smart cities

MDPI

Article

Conceptual Technological Framework for Smart Cities to Move towards Decentralized and User-Centric Architectures Using DLT

Victor Garcia-Font [1,2,3]

[1] Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Rambla del Poblenou 156, 08018 Barcelona, Spain; vgarciafo@uoc.edu or victor.garcia@urv.cat
[2] Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili (URV), Av. Països Catalans 26, 43007 Tarragona, Spain
[3] CYBERCAT—Center for Cybersecurity Research of Catalonia, Rambla del Poblenou 156, 08018 Barcelona, Spain

Abstract: Nowadays, many urban areas are developing projects that are included within the area of smart cities. These systems tend to be highly heterogeneous and involve a large number of different technologies and participants. In general, cities deploy systems to integrate data and to provide protocols to ease interconnectivity between different subsystems. However, this is not enough to build a completely interoperable smart city, where control fully belongs to city administrators and citizens. Currently, in most cases, subsystems tend to be deployed and operated by providers creating silos. Furthermore, citizens, who should be the center of these systems, are often relegated to being just another participant. In this article, we study how smart cities can move towards decentralized and user-centric systems relying on distributed ledger technologies (DLT). For this, we define a conceptual framework that describes the interaction between smart city components, their participants, and the DLT ecosystem. We analyze the trust models that are created between the participants in the most relevant use cases, and we study the suitability of the different DLT types.

Keywords: smart cities; blockchain; distributed ledger technology; framework; user-centric decentralization

Citation: Garcia-Font, V. Conceptual Technological Framework for Smart Cities to Move towards Decentralized and User-Centric Architectures Using DLT. *Smart Cities* **2021**, *4*, 728–745. https://doi.org/10.3390/smartcities4020037

Academic Editor: Renita Murimi

Received: 22 March 2021
Accepted: 12 May 2021
Published: 14 May 2021

1. Introduction

In recent years, many metropolitan areas have deployed so-called smart city projects to be able to more efficiently deal with typical urban problems, such as population growth, mobility, or sustainability [1]. Smart cities are usually considered highly heterogeneous environments, where a combination of different participants (e.g., public administrations, providers, and citizens), technologies, and protocols (e.g., traditional web technology, IoT, and wireless communications) meet.

In general, one of the goals of public administrations with their smart city initiatives is to eliminate silos and to integrate projects from different areas into a common framework that facilitates the incorporation of new projects and participants into the same technological and procedural ecosystem, facilitating integration and data transmission between systems [2,3]. Moreover, many initiatives also aim to put citizens at the center of the model. From a data perspective, this implies that citizens have to be able to control their personal data and to audit public administrators and their providers in a reliable manner. Blockchain can be key to this approach. Since the first blockchain was proposed in 2008 as part of the Bitcoin cryptocurrency [4], this technology has evolved dramatically. Nowadays, cryptocurrencies are just one of its use cases and many other applications require a blockchain as a central component. Among others, blockchains are being used in the supply chain [5], in the art market [6], in real estate [7], as an integration tool for the Internet of Things (IoT) [8], etc. From a technological point of view, distributed ledger technologies

(DLT) is the more general term used to refer to blockchains, since other proposals with similar goals do not use a chain of blocks as a data structure. In this way, a DLT acts as a digital ledger administered in a distributed manner, where data can only be appended but never modified or deleted. Moreover, DLT have evolved from completely public and permissionless systems, such as Bitcoin, where any person can send monetary transactions and, even, join the network to contribute in the ledger management to more private and permissioned systems, where users have to be granted special permission to participate in any way. This creates systems where trust models are very different from conventional hierarchical structures of centralized systems or the peer-to-peer systems, where users build trust relationships directly with a counterparty. As we see below, DLT can be deployed in a way where governance is open to anyone or closed to a reduced group. Additionally, DLT can be more or less transparent, where users may require special permission to access data. In this way, some DLT allow anonymous or pseudo-anonymous interactions among users, similar to that in cryptocurrencies, and others require well-defined identities for any participant, similar to in supply chain systems. Thus, the different DLT types create different trust models and have specific requirements that can be adequate or not in different contexts.

In a smart city, DLT can be used in many business areas for many different purposes. In this paper, we focus on a typical smart city scenario with three basic participants: public administrators, service providers, and citizens. Other smart city scenarios that do not include these three participants fall out of the scope of this paper. For example, smart city projects related to the collaborative economy, where citizens interact directly with each other. Taking this into account, the contributions of this paper are as follows:

- The paper describes to a non-technical audience the basic principles of DLT that can enable user-centric smart cities. To this end, Section 2 gathers background information to contextualize the rest of the paper. Basically, this section focuses on describing the most relevant properties of different DLT types and introduces the smart city. Section 3 highlights the importance of building user-centric systems and reviews relevant initiatives in smart cities.
- The paper defines a conceptual technological framework aimed at administrators, decision-makers, and other smart city stakeholders. The goal of the proposed framework is to aid these actors in understanding the key role that DLT can play in building user-centric systems in a highly complex scenario such as the smart city. The proposed framework follows the current trend in the blockchain space, where multiple DLT have to coexist in an interoperable way. Unlike other previous work, this conceptual framework takes a holistic view of the smart city, instead of proposing a particular solution to deploy a specific use case. In this way, the framework helps to visualize the interactions between smart city components, its participants, and the trust requirements that this entangles. The framework is defined in Section 4.
- Currently, most blockchain-based smart city projects are still in their infancy and highly fragmented. In Section 5, we review prominent initiatives in the smart city and prominent use cases from other contexts that can eventually be implemented in the smart city. In Section 6, we discuss trust issues of the selected use cases and evaluate the suitability of their implementation, taking into account different DLT types.

2. Background

This section describes the necessary background to understand the context of this paper. First, we introduce blockchain and DLT types in Section 2.1. Subsequently, we list the main characteristics of the smart city projects in Section 2.2. Nowadays, there are many types of smart cities and, here, we aim to gather the common characteristics that are relevant for the analysis in this paper.

2.1. Distributed Ledger Technologies

Blockchain technology was first described in the Bitcoin white paper [4] in 2008. At the beginning of 2009, the first Bitcoin node went live on the Internet and generated the

genesis block of the chain. Bitcoin demonstrated empirically that it was possible to enable a digital payment system that did not need a large intermediary to manage payments. Soon after, researchers around the world came up with ideas to use a blockchain in other contexts beyond payments. This led to proposals to create general purpose blockchains that could handle sophisticated use cases. Ethereum [9] is the most prominent blockchain of this type. The programs implemented on this type of blockchains are called smart contracts. These are computer programs that write a deterministic result on the blockchain depending on external inputs. These, together with other mechanisms, such as a user interface and a data storage protocol, enable so-called decentralized applications (DApps).

Nevertheless, the first blockchain platforms, such as Bitcoin or Ethereum, have several disadvantages compared to conventional computer systems that make them not suitable for all types of applications. For example, these platforms accept a reduced number of transactions per second, they are slow to store information, and users have to pay high fees in high-demand periods. Therefore, considering that applications can have different security and management requirements, researchers have proposed blockchain platforms with different characteristics and the use of alternative data structures rather than a chain of blocks. These platforms normally aim at creating a distributed digital ledger where information can only be appended but never modified or deleted. For this reason, in general terms, these are known as distributed ledger technologies or DLT.

