land

MDPI

Article

Data-Driven Intelligent Platforms—Design of Self-Sovereign Data Trust Systems

Ana Balan [1,2], Andi Gabriel Tan [3], Karima Kourtit [4,5] and Peter Nijkamp [4,5,*]

[1] Additech Fit, 700071 Iași, Romania; bam@rms.ro
[2] RomSoft, Research Department, 700291 Iași, Romania
[3] Axiologic Research, 700070 Iași, Romania
[4] Faculty of Management, Open University, 6419 AT Heerlen, The Netherlands; k_kourtit@hotmail.com
[5] Centre for European Studies, Alexandru Ioan Cuza University, 700506 Iași, Romania
* Correspondence: pnijkamp@hotmail.com

Abstract: Urban areas provide the seedbed conditions for a variety of agglomeration advantages, including incubator conditions for the ICT sector. This study aims to present the foundations for a data-driven digital architecture based on the notion of open access platform organisations (e.g., platform cities). The principles of coordinated multi-actor data handling and exchange mechanisms centre in particular on privacy and confidentiality regulations. These are highlighted and tested on the basis of the data exchange architecture in a particular Industry 4.0 sector, viz., the medical–pharmaceutical sector. To cope with these issues, self-sovereign data trust systems are designed and tested using an OpenDSU data environment. Several building blocks of this architecture are presented and assessed. The conclusion of this study is that OpenDSU technology offers promising departures for handling privacy-sensitive and confidential data exchange in open platform organisations, such as smart cities.

Keywords: digital service platforms; self-sovereignty; digital trust ecosystems; blockchains; decentralised brands; verifiable credentials; PharmaLedger; data-sharing unit (DSU); OpenDSU; decentralised identifiers

Citation: Balan, A.; Gabriel Tan, A.; Kourtit, K.; Nijkamp, P. Data-Driven Intelligent Platforms—Design of Self-Sovereign Data Trust Systems. *Land* **2023**, *12*, 1224. https://doi.org/10.3390/land12061224

Academic Editor: Nicos Komninos

Received: 25 March 2023
Revised: 1 June 2023
Accepted: 6 June 2023
Published: 13 June 2023

1. Intelligent Data-Driven Cities: Towards Platform Cities

"Digital tools and solutions are transforming public services and how governments respond to citizens' needs. Many cities have been actively engaging in modernisation and re-engineering of government processes and services and have seen high returns through simplified governance and increased efficiency, effectiveness and outreach. However, cities face many challenges in the processes of digital transformation including re-thinking governance, allocating or re-skilling and adopting new technologies, as well as legislative and policy issues." [1].

The compact land use in modern cities [2] is not only characterised by a geographically concentrated, high-density pattern of people and businesses in the urban built environment, but also by a spatial concentration of high-quality incubator conditions for new services, especially in our contemporaneous ICT age. Consequently, urban agglomerations and urbanised areas tend to become not only big data engines, but also advanced digital services machines and data factories.

In our digital society, the abundant presence of data has induced fundamental changes in our daily modus operandi. The contemporary information economy has heralded a new epoch in human history, in which—after large-scale industrialisation and global service delivery—data handling has become a critical component of socioeconomic progress. Data are sometimes even seen as "modern gold", which is decisive for the welfare of nations, regions and cities [3]. Notwithstanding the potential functional economic value of data, it ought to be recognised that data—just like gold—only create their value if they are used as

an intelligent resource in the complex multi-actor fabric of national, regional and urban economies [4,5].

A prerequisite for value generation from data is access to the user. Despite the current ubiquity of data, there is not yet a user-oriented platform for sharing data. Many data have an exclusive business function and do not lend themselves to broader societal use; other data are privacy-sensitive and are, by law, subjected to various strict use regulations [6]. Since data are not equally accessible in all countries, regions or cities and since the ability to handle complex data differs between people and also between geographical areas, data tend to create new equity issues, spatially and socially.

In order to grasp the emergence of platform cities, we need to understand the intricate tapestry of challenges and bottlenecks that traditional cities have encountered, such as the overwhelming pace of urbanisation, constraints imposed by limited resources and the pressing need for sustainable development. This introspective exploration sets the stage for the transformative emergence of platform cities, which arise as a profound response to these challenges. A first illustration of digital platforms across cities presents the impact that the development and spreading of these have at the urban level [7]. With a deep understanding of the human nature of urban societies, these cities leverage the power of technology and data-driven approaches to unravel the intricacies of urban complexities, paving the way for a harmonious and balanced urban existence.

In the past decades, we have witnessed the rapid rise of an unprecedented volume of digital services (e.g., in the educational sector, the logistics and distributional sector, the medical sector, the retailing sector, the transport and automobile sector, etc.). The supply of advanced digital services in the public sector came somewhat later but is now rapidly evolving (e.g., public procurement, urban healthcare services, security management, transit information, land use data, educational support, cultural provisions, etc.). The open access to public services data is, however, still fraught with many practical and legal issues. Despite the "digital revolution", the value creation in our data-driven economy is by no means optimal or satisfactory. Nevertheless, the current digital age has undoubtedly exerted a significant impact on the delivery and quality of public services.

In a recent study by ESPON [1], some numerical estimates are provided of the improvement in services and the increase in uptake in various European cities following the implementation of digital solutions: 91% of city services improved, and 30% of European cities saw a substantial reduction in operating costs after implementing digital technology (see Figure 1).

