (PHECs). Each PHEC contains a list of participant relationship

contract (PRC) addresses and status. The relationship between the RC and PHEC represents the blockchain structure. Likewise, each entry in the PRC in the Oracle database represents an agreement between the participant (for instance, the user requests a fabrication service) and meta-data that belongs to this relationship. Finally, the usage of a cloud Mongo database can be viewed as a security mechanism to enforce cryptographic proof that data sent by the virtual machine node are not altered.

Another pertinent work presented in [52] proposes a middleware approach for utilizing BCT services and capabilities to enable more secure, trustable, traceable, reliable and autonomous smart manufacturing applications. This approach will offer many advantages to secure and establish good trust among involved parties in the manufacturing value chain. A Man4Ware proposal in [52] views all resources in the smart manufacturing environment including sensors, actuators and IoT [26] devices as services that can be requested and deployed by other services in smart manufacturing applications. Furthermore, the addition of BCT services in Man4Ware will further improve the environment and facilitate more secure, traceable and immutable features in intelligent manufacturing applications. In addition, this will enable a variety of new applications to realize the promising benefits of Industry 4.0 for smart manufacturing. Man4Ware can be used as the supporting development and execution framework and to provide the integration mechanisms for these applications. Man4Ware is a service-oriented middleware (SOM) [52] designed to develop, execute and support distributed services for smart manufacturing applications. It offers the essential services to provision the development of the proposed model for smart manufacturing. It can be used to integrate the different technologies needed for complete smart manufacturing solutions that include various components like industrial IoT embedded in a robot, manufacturing CPS, fog manufacturing and cloud manufacturing, as shown in Figure 6 [52].

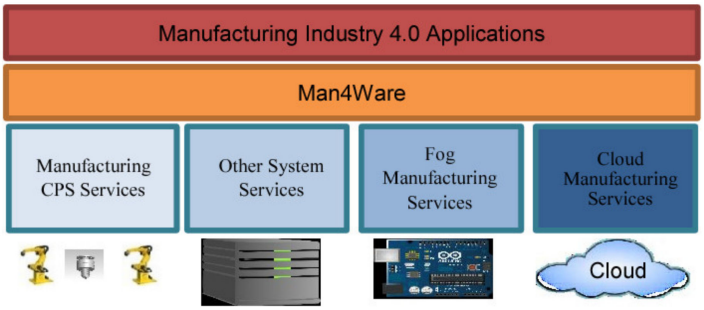


**Figure 6.** Man4Ware integrates various technologies to enable smart manufacturing applications [52].

Industry 4.0 is not a far-fetched concept, and the complexity of such systems requires a more robust security solution [53]. To establish secure remote user authentication with detailed access control for Industry 4.0 applications, the author in [53] offers a new framework based on a BCT named BSeIn. The proposed framework exploits the underlying characteristics of the BCT as well as several cryptographic materials to create a decentralized, confidential and auditable solution. In particular, it used anonymous terminal authentication (i.e., attribute-based signature (ABS)), efficient gateway authentication (i.e., message authentication code (MAC)) and confidentiality of requested messages (via certificateless multi-receiver encryption (CL-MRE)). In addition, it is demonstrated that BSeIn is safe, and an evaluation of the performance of the prototype is addressed. The latter, contains a hierarchical framework comprising four tangible layers, which is designed to vertically integrate inter-organizational value networks, an engineering value chain, manufacturing factories, etc. The conceptual framework allows a flexible and reconfigurable smart factory to be efficiently implemented. However, authors need to consider security inherent in existing (stand-alone) devices and networks as well as those that may arise in such integrations. Especially the existing solutions are insufficient to address these fundamental security concerns. BSeIn is a BCT-based system for secure mutual authentication to enforce fine-grained access control polices. The proposed system (with integrated attribute signature, multi receiver encryption and message authentication code) is designed to provide privacy and security guarantees

such as anonymous authentication, auditability and confidentiality. BSeIn [53] also scales well due to the utilization of a smart contract. Then, authors evaluate the security and performance of BSeIn. The participants involved in BSeIn include terminals, a BCT network, a cloud, an industrial network and physical resources, as shown in Figure 7. Terminals are often some remote telecommunication devices (e.g., mobile devices) that can remotely request access or process the commands.