The authors of [10] proposed a widely used DLT classification, which can be summarized as follows:

- Public: Platforms where data are public and users can interact with the DLT without requiring special permission.
- Private: Platforms where data are not public and users can only interact with the DLT if they have been granted permission.
- Permissionless: Platforms where any user can connect and participate in the administration of the DLT.
- Permissioned: Platforms where users have to be granted special permission to connect and execute management operations on the DLT.

DLT can be public or private and, in turn, permissionless or permissioned. For example, Bitcoin is a public and permissionless blockchain, since anyone can add a node to the Bitcoin network, can contribute validating transactions, and can generate new blocks. Additionally, anyone can become a Bitcoin user without being granted special permission. The only requisite is to own some bitcoins to pay for the transaction fees. At the other end, there are private and permissioned DLT, such as Hyperledger Fabric [11] that allows users to deploy a DLT in the nodes of their choice with strict policies regarding not only who can administer these nodes but also who can view and transact with the blockchain. In the middle, there are public and permissioned DLT, such as EOS [12]. In this type of platform, users can participate freely just as in Bitcoin. However, special permission are required to produce blocks and to manage the network. More exceptionally, there are also proposals for private and permissionless DLT, such as the LTO Network [13].

In general, DLTs are append-only systems that basically aim at being transparent, immutable, and secure. Furthermore, DLT put governance in multiple hands, not having to rely only on a single entity to correctly administer a system, contrary to conventional databases and computer systems. Depending on the specific use case, a type of DLT may be better suited than others. For example, a worldwide payment system, such as Bitcoin, requires a high level of decentralization to enable a censorship-resistant trustless model, where users do not need to trust anybody else in the system, but they can trust that their payments will be correctly processed. On the other hand, entities belonging to a supply chain may want to use a blockchain to facilitate the exchange of information between them, but they do not require a completely trustless system. In this case, the participants do not trust each other and, therefore, they do not want to rely on a single participant to run the information system of the supply chain. Hence, there is no need to open the system to the general public or to let other entities external to the supply chain join the network.

2.2. Smart Cities

Smart cities are characterized as highly heterogeneous systems that focus on several thematic dimensions, involve multiple stakeholders, and use a plethora of different technologies. From a thematic perspective, various studies classify smart city projects considering the following areas: smart economy, smart mobility, smart environment, smart people, smart living, and smart governance [14–16]. A city can cover several of these areas or put the focus only on areas that have the greatest impact on the lives of its citizens. According to [17], in the upcoming years, smart sustainability will be the principal focus for researchers in the smart city field. To reach this conclusion, the authors have performed a deep and systematic data analysis using language processing and time series mechanisms on the top 200 publications about smart cities indexed in Google Scholar.

Regarding the stakeholders participating in a smart city, it is possible to distinguish several direct participants, such as municipal administrators, service providers, citizens, and companies established in the city. However, other indirect participants should also be taken into account, such as companies from other urban areas that access the city to sell their products, citizens from other cities who visit it, the political opposition that requires transparent systems to scrutinize the political action of the rulers, etc. Furthermore, in the literature, there are many projects classified as belonging to the field of smart cities that involve different actors and create dynamics between citizens and private companies without involving the public administration, such as collaborative economy applications [18]. In this paper, we focus only on the use of DLT to create user-centric smart cities where the public administration is the main axis of the project. Thus, in this scenario, we reduce the actors to the public administration, service providers, and citizens (considering these as any actor that requires the services offered by the smart city or its providers).

From a technological perspective, smart cities tend to incorporate a very wide variety and heterogeneity of technologies. On the one hand, there is a widespread use of consolidated technologies, such as web portals to carry out bureaucratic procedures or the issuance of digital certificates for citizens. On the other hand, many projects use newer and more immature technologies, such as wireless sensor networks (WSN) and other IoT devices that are deployed in the streets to collect data and to interact with citizens. These use a plethora of different communication systems and specifications (e.g., ZigBee, 6LoWPAN, and LoRa). Therefore, many technological options lead to a context with many different protocols and security requirements. Moreover, some of the deployed devices have a low computational and storage capacity and are battery-powered, which creates additional difficulties to run conventional communication and security protocols. This high heterogeneity makes it difficult to define a specific architecture with a clear interaction between the different technological layers. Moreover, in the case of including DLT, the trust model and interaction between the different parties is generally approached in a silo perspective taking into account only the proposed system and not the smart city and the DLT ecosystem holistically. One of the most cited articles in the literature is [19]. The authors propose a simple framework with four layers: a physical layer (with sensors and actuators), a communications layer, a database layer (where permissioned and permissionless DLTs are included), and an interface layer. Although this is a first approach to the problem, in our paper, we propose a more detailed framework and analyze more in-depth the trust relationship with different DLT.

3. The Citizen at the Center of the System

In the literature, approaching problems from a user-centric perspective has been a topic of interest for years. Although DLTs are, currently, a hot topic in this field, there are many other ways to approach this problem, especially in the smart city scenario, which encompasses a plethora of different technologies. Among them, online social media are a valuable source of citizen data for many user-centric proposals. In [20], the researchers use geolocated messages on the microblogging site Twitter to predict crowd behavior and events taking place in a city. In [21], the authors propose a system that analyzes geolocated

messages on Twitter to know where important events are taking place and, in this way, to establish priorities in the data gathered by other means in the city. For instance, with this system, in the event of an accident, messages sent by WSN with information gathered by sensors near the location of the accident could take priority in cases of congestion in telecommunication networks.

Going one step further, the authors of [22] propose CityPulse, a framework that enables the integration of smart city data in a single system in a distributed manner. Beyond breaking silos and gathering data from multiple domains, as many other frameworks propose, CityPulse uses semantic discovery and data analysis techniques over large-scale data generated mainly by IoT and online social media to enable a dynamic view of the city. In this way, citizens can be aware of what happens in the city and how they can be affected. This type of framework is of utmost importance for user-centric smart cities. The analytic mechanisms that it enables are necessary and compatible with the conceptual framework that we describe in this paper. Our proposal is meant to ease the integration of DLT data to other systems and to assist system managers in becoming aware of trust issues that derive from decentralizing governance, besides distributing computation, storage, or information gathering, as CityPulse does.

On the other hand, it is important to highlight that technology is just one of the components to build user-centric systems. Technology can be the enabler, but it should never be the ultimate goal. DLT can help deploy new business cases and conceptual models. However, it is important to base new user-centric designs on a multidisciplinary approach considering economic, architectural, and many other factors. In [23], the authors aim at improving cities, focussing on historic public social housing neighborhoods, using a user-centered design-driven method. This work is a socio-technical and didactic experience in which researchers and students follow five phases to gather detailed local information about the neighborhood and to involve the community in the improvement process. These phases are a historical research and survey on the neighborhood, an on-site visit, a hands-on training, an architectural design project, and an on-site exposition. The last phase is crucial to ensure the participation of the community in the enhancement project. Hence, this type of work shows that it is of great importance to study the real needs of the citizens and, then, to select the most appropriate technologies to solve those needs. The blockchain space still has to prove that DLTs are economically effective and a good governance tool for many scenarios.