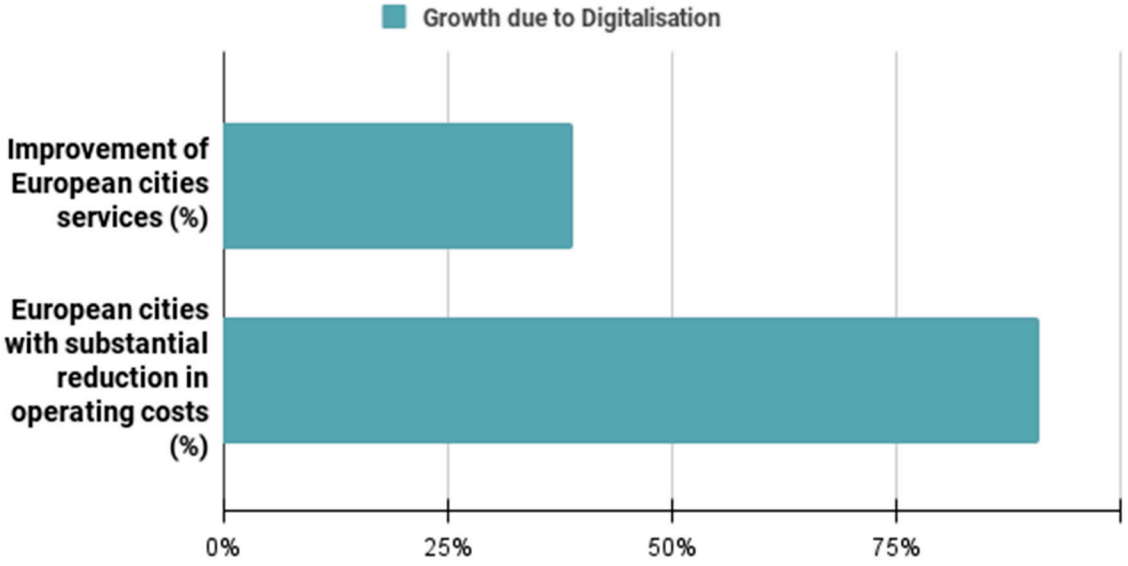

Figure 1. Implementation of digital technology effect. Source: ESPON (2020, p. 4) [1].

Clearly, there is an enormous variety in the provision of digital public services, ranging from spatial planning to welfare services. In the above ESPON study, a systematic list of important urban digital application fields in various European countries is presented, notably: "e-inclusion of citizens in local governance, spatial planning and construction, social and welfare services, education, urban public transport, road infrastructure and parking, healthcare, culture, leisure and sports, and tourism" [1]. The distribution of such services over different policy domains and different territories appears to be rather skew; however, there is certainly scope for improvement. The ESPON report ends with the recommendation to use cities as testbeds for new digital applications by opening up urban digital infrastructure so that public data could be more easily shared by various agents in the city, leading to an efficiency rise in the development and use of public service information.

Against the background of the above observations, we regard digital cities as spatial, open source data platforms characterised by multi-agent systems that are driven by distributed artificial intelligence [8]. Thus, digital cities house a range of smart activities. These epitomise a holistic vision of urban environments that transcend more efficiency and resilience. They cultivate an all-encompassing environment that encourages their diverse communities' active participation and engagement. Among the earliest iterations and proposals for platform cities [9–11], innovative ideas were set forth to reimagine urban environments. These early concepts laid the foundation for the transformational paradigm of smart and digital cities, exploring the potential of integrating advanced technologies and open data platforms.

The present paper seeks to present core principles of distributed data intelligence in such digital core areas (e.g., in platform cities) and to design the architecture of data-driven self-sovereignty in multi-agent shared platforms (including blockchain systems), while an empirical illustration of the potential of platform organisations will be presented for the healthcare sector to prove the possibility of simultaneous coexistence of data self-sovereignty and platform organisations.

This paper is organised as follows. After this introductory section, in Section 2, we will sketch the scene of digital technology applications in platform cities from the perspective of data sovereignty. The future development of platforms should consider the advancement of digitalisation hand in hand with the sovereignty of data. Section 3 will then zoom in on the concept of "digital trust ecosystems", followed by an exposition in Section 4 of the potential of self-sovereign data platforms in the healthcare sector. Next, Section 5 will provide an illustration of the design of a shared platform for digital trust ecosystems in healthcare, while Section 6 will conclude the paper.

2. Data Sovereignty in Digital Technology Services

2.1. Digital Technology and Self-Sovereignty

The unprecedented rise in modern technology—facilitated by the spearhead technology of ICT—has prompted the notion of a new—fourth—Industrial Revolution, sometimes coined Industry 4.0 [12]. Industry 4.0 is essentially a connected set of advanced technologies which, through integrated digitalisation, has led to an unprecedented increase in efficiency in all (public and private) sectors (see also [13,14]).

Digital technology is like an umbrella that covers computers, the internet, smartphones, and much more [15]. When we talk about digital technology, we may refer to artificial intelligence (AI), 5G, the Internet of Things (IoT), blockchains, digital twins, etc. With the help of digital technology, people's lives have improved substantially, starting from social connectivity, remote (online) working, entertainment, news gathering and so on. It is being scaled and distributed more and more, compared to previous periods. The adoption of digitalisation by the mass is increasing [16] and people are beginning to better understand digital technology, its scope and its essence. As individuals understand how the digital technology world operates—characterised by anonymity and uncontrolled power—they feel the need for autonomy, independence, security and the power to do what they really want without interference. Their needs could be assimilated into sovereignty

and self-organisation, but given the environment of interactive digital systems, we may call it digital sovereignty.