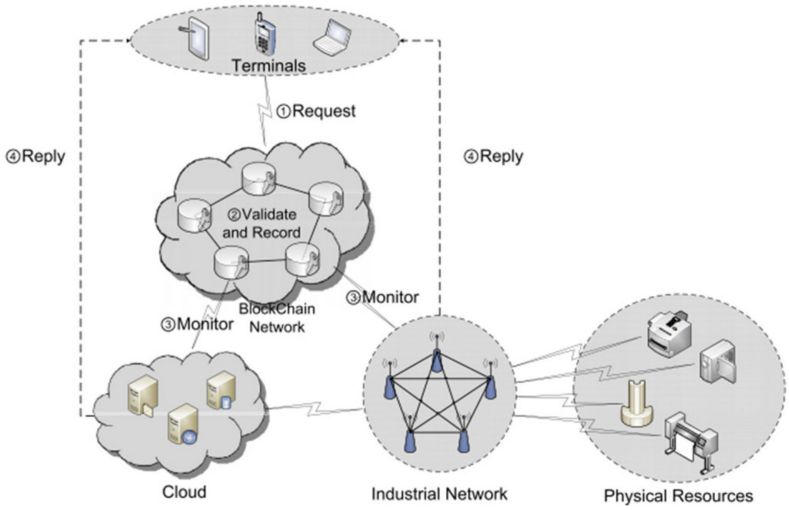


**Figure 7.** BSeIn system architecture [53].

When these participants wish to make a request, they need to publish a corresponding transaction to the BCT network. In the BCT network [53], the authors adopt a permissioned fabric that comprises some processing and consensus nodes (i.e., permissioned nodes) responsible for maintaining the BCT according to a consensus mechanism. In this system, they adopt a practical consensus mechanism (PBFT) unlike the Bitcoin BCT (uses proof of work, PoW). Permissioned nodes are classified into a "validation node" (responsible for verifying transactions, abbreviated as "vdn") and "bookkeeping node" (takes charge of chaining validated transactions into the BCT, abbreviated as "bkn"). After permissioned nodes reach a consensus on the received requests from terminals, the requests will be recorded in the BCT. The cloud hosts a number of information systems (e.g., ERP) which collect and process massive data from various physical resources and respond to the access data requests from terminals. That is, the cloud monitors the BCT network and responds to the requested data or terminals. Regarding the industrial network, in contrast to the cloud, it is mainly tasked with dealing with requests from terminals, and such requests are mainly control commands. Once the industrial network has monitored the BCT network and received the control requests, it communicates with the relevant physical resource to execute the control commands and send the results to the relevant terminals. Finally, for physical resources, the function of this participant in BSeIn is the same as that in the conventional system, in the sense that they need to transfer the (massive) data to the cloud via the industrial network and execute the control orders from the industrial network.

The final work is presented in [43], which provides a comprehensive overview of the FAR-EDGE reference architecture (RA). The FAR-EDGE RA is the conceptual framework that drives the design and the implementation of the FAR-EDGE platform, which describes the basic elements necessary for the development of digital automation platforms using advanced computing capabilities and BCT for industry. In addition, the paper also describes the design of a platform that adheres to the FAR-EDGE RA, including details of the various components it includes and how they interact. The design for each individual tier of the FAR-EDGE platform, which adheres to the RA, is presented in Figure 8. The different proposed layers are field tier, edge tier, ledge tier and cloud tier. The field tier is the realm of edge nodes (EN), which connect the real world to the digital world of information technology (IT) and vice versa. The ENs have enough computing capabilities on board to be active actors in a CPS,