One of the main aims of this paper is to show decision-makers and other stakeholders that DLT open new possibilities to build user-centric smart city systems. However, this paper highlights that using these technologies entangles certain trust requirements that have to be carefully studied before adopting a DLT, since promoters may end up losing control of their systems by sharing the governance with other parties. Currently, there are many proposals to use DLT in areas related to urban management and smart cities. Nevertheless, as far as we know, there is no major city that has adopted these technologies as a core component of its systems. Smart cities have oriented their goals towards different directions, which make the projects very different and, therefore, when DLT adoption comes, the technical solutions implemented in some cases will not be suitable for others. On the other hand, learning from previous similar experiences and knowing other cities with common characteristics and goals is key to deploying successful systems and to avoiding mistakes. In [24], the authors identified archetypes of smart cities by examining the plans of 60 prominent projects, by extracting key categories, and by clustering the projects. This allows the authors to find common patterns between cities and to classify and divide the projects into three basic models: the Essential Services Model, the Smart Transportation Model, and the Business Ecosystem Model. This type of classification can be useful for citizens to better understand their cities and to be able to compare them with other municipalities. Furthermore, this can also serve to connect stakeholders from different urban areas and to be an aid for city planners and smart city administrators to formulate their plans and to seek advice in other similar projects.

4. Framework

In this section, we define a conceptual framework that abstracts a user-centric decentralized smart city architecture. This architecture is based on the DLT ecosystem to achieve decentralization and transparency and to allow data generators to gain control over their data. In this way, public administrations do not have to completely trust providers on the correct operation of some services and citizens do not have to trust providers or public administrators with their personal data. The proposed framework is shown in Figure 1. The following subsections discuss in more detail the main interactions between participants, the key technological components, and the DLT ecosystem.

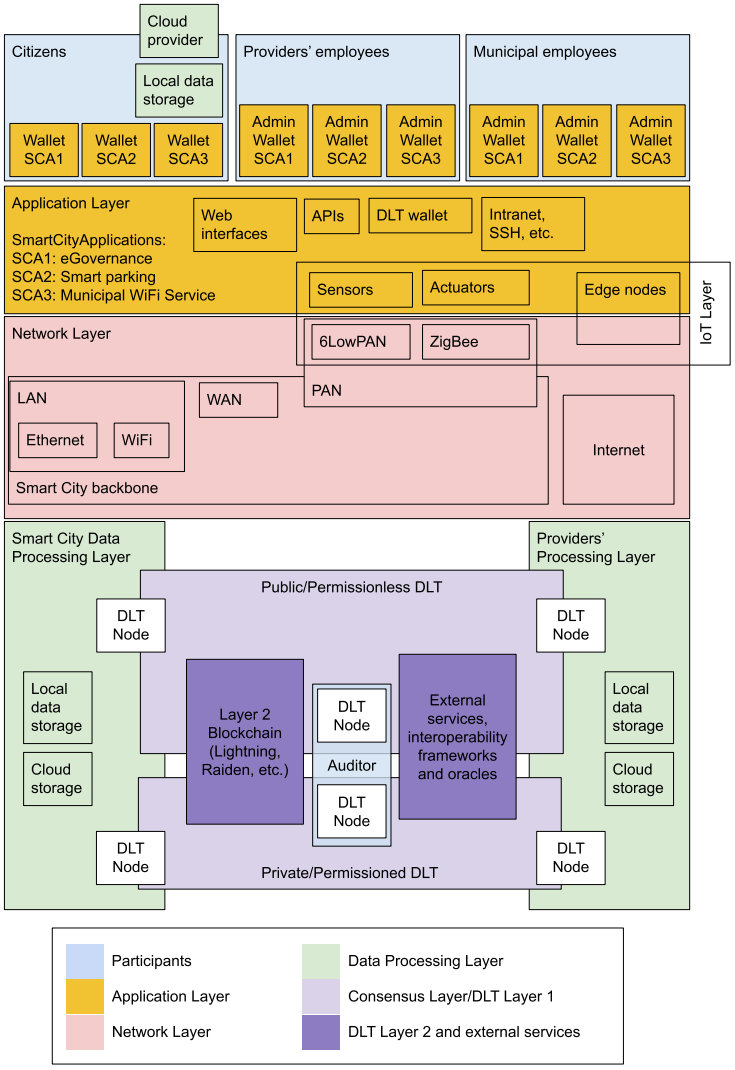

Figure 1. User-centric smart city framework based on DLT.

4.1. Participants

The main participants interacting with the proposed framework are represented in light blue in Figure 1. These participants are citizens, providers' employees, municipal employees, and auditors. The representation of institutions (e.g., the municipality) or IoT elements with digital identities has been ruled out because a principal goal of this framework is to increase transparency and accountability on people making decisions and actions in the smart city. In this way, any action affecting the state of the system is directly or indirectly linked to a person or a group of people represented among the aforementioned participants. If an action is triggered, for example, by an autonomous technological component or by a corporation, the initiator may not be a natural person, but

the digital identity representing the initiator of the action must have been granted rights by another digital identity. This can lead to a chain of permission where, at the top, there will always be a natural person from one of the main participant groups. One of the main aims of this framework is to register transactions for all interactions in a way that can be considered transparent.

For this proposal, we have considered a citizen as any actor that interacts with the smart city to provide any information (e.g., interacting with a sensor or an actuator in the street) or requests a service from the system or, in more general terms, someone that has some interest in the state of the smart city. Thus, this is not limited to city inhabitants and a citizen can also represent tourists, merchants, the driver or the owner of a vehicle circulating in the municipality, etc. These actors interact only with the application layer of the smart city deployed by municipal entities or by providers.

Providers' employees and municipal employees represent all of the actors that participate by making decisions, managing equipment, or providing a service. The interaction of these actors with the system can be performed at different levels depending on the responsibility of each employee. In this paper, we highlight the importance of authenticating users and of registering all actions to build a transparent and traceable smart city. For this reason, actions must be always made by the actors using a wallet-type application, as described in the next section.

Finally, auditors are any type of actor that has sufficient authority to validate the information registered in a certain smart city subsystem.

The proposed framework enables complex interaction examples. For instance, a delivery company can grant permission to drive a vehicle to one of its employees. If the driver exceeds the speed limit and is caught by a traffic camera, the municipal authority can automatically issue a traffic ticket to the driver, can verify that the company has the required permission to deliver goods in the area, and can issue a fine if not. On the other hand, the driver and the delivery company can verify that the traffic ticket and the fine were issued by registered municipal agents using a traffic camera complying with the regulation to be deployed in a specific location, installed by an official provider, following all the requirements and certifications.

4.2. Application Layer

The application layer includes the components with which the different actors interact with the system. Since the smart city is a highly complex and heterogeneous system, this layer can have different shapes depending on the specific use case. For example, smart cities use traditional interfaces such as websites, API end-points, or more innovative IoT elements.