The generic term "sovereignty" [17]—understood as the power of an entity to govern itself—is often associated with state sovereignty and has, over time, undergone various reinterpretations. In the opinion of most people, the state should provide the proper environment for all their needs; a better mindset would exist if things were seen in their essence. Digital sovereignty should, therefore, be understood and implemented by each individual and then by individuals or agents be divided or shared between all actors involved (from state to cities, communities, companies, etc.).

The state has the competence to protect the borders of the digital world in its territory. Therefore, in this sense, the state addresses the issue of sovereignty in relation to other states. However, referring to digital sovereignty, the main objectives of the state are related to autonomy and security. Data localisation was the first governmental attempt to restrict access to specific types of data by limiting the storage and management of data to a defined space and perhaps to restrict the benefits for the regional suppliers of internet services [18,19]. The fragmented localisation of data was proposed in various states, from Europe to Brazil and India [20,21].

On the other hand, we have learnt in the meantime that the current COVID-19 pandemic is the main engine that has laid the basis for many digitalisation initiatives of cities, public administrations and local organisations [22]. The activities and operations of government institutions, businesses and legal entities can be seen as the functional responsibility of cities as administrative actors. The public and local administrations are asked to change their modus operandi and to change their software, programmes and technologies to ensure the transparency, decentralisation and security of necessary data. Digital sovereignty at the corporate level can be seen in relation to the digital environment from abroad. The purpose of sovereignty is, in this case, to create strong, spearhead industries so that they do not depend on the digital services of superpowers such as China, America, etc. Clearly, the geography of digital technology deserves due attention.

The ultimate beneficiaries of digital sovereignty are citizens. "Increasing digital literacy means raising users' strict awareness regarding digital technology and how their own data is used, and not just knowing how to use specific digital gadgets" [23]. The more citizens understand the phenomenon of digitisation and technology, the more they may want their rights to prevail. In this case, sovereignty or self-sovereignty can be equated with freedom, privacy, confidentiality and the right to decide freely and willingly. Therefore, citizens can be assimilated with self-sovereign identities (SSI) because they want as much autonomy as possible, which means that they can make decisions themselves from as many points of view as possible.

"Self-sovereign identity" (SSI) is an advanced identity management framework that ensures the security and maintenance of trustworthy identity records [24]. Decentralised systems are used for storing the identity records, granting users the ability to control their personal identity information [25]. Self-sovereign identity (SSI) solutions aim to grant users total control over their personal identity information (PII) by enabling them to store, manage and share their identity information on their own terms. In an SSI system, users give their explicit consent for the use of their PII, and can choose which parts of their identity information to share, with whom and for what purposes. This grants users greater privacy, control and autonomy over their identity, as well as protection against identity theft and data breaches, offering an alternative for problematic centralised storages [26]. The above objectives can be achieved and implemented with the help of decentralisation. In this regard, one way to improve digital sovereignty is through self-sovereign apps. The purpose of these digital revolutions is to eliminate the intermediaries (the third parties) and to have only two entities, so that the one who has control over the data would be just the individual himself (see also [23]), as is exemplified in blockchain systems, often with a local user orientation.

2.2. Blockchain Systems

Blockchain is a disruptive and often place-based usage and innovative technology, a distributed ledger that, due to its properties, traceability, immutability and transparency, ensures the trust between participants and revolutionises the interactions between them. Like any other new technology, this is not enough. According to Meiklejohn [27] and Kosba et al. [28], blockchain cannot guarantee transactional privacy. Another challenge is related to scalability (see [29]). To increase the adoption rate of blockchain technology, the concept of DApps (decentralised applications) was implemented to make the applications more "transparent, distributed and flexible" [30]. To achieve more control over our own data and to avoid trading with our personal information, decentralisation and DApps represent viable solutions. The DApps are working on a blockchain through smart contracts. It is a great advantage that smart contracts cannot be altered. Data and codes are kept securely, but in terms of the most relevant property, this part of the modification of the anchored data raises the issue of data privacy [31]. Other challenges are related to the possibility of scaling these DApps and solving the network congestion problem. Given that DApps have their own challenges, the mass adoption of these decentralised applications will be difficult.

Self-sovereign apps (SSApps) propose solutions to the challenging code execution of DApps, reduce the costs of infrastructure and the level of complexity regarding consensus algorithms and deal with sensitive data [32]. All information is stored off-chain; instead, it is notarised and anchored in the blockchain and does not load as much blockchain. The fundamental role of SSApps is to assure the entire control of the personal data to the user.

The idea of decentralisation can be hard to assimilate, especially for individuals who are not from this space (used with blockchain technology). Decentralisation [33] refers to the distribution of control and decision making across a network of nodes or participants rather than relying on a single central authority to manage the process. DApps (see also [34] can provide a solution to enable complete owner control over data. DApps are open source (transparency), more secure and more resistant to cyberattacks than centralised applications. Additionally, privacy is more protected in DApps compared to centralised ones. The development of DApps requires many resources, and most of the time, the additional cost is supported by the users or companies that use that DApp. In addition to this issue, regardless of encryption/anonymisation strategies being enforced on the on-chain data, the utilisation of data is possible through the correlation of data [35]. Therefore, according to these issues, the adoption of DApps by the masses, at a large scale, will be difficult to achieve.