i.e., intelligent devices that are conveniently called "Smart Objects", ranging from a simple PLC to a fully-autonomous smart plant. Typically, smart objects are controller boards with some significant processing power and a good network connection but lack any (usable) local storage. The platform defines two components that can be run on such a device, namely policy decision point (PDP) and ledger clients. At the platform level, edge computing is supported by seven components, two of them with enabler status such as edge automation services, an edge analytics engine, field abstraction, data routing and pre-processing, policy decision point a system entity that makes authorization decisions for itself or for other system entities that request such decisions, ledger clients and node management. All Components are meant to be deployed on edge gateway (EG) machines. The ledger tier is where the full potential of edge computing is unleashed. It allows for truly distributed process logic to work in use cases that require some level of coordination as is true for most industrial scenarios without any centralized service being in charge of it. It employs the distributed ledger and smart contract patterns both key elements of BCT technologies. The peer nodes run the distributed ledger enabler and the orchestration services, configuration services, data publishing services and synchronization services components. Finally, the cloud tier includes a total of eleven components, three of them having enabler status. They are classified as (i) public cloud services, which are accessible through three open application programming interfaces (API)s, namely the open API for automation, the open API for analytics and the open API for virtualization; (ii) internal cloud services, including identity management, model repository and data storage; and (iii) platform cloud tools, including security management, policy decision point (edger clients, real-to-digital synchronization) and platform management components.

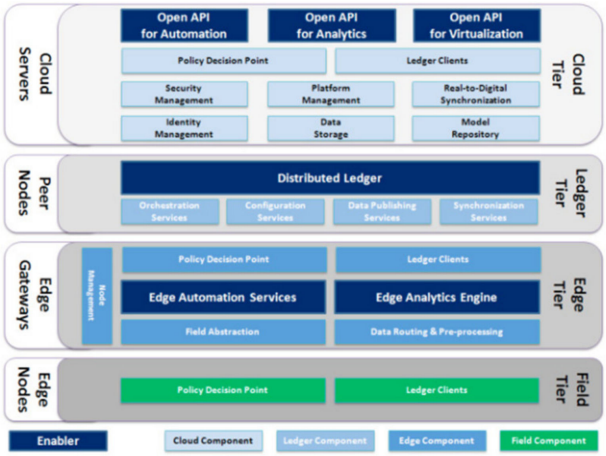


**Figure 8.** FAR-EDGE platform design [43].

In light of the security challenges and requirements of the main related works presented above, Table 4 contains a summary of requirements, highlighting the main aspects inherent in each framework based on BCT in the context of Industry 4.0.

**Table 4.** A comparative study between the different related works based on BCT in Industry 4.0 as a function of security features.

| Security Features | 2FA [50] | FabRec [51] | Man4Ware [52] | BSeIn [53] | FAR-EDGE [43] |
|---|---|---|---|---|---|
| Confidentiality | ✖ | ✓ | ✖ | ✓ | ✓ |
| Integrity | ✖ | ✓ | ✓ | ✖ | ✓ |
| Availability | ✖ | ✓ | ✖ | ✖ | ✖ |
| Privacy | | ✖ | ✖ | ✓ | ✖ |
| Multifactor Authentication | ✓ | ✖ | ✓ | ✓ | ✖ |

✓ yes, ✖ No.

According to Table 4, we found that no work can provide the complete security features. Secondly, 60% of works provide confidentiality, integrity and multifactor authentication. In contrast, only 20% of works take care of availability and privacy issues. In conclusion, we believe that more efforts should be accorded to preserve availability and privacy in future works based on BCT in the context of Industry 4.0 by employing fine grained access control mechanisms and using lightweight attribute-based encryption (ABE) techniques [54].

## 6. Open Issues and Future Research Directions

There are some performance and security issues regarding the usage of BCT for Industry 4.0 that still remain without solution until now. Firstly, the security of BCT depends on its method of implementation and the usage of software and hardware in that implementation. Since all the transactions made by users in BCT are public, there is a possibility that private information of users can be revealed. A compromised data user can be viewed as a potential risk to launch an intrusion attack and DoS attack as well. One solution is to enforce IT staff working in the industrial environment by supporting Industry 4.0 to follow a policy for protecting confidential data by applying information security standards like ISO/IEC 27000-series and NIST recommendations. Secondly, as the number of miners (i.e., block) increases, the size of the BCT also increases continuously [19,42]. This increases the cost of storage and reduces the speed of distribution over the whole network, leading to a rise in the number of issues like the scalability and availability of BCT [55]. For instance, when the number of blocks is increased dramatically the scalability of the BCT becomes an issue and can lead to an increase in the latency of the entire network.

