Integration of IoT and Blockchain to in the Processes of a University Campus

William Villegas-Ch 1,*, Xavier Palacios-Pacheco 2 and Milton Román-Cañizares 1

1 Escuela de Ingeniería en Tecnologías de la Información, FICA, Universidad de Las Américas, Quito 170125, Ecuador; milton.roman@udla.edu.ec
2 Departamento de Sistemas, Universidad Internacional del Ecuador, Quito 170411, Ecuador; xpalacio@uide.edu.ec
* Correspondence: william.villegas@udla.edu.ec; Tel.: +593-098-136-4068

Received: 8 May 2020; Accepted: 9 June 2020; Published: 18 June 2020

Abstract: Currently, universities, as centers of research and innovation, integrate in their processes various technologies that allow improving services and processes for their members. Among the innovative technologies are the Internet of Things that, through a variety of devices, allows obtaining data from the environment and people. This information is processed in cloud computing models and Big Data architectures that obtain knowledge through data analysis. These results lead to improving processes and making better decisions that improve the services available at the university. The integration of technologies allows for the generation of a sustainable environment that seeks the cohesion of the population with the environment, in such a way that economic growth is guaranteed in balance with the environment. However, all technology needs to guarantee the security of processes and data, and for this purpose, a new technology such as blockchain is integrated, which seeks to respond to two needs, the security and agility of processes. Integrating this technology in a university requires the analysis of the blockchain components to generate a new layer that adapts to the architecture of a university campus. This ensures that the data are kept cryptographically private to avoid exposure and that the entire process is verified by multiple blocks.

Keywords: blockchain; Internet of Things; security of information; smart campuses

1. Introduction

Currently, the use of emerging technologies has exponentially grown in society, and this has allowed improving many aspects of the quality of life. The enhancement that these technologies have brought is mainly due to the penetration of the Internet, which has caused large industries to support the design and creation of devices that interact with people or with each other, through the use of the Internet [1]. These devices have better performance, and their dynamic communication with people allows these devices to be involved in most of people’s activities [2]. In fact, several of these devices are not focused on personal use, but instead, are focused on solving problems in environments where hundreds or thousands of people live. The speed at which society operates results in technologies that perform activities that often people do not want to do themselves [3]. From this point of view, the responsibility of controlling the performance of an activity entrusted to the devices can be done remotely. These characteristics of the devices make them part of the Internet of Things (IoT) [4].

The IoT allows the connection of many devices to the network, through sensors and actuators that perform a variety of tasks [5]. These tasks can be for domestic use or in very large environments such as campuses or cities, where their main task is to collect information from the environment and perform an action [6]. A proof of this is home automation, which has traditionally required private technology to function properly. With the use of IoT, this approach has changed. Now, such platforms
are available, and innovation is focused on the development of applications that use the services of various platforms to perform more complex tasks [7]. The IoT has positioned itself as one of the pillars of the digital environment. In this way, traditional environments use information technology (IT) included in architectures that work alongside emerging technologies to provide the environment with some intelligence [8]. An example that is increasingly visible is smart cities. These macro environments have an infinite number of services that need IoT to improve their use, especially in areas such as mobility and security [5]. In addition, concepts such as human cyber-physical systems to monitor, control, and manage conditions efficiently are integrated with the aim of ensuring adequate conditions at a lower cost [9,10]. These systems are built from the transparent integration of physical and computational components. These systems outperform today’s simple integrated systems in terms of capacity, adaptability, scalability, resilience, security, and usability [11].

The way in which IoT manages the services of an environment is through its architecture, which is built in layers and based on the collection of information. The devices always sense the medium, and this generates a large volume of data that act as raw material for cloud computing [12]. The operation of IoT, although it presents unique advantages to improve user experience, also presents several problems that have occurred precisely in the data acquisition layer and the way they are transported [13]. This puts user and organization data at risk, because according to reports and research on IoT security, there are precedents in which security levels have been compromised and information has been affected [14]. These deficiencies have to do directly with the great moment that passes the devices that incorporate this technology. This has led manufacturers to focus on the sale of a product and not on the quality of the device that must meet standards that allow it to provide high levels of safety. Many of the security flaws found in the IoT include manufacturers that leave back doors open in order to obtain information about the use of their products and thus improve their sales [15]. Information management is currently an issue that should be considered a priority in the deployment of any architecture that includes the use of emerging technologies. There are policies and standards that are being worked on to preserve data security, but at the same time, it is important to look for models that ensure the proper use of information.

The combination of technologies has often allowed us to improve a system, architecture, or model and strengthen its use in society [16]. This reference is applicable in the use of emerging technologies, and there are specific cases that are a sign of the strength of this combination [1]. This is the case of university campuses that adopt the Internet of Things, Big Data, and cloud computing to become smart campuses [17]. The priority is the personalization of the services dedicated to all members and forging sustainable ecosystems [18]. Within this same environment, the integration of a technology that, like IoT, has exponential growth, the blockchain, has been considered. The blockchain is a unique registry, agreed and distributed in several nodes of a network. This technology allows the transfer of digital data with very sophisticated coding and in a completely secure way [19]. Each block has a specific and immovable place in the chain since each block contains information from the hash of the previous block. The entire chain is stored in each node of the network that makes up the blockchain, so an exact copy of the chain is stored for all network participants [20].

Blockchain technology becomes the ideal partner for IoT because it guarantees the handling of information and insecurity in the user disappears by not revealing information from the source and the recipient. This is ideal in an IoT deployment, solving the problems it presents so far [21]. But, how a blockchain architecture can be integrated into the IoT architecture without affecting the available services of an environment? The answer is to create test benches, where the implementation of these technologies is done in a controlled environment and the data is not compromised. To do this, the work proposes to create an architecture that integrates both the IoT and the blockchain within a university campus [22]. University fields can be as large as small cities and handle similar governance models. The advantage of creating this architecture on a university campus is to provide the desired controlled environment and define all the real variables of a scaled environment. The results obtained
will help the work to be replicated in places such as large cities, reducing the risk and the economic
cost of integrating technologies.

This article is organized as follows: Section 2 reviews the concepts used in this research; Section 3
describes the proposed method; Section 4 shows the results of the investigation; Section 5 discusses
the results obtained and finally; Section 6 presents the conclusions.

2. Preliminary Concepts

For the development of this work, several concepts have been used that give a guide of all
the components that should be included for the design of the proposal. These concepts clarify
the environment where the work is carried out, in addition, it shows the operation of each of the
technologies individually. This is the starting point that provides the basis for the integration of
technologies and ensures data security in a controlled environment.

2.1. University Campuses

University campuses are geographical areas that contain infrastructure and different spaces that
belong to a university. A campus is composed of several faculties, green areas, libraries, etc. All these
areas are intended for students and staff related to education to develop their life on campus with all
the services they need [17]. Much of the infrastructure of a university campus links to information
and communication technologies (ICT). The concept of the university campus is taken for this work
because of the importance of defining the environment where IoT devices are applied [23]. In addition,
it is necessary to identify the type of communication technologies and architectures that are used
within the campus. Accordingly, an architecture that encompasses the greatest number of variables
and scenarios can be established to convert the proposal into a generic architecture that is replicated in
other environments [24].