As we mentioned in the previous paragraphs, the concept of self-sovereignty can be implemented in various applications where the users (regular users or companies) have control of the data and enjoy other advantages. Compared with DApps, the concept of SSApps is different because SSApps are "light" in the sense that, because of their operation, they do not load very much the "blockchain", while in principle, every SSApp can have its own "blockchain". The SSApps are agnostic and have the same properties as data-sharing units (DSUs) [36] in the sense that a DSU can contain any type of code (e.g., HTML, CSS, JS) required to launch and run an application in a browser and view like any other web application or even in another environment capable of executing the application code loaded from the DSU and displaying any output. Compared with DApps (see, e.g., [34], one can use just Solidity and no other language programming. For example, DApps' smart contracts cannot be modified/edited and can only be updated with another smart contract that contains the old smart contract. Another advantage is that SSApps can be shared with more users, while any update or modification can be seen in real time (e.g., Google Docs). With the key, the owner holds total control of application data which are cryptographically managed [36]. Additionally, in this case, spatial user networks—often at a local scale—may be very important.

3. Digital Trust Ecosystems and Decentralised Brands

The concept of "Digital Trust Ecosystems" (DTEs) is used to create new governance models for economic and social activities taking place between big corporations or even between companies and individuals using digital technologies [23]. Despite their global scope, they are often based on local or regional constellations of users. A digital ecosystem can be defined as a dynamic, interconnected network where the participants (stakeholders, customers, employees, individuals) interact with each other, in this case digitally, to create value for all entities that are part of the network concerned. A digital ecosystem is more than a conventional ecosystem. Over time, many have come to believe that changes in technology have always been an important component in the progress of human societies [37]. Therefore, progress is associated with the keyword around which everything revolves, viz., "trust". Trust can be described as the conviction or confidence in the honesty, competence or moral character of an entity. The trustworthiness of an entity refers to the degree to which it merits trust based on its reliability, credibility and consistency [38]. The concept of "trust" is subjective and amplified over a period of time; it refers to the level of confidence given by the participants of a virtual or physical network in the organisation's ability to maintain technology resources and information assets in a way that ensures privacy, integrity and security for them.

A digital trust ecosystem is a digital environment based on a multitude of connections created between the stakeholders, parties and entities, where the trust they give is the basis of the links created between them to meet their needs or objectives in a specific context, while there are no intermediaries and where the trust relationships are interconnected and work under a digital governance framework. Since 2005, the internet has exposed us to growing dangers (proliferating episodes of theft and deception) that will cumulatively erode public trust in the Internet [39]. For example, a recent survey found that over half of Americans do not use a product or service due to concerns about their privacy [40]. In this sense, it is challenging to propose the specific concept of DTE as a solution to actual people's needs and their concerns. This implies that a transparent and well-defined governance model for the ecosystem is necessary [41–44]. Additionally, to further highlight the direction in which a new DTE system may be heading, according to a study by Forrester Research, by the end of 2022, around 58% of US sales will be partially or entirely carried out in a digital ecosystem [45].

One of the first attempted governance revolutions emerged through the concept of DAO (Decentralised Autonomous Organisation). A DAO is a "virtual" organisation where the governance of human society is conducted without intermediaries in order to obtain "objective" and "fair" governance which operates with "smart contracts" technologies based on the idea that "code is the law" and that everything that happens is "on-chain" (e.g., Dtravel DAO) [23]. According to [46], numerous identity providers generate revenue by gathering behavioural data from their users, which they utilise to create advanced systems for analysing and predicting user behaviour. Therefore, the purpose of the concept of DAO was to replace the intermediaries in social and economic interactions, but scientifically this is just the incipient form of a "Decentralised Brand". Clearly, the role of institutions as a support mechanism is important in this context.

To better understand DTEs, we first interpret the concept of a "Decentralised Brand", which normally has both an organisational and geographic feature. Any form of human organisation has two types of important characteristics: it has a pattern of functioning and a name that is associated with its identity and its own "personality" that reflects the characteristics resulting from its pattern of functioning [23]. These two characteristics may be assimilated as a "community brand". Compared to traditional brands, community brands provide some unique and valuable benefits to consumers [47]. The functioning pattern is the social technology (political and economic governance) that is copied and modified by each community individually [23]. It might be functional for people to organise themselves into small "villages" that we could call "Smart Villages" to represent their interests.

It is noteworthy that after more than two centuries, the idea of limiting the power of states over citizens, promoted by Adam Smith's seminal book "The Wealth of Nations" (1776), can be revisited with the help of the concept of a "Digitalised Brand", where the idea of "liveable cities" seeks to imagine cities as environments that facilitate the free collaboration between communities that respect the principle of "membership as stake", which we call "Smart Villages". Moreover, this type of organising the governance of cities will have the benefits of a significant common property (cooperative or shareholding) with an economic and social safety net which has the possibility to be represented by dedicated people that have a tangible common interest with the people they represent. Clearly, the direct solutions to immediate current problems include crowdfunding, with DTEs as alternatives to the big corporations that build an economy that may weaken civil liberties and democracy [23].

The concept of a "decentralised brand" might be implemented and used more transparently with the help of digital sovereignty. On the other hand, the future challenge is to not consider digital sovereignty as an aim itself, but to create the procedural scenery for a digital trust ecosystem with democratised digital sovereignty [48]. Therefore, decentralised brands serve to ensure at least both security and transparency. Usually, structured forms of social organisations are created to benefit only those who run it, in ways that are not necessarily transparent to "members", though they generally lead to instability (or even the destruction of that social entity), but also to progress (as a side effect of the arms race to achieve fairer relationships and better benefits).