Some of the future research directions in using BCT in Industry 4.0 are as follows:

1. Various consensus algorithms are being designed to support high throughput along with a large number of nodes or users. More efficient and reliable consensus mechanisms can be designed to reach consensus among the nodes along with preventing rampant use of computation power. The current consensus algorithms are highly resource intensive and less efficient.
2. The data analysis and prediction in near real time and in the proximity of the IIoT node is crucial for successful deployment of IIoT applications in the industrial field. Various machine learning (ML)-based algorithms can be designed to analyze the data in the node itself to prevent the data transit for analysis and prediction. The latter process can further enhance the security of the application by preventing data movement [56]. Moreover, integration of BCT in IIoT applications is an emergent technique getting more attention from researchers recently, which can play an important role in tackling security issues and privacy violations.
3. We believe that the new architecture of IIoT has to include a BCT layer [57] that can be viewed as a roadmap towards a definition of standard architecture and can be implemented effectively in industrial IoT applications.
4. A limitation regarding the implementation of BCT in the 5G mobile system and further applications, for instance 6G, in spite of the existence of a limited number of works [7,57–59], is a big challenge for researchers in the near future.
5. Integration of new technologies based on BCT for Industry 4.0 is a big challenge for researchers that can be considered as double-edged sword. On the one hand, digital transformation is an effective solution to enhance process and productivity in industry. On the other hand, adding more technologies can lead to more vulnerability and raising the number of cyber-attacks targeting manufacturing based on Industry 4.0. Finally, some recent works are oriented to creating a dataset for cyber-security attacks in the context of IoT and IIoT in cloud/fog systems by using ML and deep learning to build an adaptive learning model that can classify and detect a wide range of cyber-threats and attacks [60].

6. BCT is a better guarantor compared to other technologies with an effective cost by exploiting traceability and nonrepudiation of BCT features, to check and verify who and which action is leading to hampering the sustainability charter (i.e., societal environment). Additionally, in parallel to economic performances, a smart contract is considered as a core component of BCT that can take into consideration environmental performances (i.e., minimize negative external factors of the fabrication process) and societal as shown in Figure 9 (i.e., promote employability and enhancement of citizen quality of life) [61–63].
7. It will be useful to design global implementation frameworks and develop methodological guides to support the deployment of BCT in Industry 4.0 systems and architectures.