A university campus integrates a large number of individuals who are responsible for
administrative and academic activities. For the development of these activities, the campus makes
available to the user certain technological services such as computer systems, communication services,
laboratories, etc. However, to offer the required technological services, the large number of people who
are part of the university campus is considered as a variable [25]. This factor requires many resources
and an architecture that guarantees its operation. An example, common is that the new university
campuses include learning management systems (LMS). This makes the Internet service a fundamental
requirement for the development of any academic activity. Therefore, the campus infrastructure must
contain a physical and wireless network model that meets these needs. This is where work begins to
define a secure architecture for IoT management [26].

A traditional university campus has a layered network architecture, the protocol used in IPv4
in the vast majority. While the campus is limited to a fixed geographical area, it can also cover
several contiguous buildings, for example, several faculties or the environment of a matrix and
several campuses [27]. The architecture of the university campus is presented as a scalable and
modular network. In addition, it can be easily expanded to include additional buildings or campus
floors as the university grows [8]. Figure 1 shows the main modules of the university campus
architecture that includes, business campus, enterprise Edge, service provider end and remote access.

The business campus module is composed of all the campus infrastructure and includes the access,
distribution and core layers. The access layer module includes layer 2 or layer 3 switches to provide
the required port density. In this module, VLANs and trunks to the distribution layer of the building
are managed. In the distribution layer module, routing, access control and QoS are carried out [28].
The core layer module provides high-speed interconnectedness between the distribution layer modules,
the data center server farms and the business perimeter. In this module, the central axis of the design
is redundancy, rapid convergence and fault tolerance [29].
Figure 1. Network architecture of a university campus.

The business perimeter module consists of the Internet, VPN and WAN modules that connect the university to the service provider’s network. This module extends university services to remote sites and allows you to use Internet resources. In addition, it provides quality of service (QoS), policy reinforcement, levels of service and security. The perimeter module of the service provider provides Internet, public switched telephone network (PSTN) and WAN services. The campus network architecture passes through an end device. This is the moment in which the packages can be analyzed and the decision can be made whether they should be allowed to enter the business network. Intrusion detection system [30] ms (IDS) and intrusion prevention systems (IPS) can also be configured on the business perimeter to provide protection against malicious activities.

2.2. Internet of Things

IoT is defined as the grouping and interconnection of devices and objects through a private (intranet) or public (Internet) network, where all devices are visible and can interact with people or with each other. Objects or devices can be categorized into sensors and mechanical devices to everyday objects such as appliances or clothing. Anything you can imagine can be connected to the Internet and interact without the need for human intervention [31]. The objective is, therefore, a machine-to-machine interaction, or what is known as an M2M (machine to machine) interaction or M2M devices. The IoT uses network connectivity and computing capacity and extends it to everyday objects, sensors and items that are not considered computers [32]. It allows these devices to generate, exchange and consume data with minimal human intervention [33]. It allows consumer products, public services, sensors and other objects to be combined through Internet connectivity. According to several studies, the projections of the impact of IoT on the Internet and the economy anticipate that in 2025 there will be up to one hundred billion devices connected to IoT.

The concept of combining computers, sensors and networks to monitor and control different devices has existed for decades [34]. However, the integration of different trends in the technology market allows the IoT to be a reality. These trends include connectivity, the adoption of networks based on the IP protocol, computing capacity, miniaturization, advances in data analysis and the emergence of cloud computing [12]. The IoT implementation uses different connectivity models, each of which has its own characteristics. These features contribute to the four connectivity models described by the Internet architecture, Device-to-Device, Device-to-Cloud, Device-to-Gateway and
Back-End Data-Sharing. These models highlight flexibility in the ways in which IoT devices can connect and provide value to the user [35].

However, IoT also poses important challenges that could hinder the realization of its potential benefits. Attacks on devices connected to the Internet, fear of surveillance and concerns related to privacy have captured the attention of the public [36]. The technical challenges are still there, but new policy, legal and development challenges are emerging. While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services is a fundamental priority [14]. Users should be able to trust that IoT devices and related data services will be safe and free of vulnerabilities. Especially as this technology is more widespread and integrated into our daily lives. The unsafe IoT devices and services can serve as potential entry points for cyber attacks and expose user data to theft by leaving data flows with inadequate protection.

With this background, the IoT architecture meets certain requirements for this technology to be viable. It must allow it to be distributed, scalable, efficient and secure where objects can interact with each other [37]. The IoT architecture consists of a set of sensors that are part of a device that includes connection modules. These modules allow two-way communication with a gateway node, which also has a wireless or physical device connected to it [38]. Once the gateway node obtains the data from the sensors, they are sent to the cloud so that they can be available. The IoT follows a layered architecture as presented in Figure 2. The architecture describes the structure of IoT, includes physical aspects (things) and virtual aspects (services and communication protocols). Adopting a multi-level architecture allows you to focus on improving your understanding of how all the most important aspects of the architecture work before you integrate them into your IoT application. This modular approach helps you manage the complexity of IoT solutions [39].

![Figure 2. General architecture of an Internet of things model.](image)

2.3. Blockchain

It is a technology that enables the transfer of digital data with highly sophisticated encryption and in a completely secure manner [19]. This transfer does not require a centralized intermediary to identify and certify the information, but rather it is distributed in multiple independent nodes that register and validate it without the need for trust between them. Once entered, the information cannot be deleted, only new records can be added, and it is not legitimized unless most of them agree to do so [21]. The level of security provided by this system presents another advantage in communication because, if the network goes down, with only one computer or node not doing so, the information or service will never be lost or continue to function as the case may be [40].
Blockchain is a distributed technology where each node in the network stores an exact copy of the chain, thus guaranteeing the availability of information at all times. In the event that an attacker causes a denial of service, he must bypass all nodes on the network for the attack to succeed [41]. It is enough that at least one is operational for the information to be available. This feature responds to an architecture that allows digital information to be distributed, rather than copied. In Figure 3, the Blockchain architecture in a distributed network is presented where each individual participates within the network and approves and updates new entries. The system is controlled not only by separate individuals but by everyone within the blockchain network [42]. Each member ensures that all records and procedures are in order, resulting in the validity and security of the data. Therefore, parties that do not necessarily trust each other can reach a common consensus.

![Figure 3. Distributed blockchain architecture with validation nodes and member nodes.](image)

The blockchain architecture includes certain main components that are responsible for recording transactions in a process [43]. These components are the node that is the user or computer within the blockchain architecture. The transaction which is the smallest building block of a blockchain system, includes the records, information, etc., serves as the purpose of the blockchain. The block is a data structure used to maintain a set of transactions that is distributed to all nodes on the network [44]. The chain is the sequence of blocks in a specific order. Miners are specific nodes that go through the block verification process before adding anything to the blockchain structure. The consensus is a set of rules and arrangements to carry out blockchain operations. Any new record or transaction within the blockchain implies the construction of a new block. Each record is digitally tested and signed to ensure its authenticity. Before adding this block to the network, it must be verified by most of the nodes in the system.