The heading to DTEs is clear, but their establishment faces a number of problems, such as "a natural tendency toward centralisation" because the majority of actors within the ecosystem have the culture, experience and habit of classical centralised governance, and it is natural that the existing experience will influence the process of establishing the governance rules of the DTEs or "cultural and sometimes legal conflict with existing internal policies in the organisations which form the ecosystem" [23]. Of course, there are many other problems that make the creation and adoption of DTEs harder, but there are also many new opportunities. In this sense, by way of example, one of the most visible emerging DTEs is PharmaLedger [49] which is creating a blockchain platform and a shared governance body for numerous use cases in the pharma industry [23]. This will be used as an example later on in this study.

Clearly, DTEs are facing various non-technological challenges, in particular: ownership and access of data, autonomy and decentralisation, consistency and interoperability, security and confidentiality, and freedom and surveillance. These issues will be touched upon in the remaining part of this paper, with reference to new digital developments in urban healthcare and the pharma industry.

4. Self-Sovereign Data Platforms and Urban Healthcare: Practical Example

4.1. Digital Advances in the Healthcare Sector

In recent years, our world has been confronted with the global COVID-19 pandemic; cities are increasingly the spearheads of concern regarding human health. During this time, several decision and policy issues were frequently related to materials distribution and its transportation time. The solutions were represented by emerging new opportunities. For example, drones are a promising technology and represent a solution to combat public health emergencies [50]. Drones, called unmanned aerial systems (UAS), can be implemented in various scenarios [51]. Through the help of artificial intelligence, machine learning and other techniques, drones can perform independent actions and operations. In addition, they can be a substitute for transportation in areas where road access is nonexistent [52]. In this context, augmented reality (AR) is, according to Azuma (1997) [53], defined as "the concept of digitally superimposing virtual objects on physical objects in real space so that individuals can interact with both at the same time". AR technology is impacting cities to become [54] "smart, digital, and connected in various ways, including disaster response, enabling medical services and navigation management". Drones

and AR technology may change cities in a way that will allow citizens to live in a safer and cleaner environment. In support of these presented ideas, emerging tools such as video surveillance [55] and parking management [56] can be seen as modern sustainable solutions. Drones, AR and other technologies that use cloud computing enjoy a rising interest in recent data-based research. These technologies represent challenges for cloud computing regarding the collection, storage and sharing of data. Besides these, ensuring data privacy is the new challenge for all these new technologies. According to Diaz et al. (2016) [57], the adoption of cloud computing allows people to interact with data "in a dynamic and efficient way". We cannot exclude artificial intelligence (AI) and machine learning (ML) concepts through cloud computing that will be more efficient, strategic, secure and, most importantly, automatic. QoS, SLaS and FECA represent the future trends in cloud computing [58].

4.2. Smart Cities and Healthcare

Smart cities [59–61] aim to connect the existing infrastructure (healthcare, education, transport, cybersecurity challenges, etc.) in a way that provides high-quality living. Healthcare Industry advanced from 1.0 to 4.0 and has, over the years, revolutionised medicine [62]. For example, over the past decades, in Amsterdam [63], the concept of smart cities has been introduced, improved and presented as a strategic solution to well-known urban challenges. The goals of smart cities are to improve sustainability [64,65], security and privacy [66]; comfort; urbanisation [67] and professional public services. Clearly, smart cities are a generic concept describing that the urban space is characterised and governed by digitally oriented services, such as advanced healthcare services or pharmaceutical products, for instance.

The health sector represents an industry which is determinant in our lives. Healthcare in smart cities plays a significant role, and the quality of care may increase due to the emerging evolution in technological innovation. A healthcare ecosystem assembly of smart cities, at a micro or macro level, contains interactions between citizens, patients, doctors, hospitals, research institutes, etc. According to King (2017) [68], the purpose of healthcare services is to provide greater interconnectivity which has "significant benefits to patients, physicians, payers and drug developers". In the centre of these connections, the common and representative points are assigned to the "raw materials" of the healthcare sector, i.e., data. It is evident that such data often have a territorial usage dimension. The increase in electronic patient records and collection, generating more and more data, leads the healthcare sector to the concept of "big data", a term that describes that the data "is large and unmanageable" [69], and like in any other sector, this has its benefits and challenges.

4.3. Challenges and Bottlenecks in Healthcare in Smart Platform Cities

Patients are expected to receive the best and most accurate advice about and treatment of their health problems. Topol (2019) [70] noticed that "we are able to digitise and quantify almost every aspect of the human body". It is not enough to just collect and record these data. The volume, speed and variety of health data make healthcare workers and patients face challenges in managing, sharing and accessing health records in a way that ensures privacy, security and confidentiality. In addition, at the moment of recording data, there are still healthcare services offered that interfere with a provider, a third party. Clearly, the healthcare industry needs to maintain patients' trust.

Depending on the country, there are different initiatives that offer support in understanding the regulatory changes and challenges that new healthcare products involve in the development process for easy procurement and adoption. In the UK, for example, the "Code of practice for digital and data—driven health technologies" (updated 19 January 2021) was created to help developers follow the regulation of good practice that should be incorporated to ensure the trust encompassing ethical codes, usability and accessibility, technical assurance, clinical safety, data protection, data transparency, cybersecurity and interoperability [71].