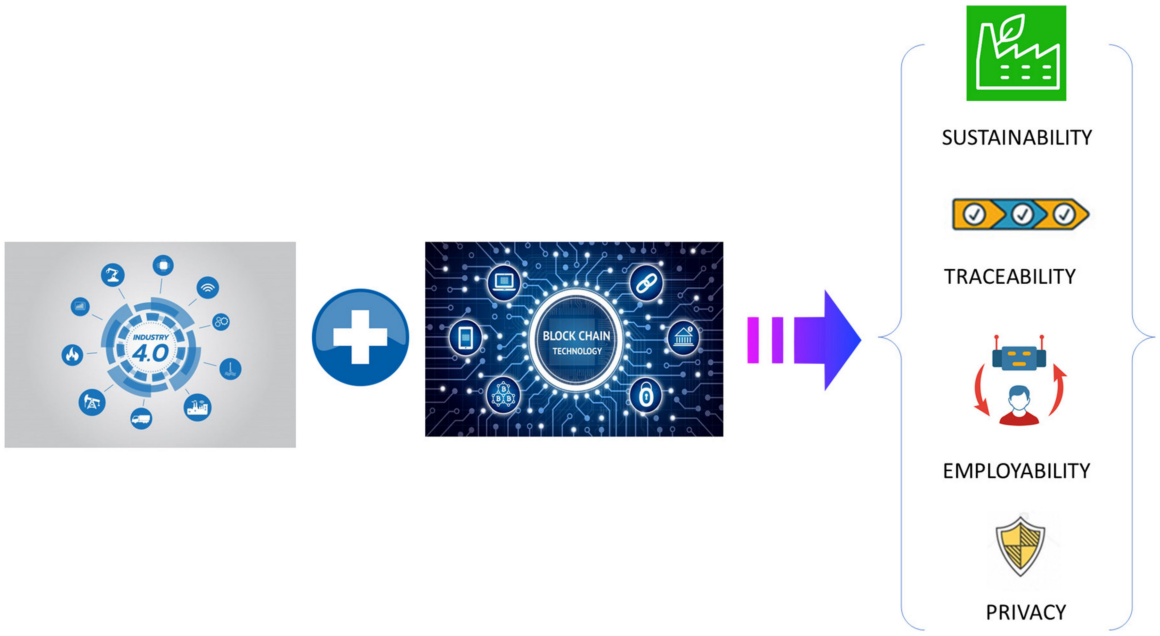


**Figure 9.** Benefits from the association of Industry 4.0 and blockchain technology.

## 7. Conclusions

Industry 4.0 is a paradigm that is changing the way that factories operate in edge of cloud computing, big data and new emergent technologies. A driver of industrial sustainability concerns the security and the safety of these technologies. BCT, which has been used successfully for cryptocurrencies, contributes to this industrial sustainability by adding security, trust, immutability, disintermediation, decentralization and a higher degree of automation through the smart contracts concept. This article presented a detailed analysis related to the usage of BCT for cyber-threats in Industry 4.0. A classification of the most important cyber-threats in Industry 4.0 for the last decade was presented and the common security solutions were exhibited as well. It was demonstrated in this work that the usage of a hash function and cryptography proofs by BCT were effective solutions against various attacks on IIoT systems such as injection and malware attacks targeting the data confidentiality and integrity related to databases and blockchain as well. Then, a detailed investigation of the most relevant BCT-based related works was presented and a solution involving two-factor authentication (2FA), FabRec, Man4Ware, BSeIn and FAR-EDGE was presented. Then, a comparison between the different frameworks based on BCT in the context of Industry 4.0 was performed as a function of security components covering confidentiality, integrity, availability, privacy and multifactor authentication. Our results revealed that 60% of the compared works in Industry 4.0 can ensure the confidentiality and integrity security components, inherited from the usage of BCT. In contrast, only 20% of works solve availability and privacy issues. In the last section, open issues and future research directions regarding the usage of BCT in the industrial field were discussed. Firstly, open research issues were exhibited including

performance and security issues in terms of scalability, network latency and data confidentiality. Secondly, future research directions covered how to improve consensus algorithms, data analysis and prediction of IIoT nodes across the implementation of ML-based solutions (i.e., via the preservation of data movement), defining a standard architecture for IIoT, the integration of new technologies based on BCT for Industry 4.0 to enforce the digital transformation process and how BCT can play a crucial role in sustainability by preserving the environment and enhancing the quality of life of citizens.

**Author Contributions:** Conceptualization, S.B.E. and A.J.; methodology, H.M. and D.T.; validation, H.G., H.M. and A.J.; formal analysis, H.M.; investigation, H.M.; resources, H.M.; data curation, S.B.E.; writing—original draft preparation, S.B.E. and H.M..; writing—review and editing, H.M.; supervision, A.J.; project administration, D.T.; All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