Nevertheless, the basic idea behind the application layer of this framework is to interact in a similar way to cryptocurrency wallets. This approach is very different from conventional user experiences and interactions, where the application layer is generally in charge of transmitting user's orders to the backend systems and presenting the results. With a wallet approach, the application layer takes a more relevant role in the system, since it is not only responsible for transmiting the orders of the user to the backend but also for storing cryptographic keys and performing cryptographic operations. Furthermore, wallets are a key component to enable decentralized and user-centric applications because they articulate the coordination between the different components that are required from and by the users. For instance, a user wallet can be responsible for coordinating with a storage system or storing locally the personal data of the user. Wallets are also responsible for downloading the necessary data from the blockchain to verify that transactions are properly processed. With this scheme, wallet applications not only execute the procedures required by the actors but also create, sign, and record in a DLT a transaction associated with each action, creating a traceable system that helps to resolve conflicts between different parties. For example, traditionally, registering a new user in a provider's database could be performed by an employee interacting directly with the database management system

(DBMS). Nonetheless, besides the changes in the database, by doing this, the DBMS would probably append some local logs with the performed operations, with these logs being controlled by the service provider and not being a reliable source of information to resolve any dispute with a third party regarding the modification of the database.

4.3. Network Layer

This layer contains the telecommunication networks that provide connectivity to the actors, to the devices, and between the different components of the framework. Smart cities tend to install a plethora of different networks, such as conventional wide area networks (WAN) and local area networks (LAN), and other types of networks to deploy services and IoT elements on the streets. Some of these are low-power wide-area networks (LPWAN) (e.g., SigFox, LoRaWAN), wireless metropolitan area networks (WMAN) (e.g., WiMAX), and wireless personal area networks (e.g., ZigBee, 6LoWPAN). Although the network infrastructure is one of the most important components of the smart city, in this paper, we focus on the role of the DLT, and the network layer is only considered as a necessary enabler.

Commonly, smart cities are designed with a high-speed broadband network as a backbone. This provides interconnectivity among the subnetworks of the city and, for many applications, it acts as a gateway to the Internet. Regarding DLT, this infrastructure allows administrators to not only deploy full nodes to join public and permissionless blockchains such as Ethereum but also to configure private and permissioned blockchains, where block generators, validator nodes, and other participants have restricted access to the Internet and, therefore, all information can be exchanged in a highly controlled environment.

4.4. Data Processing Layer

Smart cities deploy a wide range of technological projects that require many different data processing mechanisms, from simple local or cloud storage services to more complex machine learning frameworks. Currently, many blockchain projects already require some of these mechanisms to offer their services. In the beginning, cryptocurrencies such as Bitcoin used blockchain as the sole platform to store all of their information about the payment system and, therefore, all trust issues were related to a single system. Nevertheless, modern projects use cryptocurrencies only as a reward mechanism to enable distributed services or use the blockchain only as a distributed state machine, using information from external sources and storing data off-chain. Outstanding projects of this kind are Storj [25], which creates a decentralized cloud storage service, and Golem [26], which creates a decentralized cloud computing service. This type of service is a paradigm of what can be achieved by combining DLT and open APIs of other centralized or distributed systems. The same type of approach can be used by smart cities to build their own private and permissioned systems or to use their data processing capabilities in public and permissionless platforms. The next section provides more details on the interaction between DLT and external services.

4.5. DLT Layer

In recent years, the DLT ecosystem has become highly complex. For the purpose of this framework, we can divide the DLT elements in two basic components. On the one hand, the core components can be labeled as layer 1. These include the consensus mechanism, the data structure (generally, a blockchain), and the P2P network. Basically, this is what is commonly known as a blockchain or a DLT.

On the other hand, many applications based on blockchain technology do not interact directly with layer 1 protocols. Instead they use layer 2 solutions, such as token transfer platforms (e.g., Raiden Network [27]), or require interoperability mechanisms to interact with several systems (e.g., Polkadot [28]), oracles to obtain information outside of the blockchain (e.g., ChainLink [29]) and to identity platforms (e.g., ION [30]). Layer 2 protocols are scalability solutions built on top of layer 1, which create protocols that avoid having to publicly share and write in the ledger every single transaction. These solutions mainly

store transactions offline and use a blockchain to resolve possible conflicts. These solutions can enjoy similar levels of security to the underlying blockchain systems, exponentially increasing the number of transactions per second that can be processed. The most relevant layer 2 solutions can be divided into payment and state channels, commit-chains, and protocols for refereed delegation [31].

As mentioned above, all participants must interact with the system through software similar to cryptocurrency wallets. A wallet is an application that goes far beyond the creation of key pairs and the execution of digital signatures. Wallets also interact with blockchain nodes, collect relevant transactions and block headers, calculate appropriate fees, etc. In this scenario, the applications that users interact with are required to work similarly. In this way, the wallets are a key component in transfering the responsibility of storing data to the users. Then, the DLT layer is the core component used to securely orchestrate the other protocols and to be able to share the data in a way where all parties can ensure that it is authentic and up-to-date. Furthermore, this also allows establishing a non-repudiable system with which every performed action is automatically linked to a verifiable transaction. For example, a citizen using a municipal WiFi service provided by a third party supplier would have to use his or her wallet to authenticate, obtain a security token to navigate on the Internet, establish the connection, and pay for the service, if applicable. In this way, all actions related to the service could be registered in a DLT, including the service level agreement between the citizen and the provider, the payment, metrics on the quality of the offered service, etc. Most of these data would not be recorded in the DLT for privacy and scalability reasons. However, a hash of the data can be recorded in the DLT and the original data can be signed and stored separately by the two parties. Then, DLT information serves as the official verifiable record in case of a dispute. The fact that the used DLT is public, private, permissioned, or permissionless does not affect the outcome of a dispute in this situation. The main mechanism to solve this is digital signatures; the DLT is just a component to facilitate the process and to achieve a system where all participants agree on their state at any given moment in time.

In this framework, it is important to clarify the role of the auditors and the DLT. As mentioned above, auditors are any type of actor that has sufficient authority to validate the information registered in a smart city subsystem. Therefore, citizens can act as auditors in certain cases, for example, in any service deployed on a public blockchain where there is no confidential information. However, special permission might be required to audit other services managing confidential information or that use permissioned DLT. Such a system cannot be then considered completely trustless, since citizens must delegate trust in a third-party auditor. However, these types of systems greatly improve most of the current systems where records are kept only in one-party databases and complex technical and bureaucratic procedures are required to audit third-party data.

5. DLT and Smart Cities

Recent surveys on blockchain in smart cities, such as [32–35], show that most of the projects to use DLT in an urban context are still research proposals that are not being used as a core component of any real smart city system. The survey in [32] analyses 24 publications, evaluating the proposals according to several performance criteria, such as scalability, usability, cost, latency, etc., and technological criteria, such as if the proposal is based on cryptocurrencies, if it is a smart contract platform, if it is a consensus protocol, if it is modular, etc. According to their analysis, the authors state that DLT has the potential to increase security and performance as well as to reduce smart city costs. Additionally, the authors present a decentralized identity architecture for smart cities based on Hyperledger Indy.

In [33], the authors focus on studying the potential benefits and the challenges of blockchain technology in smart cities by performing a SWOT analysis. Regarding the potential benefits, the survey summarizes the well-known properties of blockchain technology (i.e., reliability, availability, immutability, irrevocability, near real-time execution, cost efficiency, and transparency). Regarding the challenges, beyond listing some other

well-known issues (e.g., security and privacy), the survey highlights that non-interoperable implementations can result in fragmentation; it is not clear how this systems will be governed; and the economic impact of DLT in this context is still unknonwn. This uncertainty reflects that DLT have still not been studied enough in the context of smart cities. Furthermore, the survey also lists examples of blockchain projects in smart cities, indicating the status of the project in 2019. The list in [33] shows relevant but fragmented initiatives from very different fields. Among them are digital identity projects (Estonia), e-health (USA), e-government (Dubai), land registry (Ghana, Georgia), and cross-border interbank payments (Singapore).