Patients and healthcare professionals are confronted with the difficulty of securely accessing, managing, integrating and exchanging health records [72,73]. Privacy and security are the main limitations in implementing digital healthcare record solutions within the public sector [74], followed by the constraints presented by the three concepts known as the main characteristics of big data: volume, speed and variety (see Figure 2). From an administrative point of view, the major challenges faced in the healthcare sector are limited staff, poor infrastructure and limited hospital beds in urban agglomerations.

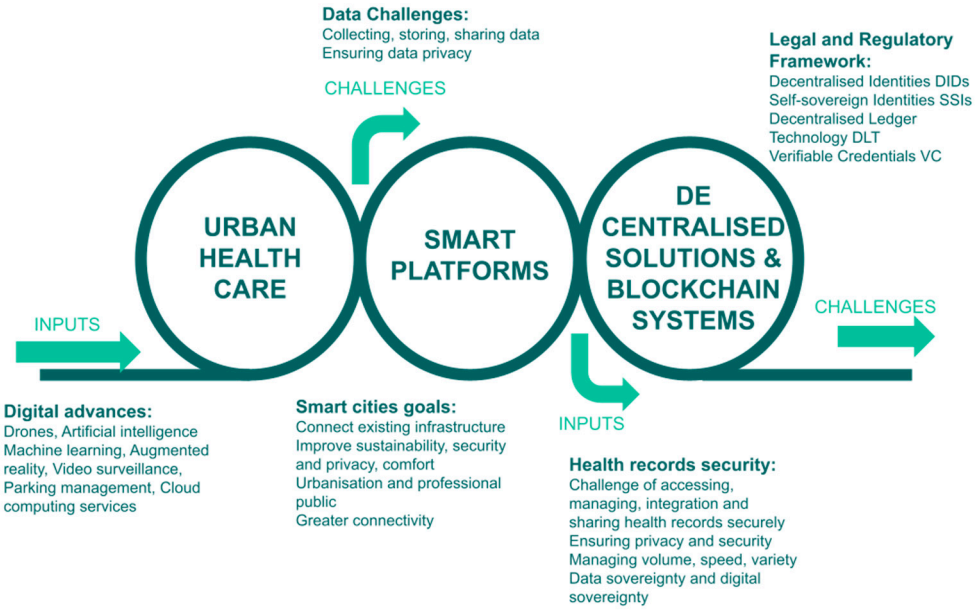

Figure 2. Perspective overview of urban healthcare framework in the context of smart cities. Decentralised solutions and blockchain systems to ensure security in accessing health record in a digital word.

In developing a performant centralised platform that improves citizens' interaction, it is pertinent to consider the ownership and control of data and not affecting privacy and confidentiality regulations. This is complicated in the case of centralised platforms dealing with data from multiple actors. When considering digital urban healthcare solutions, personal data need special attention. Tan [75] refers to this complication and presents a study on legal perspectives on the requirements and their challenges in adoption from two points of view on sovereignty: data sovereignty and digital sovereignty. In this context, the awareness of the importance of data and their privacy [76–78] over digital platforms prompts a transition from centralised toward decentralised solutions where people are in control of their own data. Cities tend to become both data-user and producer communities.

4.4. Decentralised Solutions and Blockchain Systems in Urban Healthcare

The acquisition of appropriate information and access services in different sectors of a digital society may be facilitated through internet platforms. Creating a digital identity on different platforms is common nowadays, but it is not enough to ensure security in accessing the data. This initial step of creating a digital identity should be followed by safe verification and validation processes, which may face many issues and constraints when they are dependent only on one entity, system or source that is trusted to authenticate, verify or provide access to certain information or resources, which could be corrupted and easily attacked, in both physical and digital identities.

One of the most immediate solutions to these problems was demonstrated to be decentralised identities (DIDs) [79], which have lately been created to manage the separation between identities from centralised database registries, entities and services that offer authentication and authorisation services to verify a person's identity and grant access to specific resources or information and certificate authorities, as the name suggests (See

Figure 2). Based on ten principles [80] with the user at their core, the Self-Sovereign Identity (SSI) model addresses the challenges of digital identities, for which preliminary models, prototypes and demonstrations that are designed to test and validate their feasibility, viability and potential benefits are ongoing and under continuous processes; designing, building, testing and improving. The model is still being actively worked on and developed, and updates and new features are added regularly.

Distributed ledger technology (DLT) [81] supports the automatic creation of digital identities and their associated decentralised and immutable registry. Similar to the way in which physical credentials are tied to identities, verifiable credentials (VC) [82] are bound with digital identities in web environments [83], where it is more challenging to verify and validate the information since digital arrangements are more quickly falsified than their physical and biological correspondents. In this sense, to create trust in a trustless environment, VCs must be secured from a cryptographic point of view, consider privacy and be machine verifiable [82]. Complementary mechanisms may be instrumental to create trust in a digital environment, often in an urban context (see Figure 2).

Owing to its inherent properties and manifold advantages, blockchain technology emerged as a pivotal and transformative solution in shaping the trajectory of the healthcare sector's progression [84]. Blockchain technology facilitates the trustworthy and optimal exchange of vital medical data among diverse healthcare organisations, fostering heightened synergy, streamlined operations and superior patient results. This technology already has various applications in the healthcare sector [85]. For example, MedRec [86] is a healthcare decentralised app that empowers patients with control over their medical records via blockchain. Providers securely access and update records, ensuring data integrity and privacy through smart contracts. Patients grant permissions, fostering transparency, collaboration and data protection. In addition to MedRec, other notable decentralised applications in healthcare are MedBlock, MedClick and Coral Health [87]. MedBlock utilises blockchain for secure medical record storage, ensuring data integrity and privacy. Additionally, MedClick leverages blockchain for real-time data access, improving communication and streamlining workflows, and Coral Health revolutionises health data management, safeguarding the privacy and empowering individuals with control over their information. Therefore, through the strategic utilisation of blockchain technology, these decentralised applications enact a paradigm shift in the storage, accessibility and sharing of healthcare data. This approach engenders substantial breakthroughs and enhancements within the industry, culminating in remarkable advancements and improvements.