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

## References

1. A Peer-to-Peer Electronic Cash System. Available online: http://www.bitcoin.org (accessed on 22 September 2018).
2. On Public and Private Blockchains. Available online: https://blog.ethereum.org (accessed on 22 September 2018).
3. Salman, T.; Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security services using blockchains: A state-of-the-art survey. *IEEE Commun. Surv. Tut.* **2019**, *21*, 858–880. [CrossRef]
4. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 21–22 May 2015.
5. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
6. Fernández-Caramés, T.M.; Fraga-Lamas, P. A review on the use of blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
7. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
8. Shen, C.; Pena-Mora, F. Blockchain for Cities—A Systematic Literature Review. *IEEE Access* **2018**, *6*, 76787–76819. [CrossRef]
9. Fraga-Lamas, P.; Fernández-Caramés, T.M. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
10. Lu, H.; Huang, K.; Azimi, M.; Guo, L. Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks. *IEEE Access* **2019**, *7*, 41426–41444. [CrossRef]
11. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 1508–1532. [CrossRef]
12. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2794–2830. [CrossRef]
13. Singh, M. Blockchain Technology for Data Management in Industry 4.0. In *Blockchain Technology for Industry 4.0. Blockchain Technologies*; Rosa Righi, R., Alberti, A., Singh, M., Eds.; Springer: Singapore, 2020.
14. Da Xu, L.; Xu, E.L.; Li, L. Industry 4.0: State of the art and future trends. *Int. J. Prod. Res.* **2018**, *56*, 2941–2962. [CrossRef]
15. Hofmann, E.; Rüsch, M. Industry 4.0 and the current status as well as future prospects on logistics. *Comput. Ind.* **2017**, *89*, 23–34. [CrossRef]
16. Hang, L.; Kim, D.-H. SLA-Based Sharing Economy Service with Smart Contract for Resource Integrity in the Internet of Things. *Appl. Sci.* **2019**, *9*, 3602. [CrossRef]
17. Isaja, M.; Soldatos, J.K. Distributed Ledger Architecture for Automation, Analytics and Simulation in Industrial Environments. *IFAC-PapersOnLine* **2018**, *51*, 370–375. [CrossRef]
18. Banerjee, A. Chapter Nine -Blockchain with IOT: Applications and use cases for a new paradigm of supply chain driving efficiency and cost. *Adv. Comput.* **2019**, *115*, 259–292.
19. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the application of blockchain to the next generation of cybersecure Industry 4.0 smart factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]

20. Alani, M.M. *Elements of Cloud Computing Security*; Springer Science and Business Media LLC: Basel, Switzerland, 2016.
21. Waidner, M.; Kasper, M. Security in industry 4.0-challenges and solutions for the fourth industrial revolution. In Proceedings of the 2016 Design, Automation & Test in Europe Conference & Exhibition (DATE), Research Publishing Services, Dresden, Germany, 14–18 March 2016; pp. 1303–1308.
22. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
23. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 1–25. [CrossRef]
24. He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the 2016 IEEE Congress on Evolutionary Computation (CEC) Institute of Electrical and Electronics Engineers (IEEE), Vancouver, BC, Canada, 24–29 July 2020; pp. 1015–1021.
25. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27.
26. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access* **2019**, *7*, 176838–176869. [CrossRef]
27. Liu, Y.; Xu, X. Industry 4.0 and Cloud Manufacturing: A Comparative Analysis. *J. Manuf. Sci. Eng.* **2016**, *139*, 034701. [CrossRef]
28. Panchal, A.C.; Khadse, V.M.; Mahalle, P.N. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. In Proceedings of the 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 23–24 November 2018; pp. 124–130.
29. Franke, U.; Wernberg, J. A survey of cyber security in the Swedish manufacturing industry. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–8. [CrossRef]
30. Oueslati, N.E.; Mrabet, H.; Jemai, A.; Alhomoud, A. Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. In Proceedings of the 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, 20–22 December 2019; pp. 1–7.
31. Yan, J.; Meng, Y.; Lu, L.; Li, L. Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes, and Applications for Predictive Maintenance. *IEEE Access* **2017**, *5*, 23484–23491. [CrossRef]
32. Antão, L.; Pinto, R.; Reis, J.; Goncalves, G. Requirements for Testing and Validating the Industrial Internet of Things. In Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Vasteras, Sweden, 9–13 April 2018; pp. 110–115.
33. Deloitte Industry 4.0 Report. Available online: https://www2.deloitte.com/content/dam/insights/us/articles/4323Forcesofchange/4323Forcesofchange_Ind4-0.pdf (accessed on 22 September 2018).
34. Ustundag, A.; Cevikcan, E. *Industry 4.0: Managing The Digital Transformation*; Springer Science and Business Media LLC: Basel, Switzerland, 2018.
35. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.
36. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
37. Xu, H.; Yu, W.; Griffith, D.; Golmie, N. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. *IEEE Access* **2018**, *6*, 78238–78259. [CrossRef]
38. Lu, Y. The blockchain: State-of-the-art and research challenges. *J. Ind. Inf. Integr.* **2019**, *15*, 80–90. [CrossRef]
39. Leitão, P.; Colombo, A.W.; Karnouskos, S. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Comput. Ind.* **2016**, *81*, 11–25. [CrossRef]
40. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Das, G. Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [CrossRef]