3. Method

To establish an architecture that provides security to the IoT through blockchain integration, it is necessary to identify the medium where IoT is applied and its weaknesses. This information allows establishing the variables that need to be controlled and the model that can do it.

The proposed method responds to the needs of a university campus, for which, the process consists of two parts. The first focuses on identifying all the steps that a Blockchain process integrated into the IoT must carry out. The second part is in charge of integrating each Blockchain component to a capacity and that is interacting with the entire campus architecture. In Figure 4, it shows the block diagram that explains how a process that includes the use of IoT and Blockchain works.
Once a process starts, the order entry is registered where, the IoT devices that will be necessary to acquire the event data are established. Next, the registration request is generated, where the Blockchain requests the creation of the blocks that will be necessary for the validation of the process and the data. In this same instance, a memory space is assigned to each block where the hash of the previous block is copied. In the next stage, the request is processed and notifications are sent to the different nodes that will handle the different record validation nodes and provide the necessary information for each task. Every time a state change is notified, the nodes are in charge of validating if the information is correct and if the measured variables meet the necessary requirements for the validation to be correct. Yes, the validation of all the blocks is correct, the entire record is stored in a log that is subsequently processed by Big data. Data analysis aims to generate knowledge about the results and serves to improve each process and look for possible weak points in the chain.

**Figure 4.** Block diagram about an IoT data validation process with Blockchain.

### 3.1. IoT on a University Campus

The previous concepts allow establishing how a campus works and technology, however, it is important to understand how these are integrated to improve the processes of the environment. College campuses generally include a lot of technology that supports learning and campus development. The penetration of technology on campus is so great that it can even be compared to small cities [45]. The distribution of campus allows establishing plans to improve issues such as sustainability, mobility within the campus, security, etc. [46]. All these plans include human, economic and technological resources and respond to the existing needs of the environment and people. An example of this is sustainability, a term that encompasses a lot and changes the way ecosystems relate to nature [47]. This obliges the governments of each university campus to create models that
allow improving resource management considering components such as mobility, waste management, energy, buildings, security, etc. [48]. For this, it is necessary to include technologies that improve the management of all resources and increase the quality of life for campus members.

The IoT through its devices is responsible for improving the use of resources, an example of this is the monitoring and control of different buildings. This allows reducing energy consumption through the creation of autonomous environments, where the majority of variables are monitored and the actuators take control to avoid waste in consumption [23]. A basic example is turning lights and equipment on and off. This through presence sensors and computer systems ensures that what is absolutely necessary is used [49]. Other areas such as process management have included the use of IoT devices for their tasks. These provide value by acting as virtual assistants who are responsible for improving the process and reducing the involvement of people [17]. Even the IoT serves as a learning assistant involving the use of devices to ensure that the learning methods of a classroom are appropriate for a group of students.

The IoT has become a technology with great potential in educational environments and even more so on university campuses. The deployment of IoT uses the campus infrastructure, this implies that it uses the campus infrastructure resources, both at the network and computing level. In Section 2.1, the network model that a campus uses is detailed, this allows determining the communication protocol that exists, as well as the technologies used for communication. Security also responds to this infrastructure since it depends on layers 2 and 3 to establish all the requirements for access and exit to the Internet that IoT devices need. In computing, university campuses generally have their own data centers, this allows most services to be processed locally. In other words, most of the services included in the IoT are managed through a centralized model or client-server model. Figure 5, establishes the architecture of a campus that integrates emerging technologies such as IoT, big data, and cloud computing [50]. This integration guarantees the digitization of campus and offers a personalized service to its members. This architecture combines the services integrated into the network and infrastructure of a traditional campus.

![Figure 5](image_url)

**Figure 5.** Architecture of a university campus with the integration of the Internet of things.

The vulnerabilities found in this architecture and that affect the use of IoT are presented in Table 1. The data that supports the table have been obtained from a query made to the IT department of the university that participates in this study. In the column of vulnerabilities, the problems encountered are
mentioned according to various attacks that were detected in 2019 and of which a history is kept that serves to take protective measures. The relationship between vulnerability and the attack methodology they have undergone is highlighted in the column of a possible attack. Likewise, the negative characteristics found by the experts according to vulnerability are described. The security level column is a field that has been considered to determine the risk of this happening and the rating is low, medium and high. The low value is given to a vulnerability that can be controlled directly from the network infrastructure. However, the concept and usefulness of the devices are based on the high use of the Internet, which makes it a technology that presents a medium and high-level risk.

| Vulnerability                              | Possible attack                                                                 | Level of insecurity |
|-------------------------------------------|--------------------------------------------------------------------------------|---------------------|
| Weak, predictable or in-code passwords    | Brute force attack                                                             | High                |
| Insecure network services                 | Allow unauthorized control remotely                                            | High                |
| Insecure interface ecosystem              | Security issues in web, mobile, cloud, or API interfaces                      | Medium              |
| Lack of secure update mechanisms          | Lack of firmware validation on the device, lack of security in shipping (unencrypted transit) | Medium              |
| Insufficient privacy protection           | Personal user information stored on the device or in the environment to which the device is connected that is used in an unsafe, inappropriate or unauthorized manner | High                |
| Data transfer and storage in an unsafe way| Lack of encryption or access control for sensitive data that is within the ecosystem | Medium              |
| Lack of management controls              | Lack of security support in devices released to production, system monitoring and response capabilities | Low                 |
| Unsafe default configuration              | Unsafe default settings on devices without the possibility of making the system more secure | High                |
| Lack of hardening                         | Lack of measures to strengthen the devices from the physical point of view    | Medium              |

3.2. Blockchain Requirements

To define the security architecture for IoT using blockchain technology, it is important to determine its components. This information is useful in determining the changes or updates to be made to the campus architecture [41]. First, it must be recognized that not all blockchain models are the same. In general, it is classified into four groups, public, private, federated and Blockchain as a service (BaaS). Its main differences are the administration model, the level of decentralization or the degree of transparency, among other characteristics [44]. This work corresponds to a private blockchain, however there are certain components that all blockchain models have in common. The three key components in the blockchain function are its participants, assets, and transactions.