5. Illustration of Open Data-Sharing Units (DSUs) and PharmaLedger

5.1. OpenDSUs

In this section, we will illustrate the potential of decentralised digital solutions based on DTEs by means of recently developed tools that were developed and tested in the context of the PharmaLedger consortium [49]. To create a DTE, the PharmaLedger consortium partners examined and proposed solutions for specific use cases developed in the PharmaLedger research project aiming to avoid confidentiality concerns among potential users. The main challenge was building trust in a trustless digital environment without uncovering information (or only quasi-zero information) regarding the identities of the interacting users and entities. To solve some of the most challenging pharma blockchain business use cases—such as electronic leaflets, medicine anticounterfeit, supply chain, finished good traceability and clinical trial management (from recruitment and consenting to participate in personalised medicines)—the PharmaLedger group decided to adopt the OpenDSU technology [36] infrastructure (see Table 1).

Table 1. Open DSU methodologies for ensuring confidentiality.

OpenDSU Supported Methodologies	Added Confidentiality Value
Cryptographically validated code	Enhances security by assigning responsibility and verifying the authenticity and integrity of code through digital signatures, ensuring it has not been tampered with and clarifying accountability in multi-party development scenarios
Zero-access blockchain anchoring	Minimises on-chain data storage by storing encrypted anchors and metadata on the blockchain while keeping the actual data inaccessible to anyone other than the owner
Symmetric encryption	Safeguards sensitive data, storing encrypted bricks with unique keys on servers to prevent unauthorised access and correlation and ensuring confidential communication between wallets
Multiple blockchain domains	Facilitates domain-specific storage and access of data, thereby reducing the risk of metadata correlation attacks
Decentralised gateway architecture	Ensures robust security and privacy by leveraging a distributed network of nodes for data storage and access, minimising single points of failure and enhancing protection against data breaches
Plunginisable DID methods	Offers flexibility by supporting various DID methods and actor identification methods
Validation strategies	Offers flexibility to balance confidentiality and audibility and tailors the management of decentralised data to specific needs
OpenDSU cryptographic methods	OpenDSU's extensibility allows for easy customisation and adaptation to new cryptographic techniques, achieved through anchoring code signatures in a ledger, ensuring auditability, security and a seamless transition to stronger confidentiality measures

To create the desired confidentiality and privacy awareness, an OpenDSU technology (see Table 1) was designed based on a variety of combined methodologies.

5.1.1. Cryptographically Validated Codes—A Code Signing Avoids the Associated Risks of Security Models Based Only on Data Encryption

Signing the code can help unambiguously assign responsibility for the code. Code signing is a process where a digital signature is added to a piece of code to verify its authenticity and integrity. This signature confirms that the code has not been tampered with since it was signed and that it was signed by the entity specified in the signature.

By signing the code, the signatory is making a statement that they are responsible for the code and that it meets certain standards or requirements. This can be useful in situations where multiple people or organisations are involved in developing a piece of software, as it helps clarify who is responsible for which parts of the code.

However, it is important to note that code signing alone is not enough to ensure the security or quality of code. It is just one tool that can be used as part of a larger software development process. Other measures, such as code review, testing and documentation, are also important for ensuring the quality and security of code.

While digital signatures and proper credential management can help improve the accountability and responsibility of code suppliers, in the case of supply chain use case, for example, attacks can be complex and involve multiple layers of suppliers and distributors. In some cases, the initial attack may occur at an earlier stage in the supply chain and may not be immediately apparent to the downstream suppliers and distributors. Additionally, attackers may use sophisticated methods to cover their tracks and avoid detection. However, by implementing digital signatures and proper credential management, OpenDSU can help ensure that code suppliers are held accountable for the code they provide, even if they were themselves victims of a supply chain attack.

This can create a culture of responsibility and encourage businesses to adopt better development methods and security practices. In general, it is important to have a comprehensive approach to managing the security and integrity of software supply chains. This can involve a combination of measures, such as vetting suppliers and distributors,

implementing security best practices, monitoring suspicious activity and having a plan in place to respond to security incidents. Improving responsibility and accountability in software supply chains through measures such as digital signatures and proper credential management can have an indirect but positive effect on confidentiality.

By implementing these measures, businesses can ensure that the software they receive from their suppliers and distributors has not been tampered with or compromised. This can protect against supply chain attacks that may compromise the confidentiality of sensitive information.

Additionally, the culture of responsibility and accountability that these measures help create can encourage businesses to adopt better security practices overall. This can include measures such as data encryption, access controls and monitoring suspicious activity, which can help further protect against confidentiality breaches.

While measures such as digital signatures and credential management may not directly address confidentiality concerns, they can help create a more secure and responsible software development and distribution ecosystem, which can indirectly improve confidentiality.