41. Kshetri, N. Can Blockchain Strengthen the Internet of Things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
42. Boubakr, N.; Kashif, S.; Fan, L.; Yu, W. Security and Privacy Challenges in Information-Centric Wireless Internet of Things Networks. *IEEE Secur. Priv.* **2020**, *18*, 35–45.
43. Lee, J.; Azamfar, M.; Singh, J. A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. *Manuf. Lett.* **2019**, *20*, 34–39. [CrossRef]
44. Aras, S.T.; Supriya, T.; Vrushali, K. Blockchain and its applications—A detailed survey. *Int. J. Comput. Appl.* **2017**, *180*, 29–35.
45. Cao, B.; Zhang, Z.; Feng, D.; Zhang, S.; Zhang, L.; Peng, M.; Li, Y. Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digit. Commun. Networks* **2020**. [CrossRef]
46. Pervez, H.; Muneeb, M.; Irfan, M.U.; Haq, I.U. A Comparative Analysis of DAG-Based Blockchain Architectures. In Proceedings of the 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 19–21 December 2018; pp. 27–34.
47. IOTA Developer Documentation. Available online: https://docs.IoTa.org/ (accessed on 22 September 2019).
48. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. Available online: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf (accessed on 22 September 2019).
49. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 1–15 April 2018.
50. Cardoso, J.A.A.; Ishizu, F.T.; De Lima, J.T.; Pinto, J.D.S. Blockchain Based MFA Solution: The use of hydro raindrop MFA for information security on WordPress websites. *Braz. J. Oper. Prod. Manag.* **2019**, *16*, 281–293. [CrossRef]
51. Angrish, A.; Craver, B.; Hasan, M.; Starly, B. A Case Study for Blockchain in Manufacturing: "FabRec": A Prototype for Peer-to-Peer Network of Manufacturing Nodes. *Procedia Manuf.* **2018**, *26*, 1180–1192. [CrossRef]
52. Al-Jaroodi, J.; Mohamed, N.; Jawhar, I. A service-oriented middleware framework for manufacturing industry 4.0. *ACM SIGBED Rev.* **2018**, *15*, 29–36. [CrossRef]
53. Lin, C.; He, D.; Huang, X.; Choo, K.-K.R.; Vasilakos, A.V. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *J. Netw. Comput. Appl.* **2018**, *116*, 42–52. [CrossRef]
54. Belguith, S.; Kaaniche, N.; Russello, G. PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 924–927. [CrossRef]
55. Gao, W.; Hatcher, W.G.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–11.
56. Mishra, P.; Varadharajan, V.; Tupakula, U.; Pilli, E.S. A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 686–728. [CrossRef]
57. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
58. Fan, K.; Ren, Y.; Wang, Y.; Li, H.; Yang, Y. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. *IET Commun.* **2018**, *12*, 527–532. [CrossRef]
59. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* **2020**, *20*, 3625. [CrossRef]
60. Moustafa, N. New Generations of Internet of Things Datasets for Cybersecurity Applications based Machine Learning: ON_IoT Datasets. In Proceedings of the eResearch Australasia Conference, Brisbane, Australia, 21–25 October 2019.
61. Leng, J.; Yan, D.; Liu, Q.; Xu, K.; Zhao, J.L.; Shi, R.; Wei, L.; Zhang, D.; Chen, X. ManuChain: Combining Permissioned Blockchain With a Holistic Optimization Model as Bi-Level Intelligence for Smart Manufacturing. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *50*, 1–11. [CrossRef]

62. Pérez, J.J.B.; Queiruga-Dios, A.; Martínez, V.G.; Del Rey, A.M. Traceability of Ready-to-Wear Clothing through Blockchain Technology. *Sustainability* **2020**, *12*, 7491. [CrossRef]
63. Paliwal, V.; Chandra, S.; Sharma, S. Blockchain Technology for Sustainable Supply Chain Management: A Systematic Literature Review and a Classification Framework. *Sustainability* **2020**, *12*, 7638. [CrossRef]