3.2.1. Participants

The participants are those groups that are going to be part of the digital solution with blockchain. These include the people who administer the network to the end-users, going through all the areas that have participated in the processes that the IoT uses for its management. To measure the level of each participant, the following questions are asked: What are the permissions that they will have on the network? How will you interact with the system? Will you have access to a copy of the entire chain? Will you be able to see only the transactions in which you participate or will you have access to more information? What are the transactions you can make? Depending on the answers to these questions, participants may or may not receive a copy of the entire chain and they may or may not have permission to view and validate transactions [42]. Only the participants who have a copy of the chain are considered nodes, the rest will generally access it through a web service or a mobile application, they are simply users.
3.2.2. Assets

Once the participants are identified, it is necessary to know what they are going to exchange through the blockchain network. The way to understand this group is to think that when the participants make a transaction, on many occasions they are transferring something. That “something” is the asset, and it can be a document, a certificate, a report, a token, a digital currency, etc. It is important to note that heavy documents are not stored on the blockchain. For their storage, databases connected to the blockchain are used, which allows registering their modifications without any limitation in infrastructure. This is motivated by efficiency issues since all the nodes have an updated copy of the chain and the inefficiency is directly proportional to the weight of the chain.

3.2.3. Transactions

Transactions define the rules to be applied in the blockchain process. Transactions are the way in which any modification is recorded, from changing a user’s permissions in the system to issuing a certificate or sending an economic transfer. They can also be seen as the operations by which participants create, exchange, modify or destroy assets.

3.3. Integration of Blockchain Technologies with IoT

Currently, the IoT generates a large volume of data processed by its devices, all supplied in a chain and exposed to the attack of cyber criminals. It is when the possibility arises to take advantage of the Blockchain architecture to authenticate, standardize and protect the adoption of data handled by the devices [40]. For the security of the IoT, the blockchain is capable of monitoring the information collected by the sensors, without allowing them to be duplicated by any wrong data [51]. Sensors can transfer data using Blockchain technology, without the need for a trusted third party. In addition, device autonomy, data integrity, virtual identity and point-to-point communication (P2P) are added, getting rid of technical deficiencies and bottlenecks.

In the proposed architecture, the blockchain acts as an intermediate piece of software, responsible for facilitating interaction between the components of the IoT system and with the rest of the world. This provides two fundamental elements, the separation of the more complex parts of the IoT (the physical part and the communications) and the possibility of offering blockchain-based services, such as automatic payments [52]. Integration is done by including a layer that manages the blockchain process. In architecture it is located between, the communication layer and the data processing and analysis layer, this offers universal access between technologies and services.

The blockchain layer includes several components that guarantee security in IoT processes [20]. It is important to establish that a segment of the network of the university campus has been separated for this architecture. This segment is responsible for the management of IoT devices and executes various processes that help the management of the campus. With this segmentation a scalable and modular architecture is executed, this facilitates the evaluation of the process and data transport. Without a doubt, this allows the deployment to be generated in a controlled environment that will easily be replicated in larger environments [53]. In Figure 6, the blockchain layer and each component of the layer are presented where each one is in charge of a specific task for the availability of the technology.

![Figure 6. Blockchain layer and its components for integration to IoT technology.](image-url)
3.3.1. Data Acquisition

This layer integrates the devices deployed on the university campus, these devices are sensors, actuators, cameras, etc. Various sources of data are included in the distribution of the layers of the university campus architecture. For the new architecture, only IoT related data sources are considered, traditional or structured data sources are still aligned to the normal architecture. The data acquisition layer wraps the encrypted data with a digital signature through asymmetric cryptographic algorithms and hash functions [54]. These consecutively connected data blocks form the blockchain after distributed validation. Cryptographic and hashing algorithms depend on the blockchain platform used. For example, the Bitcoin blockchain chooses SHA-256 as the hash function and the elliptic curve digital signature algorithm (ECDSA) as the signature algorithm.

3.3.2. Network

The network component is essentially a P2P network superimposed on the campus network architecture. This network runs at the top of the communication layer. The overlay network consists of virtual or physical links connecting nodes in the underlying communication networks, that is, wired/wireless communication networks.

This layer allows the communication of the nodes that make up the blockchain between the physical and virtual links. In addition, it provides a method of propagating the data blocks to the rest of the network. Each node is responsible for verifying the correctness of the received block and propagating it to its neighboring nodes. A node simply transmits the transaction block to its connected peers. Once you receive the transaction block, other peers will verify it locally. If valid, the block will propagate further to other nodes through the overlay network.

3.3.3. Consensus

This component is primarily responsible for distributed consensus for the trust of a block. Consensus can be achieved using various algorithms such as PoW, PoS, PBFT, and DPOS. It is important to consider that block propagation mechanism, such as relay network propagation and advertisement-based propagation, are the prerequisite for distributed consensus protocols. Consensus, and fundamental in all blockchain, is where the automation of trust in the data to be incorporated lies. There are also several mechanisms to achieve consensus between the nodes, and it is one of the elements that most differentiates blockchain from others.

3.3.4. Incentives

Blockchain mining occurs in this component and is responsible for tasks such as digital currency issuance, digital currency distribution, reward mechanism design, transaction cost management, etc. Every blockchain must have a consensus mechanism that rewards nodes that strive to execute consensus algorithms. This makes sense because, without these rewards, the nodes would not have to validate the blocks that do not belong to them [21]. In this component, it is essential to correctly carry out the calculation and accounting of these cryptocurrencies [42].

In this architecture that is applied to a university campus, the validation process does not have a monetary reward since everything is part of an internal campus process. in addition, all parties involved with part of the university. However, this layer has been established so that when replicating it in environments where a reward is needed for validation.

3.3.5. Services

The service component provides users with blockchain-based services for various areas such as industrial sectors, supply chains and public services. This layer opens the entire environment to the integration with applications and organizations in a standard and orderly manner.
3.4. Architecture for Managing IoT Through Blockchain

In Figure 7, the architecture that allows the management of IoT through blockchain is presented. This architecture allows the assurance in the processes of the IoT devices that are located distributed on a university campus. As mentioned in the previous section, the integration of these technologies in a controlled environment allows for a modular and phased implementation. This guarantees the proper functioning of all the services provided by the campus. Furthermore, this architecture is developed with a generic vision, whose replication in other environments is totally practical [20]. The architecture is made up of five layers, each with a specific function. These functions range from the acquisition of data to the exploitation of the knowledge generated through its analysis.

![Figure 7. Blockchain integration in a university campus architecture for IoT security.](image)

3.4.1. Interaction and Event Capture Layer

The interaction and event capture layer is in the lower part of the architecture but it is the most important for this work. Various concepts related to data acquisition are integrated into this layer. On the one hand, there are the computer systems that the university has, these systems generally handle academic and financial information of the students and the processes for the administration of the campus [32]. These systems interact with members of the campus through applications that have interfaces that allow the user to make any request and the event is stored in a distributed database.

On the other hand, there is the IoT technology that allows obtaining data on everything that happens in the environment through various devices such as sensors, actuators, etc. These devices are directly related to the environment and interact with the user or between devices [47]. The availability of devices allows their use in various areas of the campus and develop common tasks, such as monitoring a variable or even being included in sophisticated processes such as the process of acquiring a supply autonomously. Among the campus processes that use IoT devices are:
• Access control systems. Security on the university campus is controlled by biometric-type sensors or RFID readers. By detecting any event, the sensors activate the different actuators strategically located on the smart campus.