One of the most recent surveys (published in 2020) about blockchain technology and smart cities can be found in [34]. The authors of that paper conducted a systematic literature review to analyze in which fields blockchain can foster the development of smart cities and the research propositions that arise from its application in this context. The authors clustered the analyzed projects in nine different fields (i.e., healthcare, logistics and supply chains, mobility, energy, administration and services, e-voting, factory, home, and education). Although the survey presents a conceptual framework to divide the applications in areas, there are no details regarding specific blockchain platforms or the way these systems can be governed.

In [35], the authors reviewed DLT projects focused on smart citizens, smart healthcare, smart grid, smart transportation, supply chain management, and others. The survey highlights that most of the projects are still not ripe, with some only being a concept far from a real implementation, and have weaknesses. Some of the pointed weaknesses are well-known challenges in the blockchain space, such as security, privacy, throughput, storage, energy efficiency, incentives, costs, and regulation. Additionally, the paper also identifies Chile, Toronto, Stockholm, Visakhapatnam, and Dubai as promoters of blockchain-based smart city projects. Nonetheless, the paper does not provide many details on these projects, which seem to be more announcements than actual developments at the time of writing [35]. Currently, from these, Dubai seems to be one of the most advanced developments. In 2016, Dubai launched a citywide blockchain strategy to become, what they call, the first Blockchain-powered city by 2020 [36]. The strategy behind is based on three pillars: Government efficiency, industry creation, and local and international thought leadership. The project is fostering many different use cases; however, most of them are still in an early stage. In general, the initiatives focus on improving bureaucratic efficiency and creating paperless workflows. Mainly, this project aims to deploy a private DLT and it is not focused on how to integrate other blockchain initiatives in the smart city operative. In [37], the authors briefly described a pilot project developed with a blockchain as a service. Although Dubai's smart city seems to be one of the most advanced projects of this kind, it has been difficult to find detailed information about the specifics of the project and how DLTs are being used. The lack of detailed information, beyond marketing websites and brochures, is a common flaw that we noticed in many reviewed blockchain-based smart city projects announced by public institutions. This is in contrast to what happens with typical blockchain projects in the private space, where a white paper is generally published at the beginning of the project including a preliminary design of the proposed solution, and developed code tends to be open source and regularly committed to a public repository.

On the other hand, the research in [38] describes more concrete architectures that use blockchain technology in smart cities. Nevertheless, this survey only focuses on specific use cases in the field of IoT and 6G, such as the smart grid, intelligent transportation systems, and smart healthcare. In the paper, the authors proposed to use a public blockchain such as Ethereum to create P2P decentralized applications (e.g., energy trading marketplace), and off-chain solutions such as IPFS to store the necessary data linked to each blockchain transaction (e.g., smart meter recordings). Each use case is studied considering the main characteristics of blockchain technology (i.e., decentralization, trust, transparency, and immutability). The paper also highlights several challenges in each case. Among others, the authors mention infrastructure costs, throughput, and scalability issues of current

blockchain platforms; legal difficulties to create P2P energy marketplaces with current regulatory frameworks; the need for artificial intelligence and prediction platforms able to handle big data; the lack of interoperability and standardization of blockchain technologies; and the lack of trained personnel.

Hence, from a general point of view, as these surveys show, smart city projects using blockchain technology are still young and fragmented. As far as we know, there are no real use cases of smart cities where DLTs are the core component of the system and where integration with the public and permissionless ecosystem has seriously been discussed. Below, we select paradigmatic use cases in the smart city and prominent blockchain initiatives from other contexts that have the potential to be implemented in a smart city. We analyze these cases, paying special attention to the trust issues that emerge from using the different DLT types. We expect that this aids smart city managers and decision-makers in understanding the role and the trust compromises that these technologies entail.

5.1. DLT Use Cases

The smart city concept is very broad, and different types of cities have different needs that lead to completely different projects, all under the umbrella of the smart city. Here, we gather some use cases where DLT systems can be key to better public management of the municipality. Therefore, in all of the selected cases, public administration plays a relevant role in the system. Projects that can be considered from the smart city field but where the only parties interacting are citizens (such as collaborative economy platforms) or are private institutions and citizens have been discarded. The cases have been divided into the following categories: payment and token transfer systems, digital identity, authentication and authorization, traceability and immutability, and bureaucratic efficiency.

5.1.1. Payment and Token Transfer Systems

Payment and token transfer systems are the main use cases for DLT, especially public DLT. Today, there are more than 8000 cryptocurrencies and tokens indexed on the most popular websites [39]. This type of payment system must offer its participants a system where the rules on the operation of the system are transparent. Thus, both the rules of the monetary policy of the token in question (e.g., maximum supply) and the rules on how to make the transfers are defined in advance and cannot be easily altered.

In a smart city, these token transfer systems can be used in many of the services currently offered in urban areas, for example, for the payment of public transport. Beyond the advantages of digitizing a system that in many cases still works with paper tickets, the creation of tokens to represent transport tickets would greatly increase the transparency of a city's transport network. In this case, the use rate of each transport company and their routes would be publicly auditable. This would not only prevent common frauds such as registering more travelers than the actual load to obtain subsidies but also provide a fully traceable and auditable solution for analysis of the behavior of the travelers and optimization of the network of public transport. Moreover, smart contracts in advanced blockchains open the possibility to create travel tokens with ad hoc functionalities. For instance, offering different tariffs according to the occupation of the vehicles or the schedule; in journeys involving multiple companies, each could be rewarded depending on the kilometers taken by each traveler, their reputation, etc.

For this use case, public DLTs are the best alternative to solve trust issues between all of the parties. Continuing with the example of public transport, with a public DLT, citizens and all providers can verify that money spent on traveling tickets goes to providers that really offer the agreed upon service. From the side of the public administration, this offers a transparent registry that can eliminate any mistrust when paying subsidies to providers. Moreover, this offers a highly traceable and detailed information system to improve the transportation network. Furthermore, with privacy systems, such as ring signatures [40] used in the Monero cryptocurrency or the zero-knowledge proofs [41] used in Zcash, token exchange systems that are traceable, trustless, and respect citizens' privacy are possible.

Some researchers are already working on incorporating DLT systems to improve the transportation network. For example, the authors of [42] discussed the most important factors in the joint use of blockchain and artificial intelligence to contribute to a sustainable smart society. The paper also lists the security issues and the negative impact that this can have. In [43], the authors formulated calculations of a tradable mobility permit (TMP). The authors argued that the TMP can be used to alleviate traffic congestion in cities and discussed the potential of blockchain in transportation and other contexts. The transport system is just one example in a smart city environment since the exchange of tokens in this way could be implemented for many other municipal use cases.