• Automation systems. The university infrastructure is complemented directly with autonomous systems. These systems seek to reduce energy waste, as well as improve the quality of life of the university population. Several of these systems are integrated into a cognitive system, which helps to manage resources efficiently.

• Security systems. Security is vital on a university campus for them there are sensor systems or video surveillance systems that generate information about any event 24 h a day. The potential of these systems allows their data to be used for other activities, such as detecting trends or identifying the special needs of the population.

This work focuses specifically on the management of IoT technology because, by the nature of its operation, it is necessary to provide the system with a security method that guarantees the care of the information. Systems not considered as part of IoT technology follow the traditional process and are part of the security systems of the campus network infrastructure.

3.4.2. Communication and Storage Layer

In this layer, the communication represented by the data network of the campus and storage has been unified. This union is due to the close relationship between the transport of data and the way and place where it is stored. The data network responds to an enterprise network architecture composed of the access, distribution and core layer. Transportation is done mainly through the IPV4 protocol that provides sufficient characteristics for campus management [55]. The communication model is both physical and wireless, most physical communication is available to end-users who have static hosts as well for services that need a physical interface for communication. Due to a large number of campus members and the geographical extension, the use of wireless communications is essential to provide the service to all users [56].

Network security is provided by specific equipment for the care of information through firewalls, intrusion detection systems, intrusion prevention systems, DMZ, proxies, etc. The data network is responsible for transporting data from the data capture layer and storing it on local media that is contained on virtual servers in a campus data center. Another storage medium is sending data to public or private clouds. University campuses generally store data centrally and provide access to all campus systems. With the inclusion of IoT, several of the services need to be stored in public clouds for information analysis. This information is the one that needs techniques and protocols that guarantee the security of the information [30].

3.4.3. Blockchain Layer

This layer is included in the architecture of a university campus in order to provide security for IoT management. Blockchain technology in the IoT allows solving the scalability, reliability and privacy. It allows coordination between devices, in addition to tracking all connected and processing transactions. It maintains a decentralized approach that implements cryptographic algorithms so that user data is effectively private [57]. This approach eradicates failure and offers a resilient ecosystem.

Blockchain records digital interactions so that they are executed in a secure, auditable, transparent, efficient and interruption resistant manner. Each block records the operations with a timestamp and it is verified that they are incorrect sequence, without manipulations. If someone wants to add a transaction to the chain, everyone participating in the network validates it through an algorithm; the approved transactions are put together in a block and distributed to each node in the network. The new block is validated and the successive ones integrate a unique fingerprint corresponding to the previous block [54]. IoT devices within campus generate high volumes of transactions. By adopting a standardized communication model, P2P, the costs of Big Data management are reduced. So that
there is no theft and impersonation in every transaction that is carried out a consensus and validation. P2P communications guarantee the privacy and security of large IoT networks.

Based on all the devices that can communicate with ledgers, taking hold in Blockchain, the devices used in IoT end up being safe in transactions. The information provided by the user can be tracked so that the experience is fluid and continues as private and inviolable [43]. Also, by using storage and encryption, each part of the chain can trust the data. All the heavy lifting falls on technology, through machines, without the need for a person to run the processes. Blockchain solves the issues of scalability and trust. The keys are private and no one will be able to overwrite the codes, thus providing security in IoT operations.

3.4.4. Data Processing and Analysis Layer

The existing data sources in a smart campus directly influence data management [58]. For this reason, it is important to use tools capable of carrying out a quality process in data extraction and loading, considering adequate processing times [59]. The method considered cost-based, infrastructure availability is Hadoop, which is an open-source framework for storing data and running applications in clusters. Hadoop provides massive storage for any type of data, has enormous processing power, and processes virtually unlimited concurrent tasks or work [60]. The explanation of this layer is not considered in more detail since the topic covered in this work is IoT security. However, it is a very important layer within the architecture of the university campus. The authors have extensively developed data analysis using big data in the following papers [18,46,61].

3.4.5. Services Layer

Within the university campus, technological integration provides various services that contribute to the operation of the campus. These services are classified into two groups, the first group is responsible for everything related to administrative management and the second group is responsible for academic management [62]. The framework contributes to administrative management in environments such as human resources, where it provides more efficient management in organizational processes [49]. In addition, it can be used to develop tests for the evaluation and selection of candidates or the development of resources for the development of transversal competences [45]. In academic management, architecture offers new information about students and teachers in the areas of marketing and admissions to make strategic decisions in the educational model. In the learning environment, it applies its own data analysis techniques to optimize educational management, learning and student care, supporting personalized education.

4. Results

The results present the application of the architecture in a specific area, the purpose is to evaluate the operation and if it is pertinent to use the blockchain in the inventory management of the university campus. The scenario was raised specifically in the area of acquisitions were generally most universities handle a similar process. The process of acquiring assets and materials such as laboratory equipment, office supplies, or cleaning supplies involves a written or digital request to the procurement department. This request contains personal information, the requested asset or material and the cost thereof. The request is reviewed by procurement managers and authorized for purchase if available to do so. As soon as the asset or material is withdrawn by the person who requested it, it remains under their protection and as of this moment, this person is responsible for the resource, as well as for its proper use. The university participating in this study has implemented an inventory management system that runs on different devices and manages the processes described above efficiently and safely. Table 2, shows the requirements that the acquisition of assets or materials through IoT meet.
Table 2. Requirements for implementing an IoT and blockchain process in a supply chain.

| Question                                                                 | Response | Justification                                                                                                                                 |
|--------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Is a traditional database insufficient to cover the needs of the project? | Yes      | There is a need to eliminate intermediaries, it is desired that the system be decentralized to increase the availability                        |
| Can multiple writers be identified for the system?                        | Yes      | The writers in the project are the worker and supplier since the others would be unnecessary in the solution                                  |
| Is it possible that the data is replicated on different nodes?            | Yes      | There are no limitations on the fact that the information is confidential and cannot be replicated on different nodes                      |
| Do you want to eliminate trusted intermediaries?                         | Yes      | The only participants should be the workers and suppliers, the other intermediaries currently participating in the process can be eliminated |
| Is it possible to identify who will take the role of validator in the system? | Yes      | It is not a good idea to force every user (node) using the system to be a validator. The most viable alternative would be to designate a group of nodes responsible for writing the blockchain |
| Does the system involve transactions that are dependent?                 | Yes      | For example, it is not possible to carry out a transfer transaction between workers if previously there is no transaction that involves the receipt of the goods by the worker who transfers the goods |
| Does the system require the data to be immutable?                        | Yes      | It is necessary to know the different transactions that have occurred throughout the useful life of a good                              |

Once the necessary rules for supply chain applications have been identified, the application environment is detailed. Architecture is evaluated in the acquisition of perishables for the gastronomy school. The school requires for its classes and laboratories, the purchase of perishable products that are certified as fresh products that must be kept at a certain temperature throughout the tour. With this objective, periodic control of the temperature is carried out every 20 min in the container in which the products are transported. If products arrive having the “fresh products” certificate and without having exceeded the required temperature, the university, through the financial department, will make the agreed payment to the supplier company. Table 3, presents the participants in the acquisition process.

The complete process is presented in Figure 8, where the process has been listed in order to identify each of the steps and the transaction that takes place in each of them.

- 1. Shipment of cargo, the provider sends the shipment and notifies the blockchain that the transaction has been executed
- 2. Temperature control, the IoT device placed inside the container measures and sends the temperature value to the blockchain every 20 min
- 3. Sanitary and product quality inspection, the gastronomy school verifies that the product is in the required conditions and issues the certificate “fresh products” that are registered on the blockchain
- 4–7. Temperature control, the IoT device placed inside the container measures and sends the temperature value to the blockchain every 20 min
- 8. Receipt of cargo, the container arrives at the university reception point, issuing the corresponding notification on the blockchain
- 9. Payment of the shipment, the financial department that had the money withheld releases it in favor of the provider
Figure 8. Blockchain process in the purchase of perishable products with the management of IoT devices.

Table 3. Members of the acquisition process in an IoT and blockchain environment.

| Members         | Areas                              | Detail                                                                 |
|-----------------|------------------------------------|------------------------------------------------------------------------|
| Participants    | University                         | Purchaser                                                             |
| Provider        | Provider                            | Perishable product sales company                                      |
| Finance department | Finance department                | Payment area, belongs to the university                               |
| IoT device      | IoT device                          | Temperature, humidity sensors, etc.                                    |
| Certifying entity  | Certifying entity                | School of gastronomy                                                  |
| Audit entity    | Audit entity                        | Procurement area, belongs to the university                            |
| Assets          | Certificate (fresh product)        | They are emitted by IoT devices                                       |
|                 | “Ideal temperature” certificate, history of temperature evolution | They are emitted by IoT devices                                       |
| Transactions    | Notification of shipment of the shipment | Supplier company                                                      |
|                 | Payment deposit notice             | Finance department                                                    |
|                 | Issuance of the fresh produce certificate | School of gastronomy, belongs to the university                      |
|                 | Temperature measurement            | They are emitted by IoT devices                                       |
|                 | Notification of receipt of cargo    | University                                                            |
|                 | Notification of payment completion  | Finance department                                                    |

The Figure illustrates how transactions are generated as the container travels from the provider to the university. In this case, each transaction is a block. At the bottom of the figure, it is shown how of the five participants, only the provider and the university have access to all the information of the blockchain while the IoT device, the financial department and the sanitary inspector only have access to the information that they provide to the blockchain.

With this implementation it is possible to evaluate the different layers of the architecture of the university campus that was updated with an additional layer that is responsible for the management of Blockchain. The sensors that have been added in for data acquisition are governed by embedded systems that are in charge of managing all the variables that need to be measured in the process. These systems belong to the data acquisition layer managed by the IoT. The sensors capture the events and the embedded system is in charge of managing the reading times, as well as cleaning the signals. Systems send the data to the cloud computing layer where it can be processed to simply stored for further processing or analysis at a higher layer. In this specific application the data is stored in a local cloud that is located in the data center of the university campus. The Blockchain layer makes requests to the storage layer to create a specific storage location for the blocks in the chain. Each block is created with a hash of the previous block that stores the location and each temperature reading made by the sensors.
The complete chain is saved in each node of the network that makes up the Blockchain, so an exact copy of the chain is stored in all the network participants that have been detailed above. Subsequently, the request passes to the processing layer that uses a Big data architecture, which is responsible for checking the chain and the participants for sending notifications and requests for review or mining. This validation is done by users at the application layer when it comes to a smart contract or inspection. This process is repeated as many times as necessary or as requested by the verification chain. The results go back to the data analysis and processing layer where the data is worked through Big data in order to generate knowledge about the operation of the blockchain and improve processes or create projections for future processes.

5. Discussion

The integration of a blockchain layer in the university campus architecture allows it to be transformed in such a way that the security of the IoT processes that manage various tasks on campus is guaranteed. Works that deal with the subject do not clarify the operation of blockchain in the IoT process. In addition, these works focus on attempts at how technologies will be integrated in the future to generate secure environments that support the good use of information. This work highlights the inclusion of blockchain in an environment that had already been managing IoT in its processes. Being able to validate the use of blockchain in a real environment, allows the architecture to adapt to similar environments or to be the step to ecosystems such as smart cities.

Another analysis that has been determined with this implementation is the feasibility of using any IoT device, something that was restricted on campus due to the low levels of security that these have. By guaranteeing security, it is possible to continue integrating new technologies and data sources to the blockchain. This undoubtedly turns a traditional campus into a smart campus where emerging technologies such as IoT, cloud computing, blockchain, big data and artificial intelligence are integrated.

6. Conclusions

Universities, in addition to being educational centers, are research and innovation centers par excellence. This has been demonstrated by the current circumstances, since the world is going through a pandemic (COVID-19) and the universities have been present in search of solutions to all this problem. For this, the key has been the integration of technologies, since they have kept us in communication in search of solutions through agile and efficient processes. The new normality that countries live requires all the technological potential available with greater autonomy and intelligence, with the ability to make decisions in favor of humanity and sustainable development. Organizations and large cities must adopt plans that require the care of people. Where, IoT devices become the senses of ecosystems and are intended to collect data that can be analyzed in real time to make timely and accurate decisions. The development of this work serves as a test bed for large organizations and why not, smart cities that increasingly trust technologies like IoT but doubt the security it offers. By integrating it with Blockchain, IoT has the ability to protect data and it is guaranteed that each process, such as the acquisition of supplies, generates several records that are verified and validated by several nodes, making it impossible to modify the existing information throughout The whole process.

For this work, the infrastructure already deployed on a university campus was considered, this infrastructure adheres to the description of what an intelligent campus is. A smart campus, with the objective of satisfying the needs of all its members in a personalized way, already includes several layers that are specifically in charge of an action. For this reason, it was necessary to include an additional layer that is directly responsible for the management of Blockchain, this allows that each request that goes from the storage layer to the data processing layer is secured and validated by the existing registry nodes.

For the implementation it was necessary to segment certain areas in the campus data network. The area chosen for this implementation was procurement, the reason was to improve the process
carried out for the acquisition of some good or supply. Depending on approvals or various bureaucratic procedures, requests often arrived when they were no longer necessary or simply the process was lost on the way, this generated economic losses for the university, in addition, it was a process that required many human resources. When using IoT devices in the acquisition of supplies or products, several points that were registered or evaluated by several people went out of the chain. This from a financial point of view already generated economic savings in human resources. With the help of Blockchain, the process could be evaluated by several nodes, keeping a copy of the data in each one of them, therefore parameters such as quantity, temperature, times, etc., cannot be modified, guaranteeing correct acquisition, as well as, the quality of products.