Taking all of this into account, a token transfer system for a smart city requires high decentralization, since the system itself could be used to audit the city manager. Therefore, the use of private and permissioned DLT administered only by public administration and its providers cannot guarantee the necessary integrity and transparency. However, token transfer systems require high scalability in terms of speed in recording transactions, the number of transactions per second, and the number of concurrent users. The security and integrity of the system are also prominent requirements in this case. These requirements are the same as those of most cryptocurrencies based on public and permissionless blockchains. Therefore, taking into account the current scalability problems of this type of blockchains, many solutions go through the use of second-layer systems, such as the Raiden Network [27] for Ethereum.

5.1.2. Digital Identity

Self-sovereign identity (SSI) systems are a hot topic in the blockchain world. These systems have the goal of enabling citizens to create and manage their personal data autonomously, requiring only the intervention of third parties for the issuance and validation of claims and credentials. A user could, for example, request the issuance of a credential that represents an academic title, a driver's license, or other minor achievements such as attending a course. Digital signatures and following common protocols are tools that enable this type of mechanism. In this sense, the most popular specifications are decentralized identifiers [44], to create identifiers for the decentralized identities, and verifiable credentials [44], for the claims and credentials data model, both proposed by the W3C. To use these, DLTs are indeed not necessary. Nonetheless, DLT can play a crucial role as a decentralized timestamped global state registry. In this way, credentials can easily be verified, shared, revocated, updated, and appended by multiple parties. Currently, there are several solutions that aim at breaking the silos created by proprietary identity providers. Sovrin [45] is a popular SSI platform based on Hyperledger Indy [46], a public and permissioned DLT. Another popular system is uPort [47] based on the public permissionless blockchain Ethereum. Generally, interoperability is still a challenge between SSI systems.

In the smart city context, SSI can allow public administrations and providers to act as issuers and validators of credentials. These participants can also deploy DLT nodes on an SSI system to verify the correctness of the system and to provide connection points to other clients. It is not required that they deploy their own identity system or resource-demanding nodes to maintain the infrastructure. For example, they could deploy observer nodes in Sovrin. This eases data management for administrators and transfers the responsibility of correctly storing personal data to the owner of the data, avoiding large repositories with personal information that lure cyber-attackers. Of course, this is currently cumbersome for many users and remains an open problem in the blockchain space, where many users have lost (or were stolen from) thousands of dollars in cryptocurrency due to losing access to their private keys [48]. A possible solution to avoid this is that public administrations or providers offer easy-to-use centralized storage systems connected to a public SSI. Another solution would be to deploy private permissioned DLTs interoperable with the main SSI specifications. In the first case, the administrators would be able to offer an open and decentralized alternative as a choice, but they would still have to face security issues to store all of the personal data of the users. In the second case, besides these security

problems, the system would not offer greater transparency or integrity than a typical siloed proprietary identity system. On the other hand, scalability issues and high transaction fees can become a real problem for users in this use case, and therefore, currently, Ethereum and other public permissionless DLTs are not ready to effectively enable ISS. Therefore, public permissioned systems, such as Sovrin, can be a good solution to not have to rely on a system deployed and administered only by public administrators or city providers.

5.1.3. Access Control

One of the most relevant characteristics of smart cities is the high heterogeneity of devices and the large number of participants who interact with each other and with the devices. Additionally, many of the devices belong to the IoT, having low computational and transmission capacity and, sometimes, being battery-powered. This makes it difficult to deploy strong cryptography and protection mechanisms. Moreover, many of these devices are deployed on the streets, which makes them easily tamperable.

In the literature, there are some proposals to enable access control mechanisms for the IoT based on blockchain [49], even using the Bitcoin blockchain [50]. Although some of these publications demonstrate that building this type of mechanism is possible, we could not find any empirical evidence even in simulated scenarios that using these is feasible in a highly complex scenario such as in a smart city.

Indeed, a global platform for authentication and authorization (AA) would solve many mismanagement issues involving the many actors dealing with the urban technological components. A complex situation for conventional AA systems that is typical from the smart city can involve a public employee authorizing the installation of a component to a provider but giving the maintenance contract to another provider. At the same time, the providers grant access rights to the component to some of their employees. Moreover, the technological component, such as a sensor, may have to connect to an access point of a third provider.

This type of use case requires high scalability and fast transaction time. On the other hand, although a smart city may have many different providers and these may have many employees, the number of total participants cannot be considered high in computational terms. Likewise, this context does not demand a totally open system, since possible conflicting interests only involve providers and the public administration. In this case, citizens do not require exhaustive control of these matters. Citizens may require assurance that providers comply with service level agreements. However, this is not a matter that requires real-time full transparency. For this reason, permissioned and private DLT can satisfy technical and trust requirements. On the other hand, creating blockchain transactions requires performing cryptographic operations that may not be possible for IoT nodes or, at least, not recommendable for battery-powered devices [51], not to mention consensus operations of public blockchains that are demanding in terms of computational intensity and bandwidth.

5.1.4. Auditable and Immutable Registry

One of the typical use cases for DLT systems is to establish an auditable and immutable record. This type of record does not usually require saving all of the information in the DLT but only an integrity proof, such as the result of computing a hash function to the data that must be kept intact. Combining this with data structures such as Merkle trees makes it possible to efficiently save multiple integrity proofs together in a single transaction. In this way, it is feasible to use public blockchains such as Bitcoin and Ethereum for this purpose. In general, public blockchains have high fees and are slow, so they are not designed to store a large amount of information. However, in systems that generate a high volume of information, this type of blockchain can be used to register snapshots that can confirm in the future the integrity of the system on a given date.

In the smart city, most of the systems record day-to-day information that has to be auditable in the long term. However, these systems are not required to solve a double-

spend problem in a decentralized way and, therefore, using a blockchain platform for this purpose can be considered inefficient, for example, the systems of providers that centrally manage a service or systems registering contracts between the public administrations and the private contractors. Hence, scalability, integrity and high transparency are of utmost importance in these systems. Nonetheless, it is not necessary to reach a consensus for each transaction that is recorded. Therefore, a mechanism, where providers or public entities share their data off-chain with auditors or with the public and register integrity proofs in a public DLT, solves the integrity and transparency requirements for these cases.

5.1.5. Bureaucratic Efficiency

In the smart city, public administrations and providers manage large volumes of information that they share many times with multiple parties. As time goes by, the information loses quality and ends up being duplicated and outdated in different servers. This leads to inefficiencies and possible conflicts. Therefore, a platform to share a single state of the system between multiple parties would solve this problem. In this case, this platform is not required to be auditable by the public; it simply has to solve the inefficiencies between the involved parties. This problem is similar to the one in the supply chain, where there are inventory, financial, process, and other information flows between multiple stakeholders that cannot be connected properly using conventional databases and enterprise resource planning (ERP) systems. Therefore, in this context, as in that of the smart city, there is a clear need for a platform shared between a reduced number of stakeholders that records a single common state of the system and facilitates information exchange in an authenticable way through digital signatures. Private and permissioned DLTs are enough to solve the needs in this case, where information do not need to be open to the public and trust issues need to be resolved only among the parties involved in the system. Currently, systems of this kind using DLTs are in an advanced stage in the logistics and supply chain context. A prominent example is TradeLens [52], which uses IBM Cloud and IBM Blockchain, a permissioned DLT, to provide an information system for global trade and shipping. TradeLens aims to connect customs, authorities, ports, shipping companies, and many more entities with a single shared system to reduce bureaucracy, to facilitate dispute resolutions, and to make information exchange more efficient in general.

6. Discussion

This article studies the use of DLT to create user-centric smart city architectures. Taking into account the use cases described in the previous section, this section complements the discussion on how DLT properties contribute to this type of architecture and the trust issues that this entails.

Smart cities are highly heterogeneous and agglutinate several subsystems with different trust models. This requires ad hoc trust analysis for each subsystem, which can lead to the use of various types of DLT in a single smart city to tackle the needs of the different projects. On the one hand, some projects use private and permissioned DLTs to deploy a system as a state machine that facilitates sharing data to avoid deduplicated information and to improve information exchange. The main benefits of DLT here are the creation of a timestamped global state machine, with a built-in authorization, authentication, and auditing mechanism. In these cases, most of the transactions involve only two parties (or few parties in the worst case) and could have been resolved by other means before the blockchain was invented in 2009 by using digital signatures, public key infrastructures (PKI), and the choice for common protocols and data formats. In these cases, the trust model behind the system does not require a common consensus, since disputes could generally be solved by comparing the documents signed by involved parties. However, having a consensus system and a state machine facilitates not having outdated systems by avoiding the disputes beforehand and by integrating different information flows (e.g., inventory, financial, and process) in a single system. In the case requiring the expansion of transparency or integrity beyond the trust of the entities directly involved in the system,

for example, to be auditable by third parties or by citizens, participants can record integrity proofs in a public blockchain to ensure auditors that there are no collusions between the DLT managers to modify the state of the system once it has been recorded.

On the other hand, in many other projects, the trust model involves the general public or, at least, entities beyond the sole participants in each transaction. Therefore, regular snapshots are not enough. For instance, in cases where transactions are related to digital assets represented by fungible or non-fungible tokens that can be transferred and interchanged without the intervention of a central authority. In these cases, any participant has to be able to validate any transaction before accepting a token. Thus, it is required that the system offers finality and that possible double-spends are resolved with a strong consensus system, where the managing entities cannot collude to modify the state of the system to their benefit. Hence, private permissioned systems should be discarded in these cases. Public permissioned systems (e.g., EOS) would fulfill these trust requirements. However, other trust issues emerge regarding the global mismanagement of this type of blockchains generally controlled by only a few dozens of nodes.

Selecting an appropriate DLT is not an easy task, and system architects should bear in mind the blockchain scalability trilemma [53]. This describes the tradeoffs between decentralization, scalability, and security. In other words, the more relevant two of these properties are in a distributed system, the less important the third one. Therefore, deciding to use or not a DLT, and if so, deciding its type, is a matter that has to be thoroughly analyzed considering the needs of each scenario. Although public, permissionless blockchains seem ideal in terms of decentralization and finality, they entail two fundamental problems: they are slow and their fees are volatile and expensive during some periods. Private permissioned systems are scalable, and privacy requirements are easily achievable. However, in terms of decentralization and finality, these DLT provide only a bit more than conventional databases and they may reflect a distorted picture regarding the integrity and transparency of the system. Furthermore, in all cases, participants may have unexpected governance problems that require consensus among a great majority to change the system and, even, to solve known software bugs, as was the case in 2017, when Bitcoin was divided into two different projects (Bitcoin and Bitcoin Cash) due to disagreements on how to solve scalability and the transaction malleability problem. DLTs are still immature compared to conventional databases, digital signatures, PKI, and other technologies that can be alternatives to achieve data integrity, transparency, and authenticity. Other authors critically analyzed the cases where blockchains are used and listed possible alternatives [54,55].

7. Conclusions

In this paper, we focus on how DLT can be a key technology to enable user-centric smart cities. According to the literature, DLT can be classified as permissioned or permissionless and as public or private platforms. Different trust models are derived depending on the specific type. From completely trustless models enabled by public and permissionless blockchains to platforms where governance and administration depend on one or very few parties and, therefore, for an external user, the trust model is comparable to the one of a centralized system.

The smart city is a scenario that has multiple different use cases with very heterogeneous requirements. This makes it difficult to define a single blockchain-based smart city model. For this reason, in this paper, we defined a conceptual technological framework that contains an abstraction including the interactions among the main components of the smart city, its participants, and the DLT ecosystem. In the proposed framework, the actors interacting with the systems use wallet-type applications, which allows them to control their data. Moreover, for each interaction with the system, the wallets can also send transactions to record the actions performed by the users in a DLT, an immutable, traceable, and distributed state machine. In this way, the responsibility for storing and managing personal data can be transferred to its owner and, at the same time, the DLT can be used to verify that it is authentic and up to date.

Although blockchain is a hot research topic, the real deployment of this technology in smart cities is still immature and most of the use cases are fragmented. Nowadays, few smart city projects rely on DLT as a core component of their system. Moreover, current proposals tend to deploy their private network as a single DLT solution for a smart city. Nevertheless, the blockchain space is moving towards interoperability solutions to integrate use cases implemented in different DLT. Furthermore, as we have seen in this paper, smart city administrators and decision-makers must take into account that different use cases that require different trust models and, therefore, that all cannot be achieved only using one DLT type. Hence, it is of utmost importance to consider how to deal with DLT from a holistic perspective, studying, on the one hand, the trust implications concerning the citizens and the interaction with the providers and, on the other hand, the technological features of each DLT type. Furthermore, it should be borne in mind that decentralization projects in smart cities can leverage DLT but that a simple technological substitution should not be the goal of the project. DLT can contribute by removing some technological silos, by empowering users, by helping them to recover control over their personal data, by enabling mechanisms to effectively audit providers and the public administration, etc. However, much more beyond deploying a DLT is required to make a smart city decentralized, secured, paperless, auditable, or transparent.

Funding: This work was partially supported by the Spanish Government under grant RTI2018-095094-B-C22 "CONSENT".

Conflicts of Interest: The author declares no conflict of interest.

References

1. Naphade, M.; Banavar, G.; Harrison, C.; Paraszczak, J.; Morris, R. Smarter cities and their innovation challenges. *Computer* **2011**, *44*, 32–39. [CrossRef]
2. Ajuntament de Barcelona. Barcelona Digital City. Available online: https://ajuntament.barcelona.cat/digital/en/digital-transformation/city-data-commons/cityos (accessed on 25 February 2021).
3. CityOS. Available online: https://cityos.io/ (accessed on 25 February 2021).
4. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 18 November 2019).
5. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
6. MacDonald-Korth, D.; Lehdonvirta, V.; Meyer, E.T. *The Art Market 2.0: Blockchain and Financialisation in Visual Arts*; The Alan Turing Institute: London, UK, 2018.
7. Karamitsos, I.; Papadaki, M.; Al Barghuthi, N.B. Design of the blockchain smart contract: A use case for real estate. *J. Inf. Secur.* **2018**, *9*, 85741. [CrossRef]
8. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
9. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. 2014. Available online: https://github.com/ethereum/yellowpaper (accessed on 13 November 2020).
10. Carson, B.; Romanelli, G.; Walsh, P.; Zhumaev, A. Blockchain beyond the Hype: What Is the Strategic Business Value. 2018. Available online: https://cybersolace.co.uk/CySol/wp-content/uploads/2018/06/McKinsey-paper-about-Blockchain-Myths.pdf (accessed on 13 November 2020).
11. 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, 23–26 April 2018; pp. 1–15.
12. EOS. Available online: https://eos.io/ (accessed on 25 February 2021).
13. LTO Network. Available online: https://www.ltonetwork.com/ (accessed on 25 February 2021).
14. Appio, F.P.; Lima, M.; Paroutis, S. Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technol. Forecast. Soc. Chang.* **2019**, *142*, 1–14. [CrossRef]
15. Wein, T.U. European Smart Cities 4.0. 2015. Available online: http://www.smart-cities.eu/?cid=2&ver=4 (accessed on 23 February 2021).
16. Cantuarias-Villessuzanne, C.; Weigel, R.; Blain, J. Clustering of European Smart Cities to Understand the Cities' Sustainability Strategies. *Sustainability* **2021**, *13*, 513. [CrossRef]
17. Stübinger, J.; Schneider, L. Understanding Smart City—A Data-Driven Literature Review. *Sustainability* **2020**, *12*, 8460. [CrossRef]