As you can see, there is enormous potential to develop Blockchain applications in IoT solutions, this combination can solve the main problems that limit the adoption of IoT, such as security and scalability. Blockchain that have smart contracts built in can improve security and trust, and can automate entire processes that are made up of various business partners. However, there are some challenges that must be overcome. One of the main challenges of blockchain-based IoT applications is the limited computing power of many IoT devices. In our research, this problem has been solved by having a local cloud computing model.

**Author Contributions:** W.V.-C. contributed to the following: the conception and design of the study, implementation of the architecture, writing of the article and approval of the version presented. The authors M.R.-C. and W.V.-C. They contributed to the design of the platforms, the formal analysis of the research and the validation of the results. The author X.P.-P. made the following contributions to the study: performance evaluation, data analysis and interpretation, approval of the submitted version. All authors read and approved the final manuscript.

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

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

**References**

1. Butz, P.; Tauscher, B. Emerging technologies: Chemical aspects. *Food Res. Int.* **2002**, *35*, 279–284. [CrossRef]
2. Montori, P.; Bedogni, L.; Bononi, L. A Collaborative Internet of Things Architecture for Smart Cities and Environmental Monitoring. *IEEE Internet Things J.* **2018**, *5*, 592–605. [CrossRef]
3. Alvarez-Campana, M.; López, G.; Vázquez, E.; Villagrá, V.A.; Berrocal, J. Smart CEI moncloa: An iot-based platform for people flow and environmental monitoring on a Smart University Campus. *Sensors* **2017**, *17*, 2856. [CrossRef]
4. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]
5. Shwe, H.Y.; Jet, T.K.; Chong, P.H.J. An IoT-oriented data storage framework in smart city applications. In Proceedings of the International Conference on Information and Communication Technology Convergence, ICTC 2016, Jeju, Korea, 19–21 October 2016; pp. 106–108. [CrossRef]
6. Madakam, S.; Ramaswamy, R.; Tripathi, S. Internet of Things (IoT): A Literature Review. *J. Comput. Commun.* **2015**, *3*, 164–173. [CrossRef]
7. Bellagente, P.; Ferrari, P.; Flammini, A.; Rinaldi, S. Adopting IoT framework for Energy Management of Smart Buildings: A real test-case. In Proceedings of the IEEE 1st International Forum on Research and Technologies for Society and Industry, Turin, Italy, 16–18 September 2015; pp. 138–143. [CrossRef]
8. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 481–518. [CrossRef]
9. Zhou, J.; Zhou, Y.; Wang, B.; Zang, J. Human–Cyber–Physical Systems (HCPs) in the Context of New-Generation Intelligent Manufacturing. *Engineering* **2019**, *5*, 624–636. [CrossRef]
10. Zhou, J.; Li, P.; Zhou, Y.; Wang, B.; Zang, J.; Meng, L. Toward New-Generation Intelligent Manufacturing. *Engineering* **2018**, *4*, 11–20. [CrossRef]
11. Baicun, W.; Jiyuan, Z.; Xianming, Q.; Jingchen, D.; Yanhong, Z. Research on New-Generation Intelligent Manufacturing based on Human-Cyber-Physical Systems. *Chin. J. Eng. Sci.* **2018**, *20*, 29. [CrossRef]
12. Aazam, M.; Khan, I.; Alsaffar, A.A.; Huh, E.N. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In Proceedings of the 11th International Bhurban Conference on Applied Sciences and Technology, IBCAST, Islamabad, Pakistan, 14–18 January 2014; pp. 414–419. [CrossRef]

13. Mahmoodi, Y.; Reiter, S.; Viehl, A.; Bringmann, O.; Rosenstiel, W. Attack surface modeling and assessment for penetration testing of IoT system designs. In Proceedings of the 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 29–31 August 2018; pp. 177–181. [CrossRef]

14. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the International Conference on Computer Science and Electronics Engineering, ICCSEE, Hangzhou, China, 23–25 March 2012; Volume 3, pp. 648–651. [CrossRef]

15. Ray, P.P. A survey of IoT cloud platforms. Future Comput. Inf. J. 2016, 1, 35–46. [CrossRef]

16. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future internet: The internet of things architecture, possible applications and key challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, FIT 2012, Islamabad, India, 17–19 December 2012; pp. 257–260. [CrossRef]

17. Liu, M.; Li, L. The construction of smart campus in universities and the practical innovation of student work. In Proceedings of the International Conference on Information Management & Management Science, Chengdu, China, 24–26 August 2018; pp. 154–157. [CrossRef]

18. Villegas-Ch, W.; Palacios-Pacheco, X.; Luján-Mora, S. Application of a Smart City Model to a Traditional University Campus with a Big Data Architecture: A Sustainable Smart Campus. Sustainability 2019, 11, 2857. [CrossRef]

19. Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 2018, 14, 352. [CrossRef]

20. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. Internet Things 2018, 1–2, 1–13. [CrossRef]

21. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 2019, 19, 326. [CrossRef]

22. Uskov, V.L.; Bakken, J.P.; Pandey, A. Smart University Taxonomy: Features, Components, Systems. In Smart Education and e-Learning; Springer: Cham, Switzerland, 2016; Volume 59, pp. 3–14. [CrossRef]

23. Popoola, S.I.; Atayero, A.A.; Okanlawon, T.T.; Omopariola, B.I.; Takpor, O.A. Smart campus: Data on energy consumption in an ICT-driven university. Data Brief 2018, 16, 780–793. [CrossRef]

24. Popoola, S.I.; Atayero, A.A.; Badejo, J.A.; John, T.M.; Odukoya, J.A.; Omore, D.O. Learning analytics for smart campus: Data on academic performances of engineering undergraduates in Nigerian private university. Data Brief 2018, 17, 76–94. [CrossRef]

25. Prandi, C.; Monti, L.; Ceccarini, C.; Salomoni, P. Smart Campus: Fostering the Community Awareness Through an Intelligent Environment. Mob. Netw. Appl. 2019, 24, 1–8. [CrossRef]

26. Vasilieva, R.; Rodrigues, L.; Hughes, N.; Greenhalgh, C.; Goulden, M.; Tennison, J. What Smart Campuses Can Teach Us about Smart Cities: User Experiences and Open Data. Information 2018, 9, 251. doi:10.3390/info9100251. [CrossRef]

27. Dong, X.; Kong, X.; Zhang, F.; Chen, Z.; Kang, J. OnCampus: A mobile platform towards a smart campus. SpringerPlus 2016, 5. [CrossRef]

28. Nam, T.; Pardo, T.A. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, College Park, MD, USA, 11–12 June 2011; pp. 282–291.