18. Ertz, M.; Boily, É. The rise of the digital economy: Thoughts on blockchain technology and cryptocurrencies for the collaborative economy. *Int. J. Innov. Stud.* **2019**, *3*, 84–93. [CrossRef]
19. Biswas, K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications, IEEE 14th International Conference on Smart City, IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December 2016; pp. 1392–1393.
20. Lee, R.; Sumiya, K. Measuring geographical regularities of crowd behaviors for Twitter-based geo-social event detection. In Proceedings of the 2nd ACM SIGSPATIAL International Workshop on Location Based Social Networks, San Jose, CA, USA, 2 November 2010; pp. 1–10.
21. Costa, D.G.; Duran-Faundez, C.; Andrade, D.C.; Rocha-Junior, J.B.; Just Peixoto, J.P. Twittersensing: An event-based approach for wireless sensor networks optimization exploiting social media in smart city applications. *Sensors* **2018**, *18*, 1080. [CrossRef] [PubMed]
22. Puiu, D.; Barnaghi, P.; Tönjes, R.; Kümper, D.; Ali, M.I.; Mileo, A.; Parreira, J.X.; Fischer, M.; Kolozali, S.; Farajidavar, N.; et al. Citypulse: Large scale data analytics framework for smart cities. *IEEE Access* **2016**, *4*, 1086–1108. [CrossRef]
23. Lucchi, E.; Delera, A.C. Enhancing the Historic Public Social Housing through a User-Centered Design-Driven Approach. *Buildings* **2020**, *10*, 159. [CrossRef]
24. Tang, Z.; Jayakar, K.; Feng, X.; Zhang, H.; Peng, R.X. Identifying smart city archetypes from the bottom up: A content analysis of municipal plans. *Telecommun. Policy* **2019**, *43*, 101834. [CrossRef]
25. Storj. Available online: https://www.storj.io/ (accessed on 3 May 2021).
26. Golem. Available online: https://www.golem.network/ (accessed on 3 May 2021).
27. Raiden Network. Available online: https://raiden.network/ (accessed on 25 February 2021).
28. Polkadot. Available online: https://polkadot.network/ (accessed on 25 February 2021).
29. ChainLink. Available online: https://chain.link/ (accessed on 25 February 2021).
30. ION. Available online: https://github.com/decentralized-identity/ion (accessed on 25 February 2021).
31. Gudgeon, L.; Moreno-Sanchez, P.; Roos, S.; McCorry, P.; Gervais, A. SoK: Layer-two blockchain protocols. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, 10–14 February 2020; pp. 201–226.
32. Ghandour, A.G.; Elhoseny, M.; Hassanien, A.E. Blockchains for smart cities: A survey. In *Security in Smart Cities: Models, Applications, and Challenges*; Springer: Cham, Switzerland, 2019; pp. 193–210.
33. Salha, R.A.; El-Hallaq, M.A.; Alastal, A.I. Blockchain in smart cities: Exploring possibilities in terms of opportunities and challenges. *J. Data Anal. Inf. Process.* **2019**, *7*, 118–139. [CrossRef]
34. Treiblmaier, H.; Rejeb, A.; Strebinger, A. Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda. *Smart Cities* **2020**, *3*, 853–872. [CrossRef]
35. 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. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
36. Bishr, A.B. Dubai: A city powered by blockchain. *Innov. Technol. Gov. Glob.* **2019**, *12*, 4–8. [CrossRef]
37. Consensys. Blockchain Powering the City of the Future. Available online: https://consensys.net/blockchain-use-cases/government-and-the-public-sector/smart-dubai/ (accessed on 3 May 2021).
38. Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* **2021**, **172**, 102–118.
39. CoinMarketCap. Today's Cryptocurrency Prices by Market Cap. 2021. Available online: https://coinmarketcap.com/ (accessed on 25 February 2021).
40. Noether, S.; Mackenzie, A.; The Monero Research Lab. Ring confidential transactions. *Ledger* **2016**, *1*, 1–18. [CrossRef]
41. Sasson, E.B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 459–474.
42. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
43. Bagloee, S.A.; Tavana, M.; Withers, G.; Patriksson, M.; Asadi, M. Tradable mobility permit with Bitcoin and Ethereum–A Blockchain application in transportation. *Internet Things* **2019**, *8*, 100103. [CrossRef]
44. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model. 2019. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 11 March 2021).
45. Sovrin. Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. 2018. Available online: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf (accessed on 11 March 2021).
46. Hyperledger. Hyperleger Indi. 2017. Available online: https://www.hyperledger.org/blog/2017/05/02/hyperledger-welcomes-project-indy (accessed on 25 February 2021).
47. Lundkvist, C.; Heck, R.; Torstensson, J.; Mitton, Z.; Sena, M. Uport: A Platform for Self-Sovereign Identity. 2017. Available online: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf (accessed on 18 November 2019).

48. New York Times. Tens of Billions worth of Bitcoin Have Been Locked by People Who Forgot Their Key. 2021. Available online: https://www.nytimes.com/2021/01/13/business/tens-of-billions-worth-of-bitcoin-have-been-locked-by-people-who-forgot-their-key.html (accessed on 11 March 2019).
49. Pinno, O.J.A.; Gregio, A.R.A.; De Bona, L.C. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
50. Maesa, D.D.F.; Mori, P.; Ricci, L. Blockchain based access control. In Proceedings of the IFIP International Conference on Distributed Applications and Interoperable Systems, Neuchatel, Switzerland, 19–22 June 2017; pp. 206–220.
51. Elsts, A.; Mitskas, E.; Oikonomou, G. Distributed ledger technology and the internet of things: A feasibility study. In Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems, Shenzhen, China, 4 November 2018; pp. 7–12.
52. TradeLens. Available online: https://www.tradelens.com (accessed on 11 March 2021).
53. Buterin, V. On Sharding Blockchains. 2018. Available online: https://github.com/ethereum/wiki/wiki/Sharding-FAQ (accessed on 11 February 2021).
54. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.
55. Koens, T.; Poll, E. What blockchain alternative do you need? In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Springer: Cham, Switzerland, 2018; pp. 113–129.