29. Charles, D. Universities as key knowledge infrastructures in regional innovation systems. Innovation 2006, 19, 117–130. [CrossRef]

30. Abdabbah, S.B.; Ayachi, R.; Amor, N.B. Social Activities Recommendation System for Students in Smart Campus. Smart Innov. Syst. Technol. 2015, 76, 461–470. [CrossRef]

31. Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. Wirel. Pers. Commun. 2011, 58, 49–69. [CrossRef]

32. Hannan, A.; Arshad, S.; Azam, M.A.; Loo, J.; Ahmed, S.H.; Majeed, M.F.; Shah, S.C. Disaster management system aided by named data network of things: Architecture, design, and analysis. Sensors 2018, 18, 2431–2451. [CrossRef] [PubMed]

33. Li, S.; Xu, L.D.; Wang, X. Compressed sensing signal and data acquisition in wireless sensor networks and internet of things. IEEE Trans. Ind. Inf. 2013, 9, 2177–2186. [CrossRef]
34. Chen, X.Y.; Jin, Z.G. Research on Key Technology and Applications for Internet of Things. Phys. Procedia 2012, 33, 561–566. [CrossRef]
35. Barthel, R.; Leder Mackley, K.; Hudson-Smith, A.; Karpovich, A.; De Jode, M.; Speed, C. An internet of old things as an augmented memory system. Pers. Ubiquitous Comput. 2013, 17, 321–333. [CrossRef]
36. Rahmani, H.; Sahli, N.; Kamoun, F. Privacy in the Internet of Things: threats and challenges. Wiley Online Library 2011, 7, 2728–2742. [CrossRef]
37. Yaqoob, I.; Ahmed, E.; Hashem, I.A.T.; Ahmed, A.I.A.; Gani, A.; Imran, M.; Guizani, M. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wirel. Commun. 2017, 24, 10–16. [CrossRef]
38. Swan, M. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. J. Sensor Actuator Netw. 2012, 1, 217–253. [CrossRef]
39. Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the architecture of Internet of Things. In Proceedings of the ICACTE 3rd International Conference on Advanced Computer Theory and Engineering, Chengdu, China, 20–22 August 2010; Volume 5, pp. 484–487. [CrossRef]
40. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. Sensors 2018, 18, 2575. doi:10.3390/s18082575. [CrossRef]
41. Kshetri, N. Can Blockchain Strengthen the Internet of Things? IT Prof. 2017, 19, 68–72. [CrossRef]
42. Pilkington, M. Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations; Edward Elgar Publishing: Cheltenham, UK, 2016; pp. 225–253.
43. Cachin, C.; Schubert, S.; Vukolić, M. Architecture of the Hyperledger Blockchain Fabric. In Leibniz International Proceedings in Informatics; LIPIcs: Wadern, Germany, 2017; Volume 70, pp. 24.1–24.16. doi:10.4230/LIPIcs.OPODIS.2016.24. [CrossRef]
44. Teslya, N.; Ryabchikov, I. Blockchain-based platform architecture for industrial IoT. In Proceedings of the 2017 21st Conference of Open Innovations Association (FRUCT), Helsinki, Finland, 6–10 November 2017; pp. 321–329.
45. Gaglio, S.; Lo Re, G.; Morana, M.; Ruocco, C. Smart assistance for students and people living in a campus. In Proceedings of the International Conference on Smart Computing, Washington, DC, USA, 12–15 June 2019; pp. 132–137. [CrossRef]
46. Villegas-Ch, W.; Molina-Enriquez, J.; Chicaiza-Tamayo, C.; Ortiz-Garcés, I.; Luján-Mora, S. Application of a Big Data Framework for Data Monitoring on a Smart Campus. Sustainability 2019, 11, 5552. [CrossRef]
47. Boran, A.; Bedini, I.; Matheus, C.J.; Patel-Schneider, P.F.; Keeney, J. A smart campus prototype for demonstrating the semantic integration of heterogeneous data. In Web Reasoning and Rule Systems. RR 2011; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6902, pp. 238–243. [CrossRef]
48. D’Adamo, I.; Falcone, P.M.; Ferella, F. A socio-economic analysis of biomethane in the transport sector: The case of Italy. Waste Manag. 2019, 95, 102–115. [CrossRef]
49. Barbato, A.; Bolchini, C.; Geronazzo, A.; Quintarelli, E.; Palamarcu, A.; Piti, A.; Rottondi, C.; Verticale, G. Energy optimization and management of demand response interactions in a smart campus. Energies 2016, 9, 398. [CrossRef]
50. Pompei, L.; Mattoni, B.; Bisegna, F.; Nardecchia, F.; Fichera, A.; Gagliano, A.; Pagano, A. Composite Indicators for Smart Campus: Data Analysis Method. IEEE Int. Conf. Environ. Electr. Eng. 2018, 1–6. [CrossRef]
51. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an Optimized Blockchain for IoT. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
52. Huckle, S.; Bhattacharya, R.; White, M.; Beloff, N. Internet of Things, Blockchain and Shared Economy Applications. Procedia Comput. Sci. 2016, 58, 461–466. [CrossRef]
53. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, Kona, HI, USA, 13–17 March 2017; pp. 618–623. [CrossRef]
54. Rahulamathavan, Y.; Phan, R.C.; Rajarajan, M.; Misra, S.; Kondo, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 11th IEEE International Conference on
55. Nie, X. Constructing Smart Campus Based on the Cloud Computing Platform and the Internet of Things. In Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering ([ICCSEE]), Guangzhou, China, 22–23 March 2013; pp. 1576–1578. [CrossRef]

56. Luo, L. Data Acquisition and Analysis of Smart Campus Based on Wireless Sensor. Wirel. Pers. Commun. 2018, 102, 2897–2911. [CrossRef]

57. Kondaveeti, S.A.; Shekhar, S. Continuous Security in IoT Using Blockchain. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018; pp. 6423–6427.

58. Villegas-Ch, W.; Luján-Mora, S.; Buenaño-Fernandez, D.; Palacios-Pacheco, X. Big data, the next step in the evolution of educational data analysis. Adv. Intell. Syst. Comput. 2018, 721, 138–147. [CrossRef]

59. Ortiz-Garcés, I.; Yánez, N.; Villegas-Ch, W. Performance Data Analysis for Parallel Processing Using Big data Distribution. In Information Technology and Systems. ICITS 2019; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2019; Volume 918, pp. 602–611. [CrossRef]

60. Villegas-Ch, W.; Luján-Mora, S.; Buenaño-Fernandez, D. Towards the Integration of Business Intelligence Tools Applied to Educational Data Mining. In Proceedings of the 2018 IEEE World Engineering Education Conference (EDUNINE), Buenos Aires, Argentina, 11–14 March 2018; pp. 1–5. [CrossRef]

61. Villegas-ch, W.; Arias-navarrete, A.; Palacios-pacheco, X. Proposal of an Architecture for the Integration of a Chatbot with Artificial Intelligence in a Smart Campus for the Improvement of Learning. Sustainability 2020, 12, 1500. [CrossRef]

62. Yan, H.; Hu, H. A study on association algorithm of smart campus mining platform based on big data. In Proceedings of the International Conference on Intelligent Transportation, Big Data and Smart City, Changsha, China, 17–18 December 2017; pp. 172–175. [CrossRef]