5.1.2. Zero-Access Blockchain Anchoring—To Minimise the On-Chain Data Storage to Encrypted Anchors and Information to Other Blockchain Network Participants

The concept of zero-access blockchain anchoring entails storing encrypted data on a blockchain in a manner that restricts access to all but the data owner. This technique relies on cryptographic keys and digital signatures to ensure that the data can only be accessed and modified by the authorised owner. The fundamental idea is to store an encrypted version of the data as an anchor on the blockchain, accompanied by metadata describing the data and the encryption key. The actual data are stored elsewhere, such as in a private data storage system or an off-chain storage service. To access or modify the data, the data owner utilises their private key to decrypt the information and carry out the necessary operations.

Implementing this technique allows for minimising the volume of data stored on the blockchain, as only the encrypted anchors and metadata are stored. This can alleviate the costs and scalability concerns associated with on-chain data storage. Moreover, since only the data owner possesses access to the actual data, this technique significantly enhances the privacy and security of the information, preventing exposure to other participants on the blockchain network. This aspect holds particular significance when dealing with sensitive or confidential data, such as personal or financial information. Zero-access blockchain anchoring demonstrates promise as an approach to securely and efficiently store data on a blockchain while concurrently reducing the amount of data requiring on-chain storage.

5.1.3. Symmetric Encrypted Messages

The PharmaLedger system stores all DSUs as symmetrically encrypted bricks on servers. Each brick is protected by a unique key that is randomly generated to safeguard the confidentiality of sensitive data. This technique prevents the unauthorised access and correlation of data.

Symmetric encryption is also used to secure communication between OpenDSU wallets. The exchange of encrypted messages between wallets is a crucial aspect of ensuring the confidentiality of communication in the PharmaLedger system.

5.1.4. Multiple Blockchain Domains and Decentralised Gateway Architecture (DGA)

OpenDSU is designed to support multiple blockchain domains, which allows for data to be stored and accessed in a way that is specific to each domain. This means that data can be segregated by domain, which can help minimise metadata correlation attacks.

In addition, OpenDSU's DGA (Decentralised Global Access) architecture is designed to provide a high level of security and privacy. The architecture uses a distributed network of nodes to store and access data, which helps prevent single points of failure and reduces the risk of data breaches.

By using OpenDSU's DGA architecture to support multiple blockchain domains, data can be stored and accessed in a way that minimises the risk of metadata correlation attacks. This can help protect the privacy and security of sensitive data, while still allowing for efficient and effective data management.

5.1.5. Pluginisable DID Methods and Validation Strategies

OpenDSU, which is an open-source library for decentralised data management, allows the addition of various DID (decentralised identifier) methods, as well as other methods for identifying actors, such as X.509 certificates, individuals or organisations. This provides flexibility for developers to choose the appropriate method based on their specific use case and requirements.

The validation strategies concept in OpenDSU allows developers to choose the appropriate level of compromise between confidentiality and audibility. This means that they can balance the need for data privacy with the need for auditability and accountability.

In addition, OpenDSU allows the integration of code libraries that implement any DID method. Different DID methods have different privacy characteristics, which provides developers with the ability to choose the DID methods that ensure the right balance between trust, audibility and privacy.

From this perspective, OpenDSU provides developers with a flexible and customisable framework for managing decentralised data that can adapt to their specific use cases and requirements.

5.1.6. OpenDSU Cryptographic Methods

OpenDSU is designed to be extensible, which means that it can be easily customised and adapted to support new cryptographic techniques and technologies as they emerge. This is achieved by anchoring code signatures in a ledger, which enables developers to introduce new cryptographic techniques gradually over time.

By anchoring code signatures in a ledger, OpenDSU provides a tamper-evident record of all changes to the codebase. This means that any changes made to the code can be audited and verified, providing an additional layer of security and ensuring the integrity of the system.

This approach enables the gradual introduction of new cryptographic techniques to protect confidentiality. For instance, if a new cryptographic technique is developed that provides stronger confidentiality guarantees, developers can introduce it gradually by signing new codes with the new technique and anchoring it in the ledger. This enables a smooth transition to stronger cryptographic techniques without disrupting the existing system.

The extensibility of OpenDSU enables it to adapt to evolving security threats and stay up to date with the latest cryptographic techniques and technologies.

Based on these benefits, confidentiality methods were further adapted in the selected PharmaLedger use case toward special methods. In this sense, based on the uniqueness and particularity of the use case, special methods were selected.

5.2. Special Methods in Selected PharmaLedger Use Case

Privacy issues and risks can be classified as "privacy issues", "trade secrets issues" and "legal issues". Privacy issues involve the protection of the personal data of patients (in particular). The problems related to the protection of "trade secrets" arise from the fact that, due to the nature of the blockchain, the systems of the companies are connected and could leak sensitive information about commercial activity. Problems of a "legal nature" are due to non-compliance with the legal provisions or internal procedures of companies.

Decentralised identifiers (DIDs) are verifiable decentralised identities that are bound to physical identities or human persons. It is strictly forbidden to attach any information to the DID document itself, even a person's public name or other identifiable information such as email address. The DID correlation represents an important issue raised by the user community. A reasonable solution is to use pairwise DIDs to assure a still-unique rela-

tionship. As an illustration, a clinical site actor (using advanced randomisation techniques) may issue an implemented anonymised DID, add verifiable credentials and present it to the trial participant using the public DID of the trial participant, but without storing it in the clinical site enclave. The trial participant uses the verifiable presentation to verify the issued credential, validate it and create the anonymised DID. From this point on, during the trial, the patient no longer uses their public DID for message exchange between themselves and other actors (see Figure 3). Thus, all the actors using the trial participant data use the anonymised DID, and even the clinical site will no longer know the public DID of the patient.

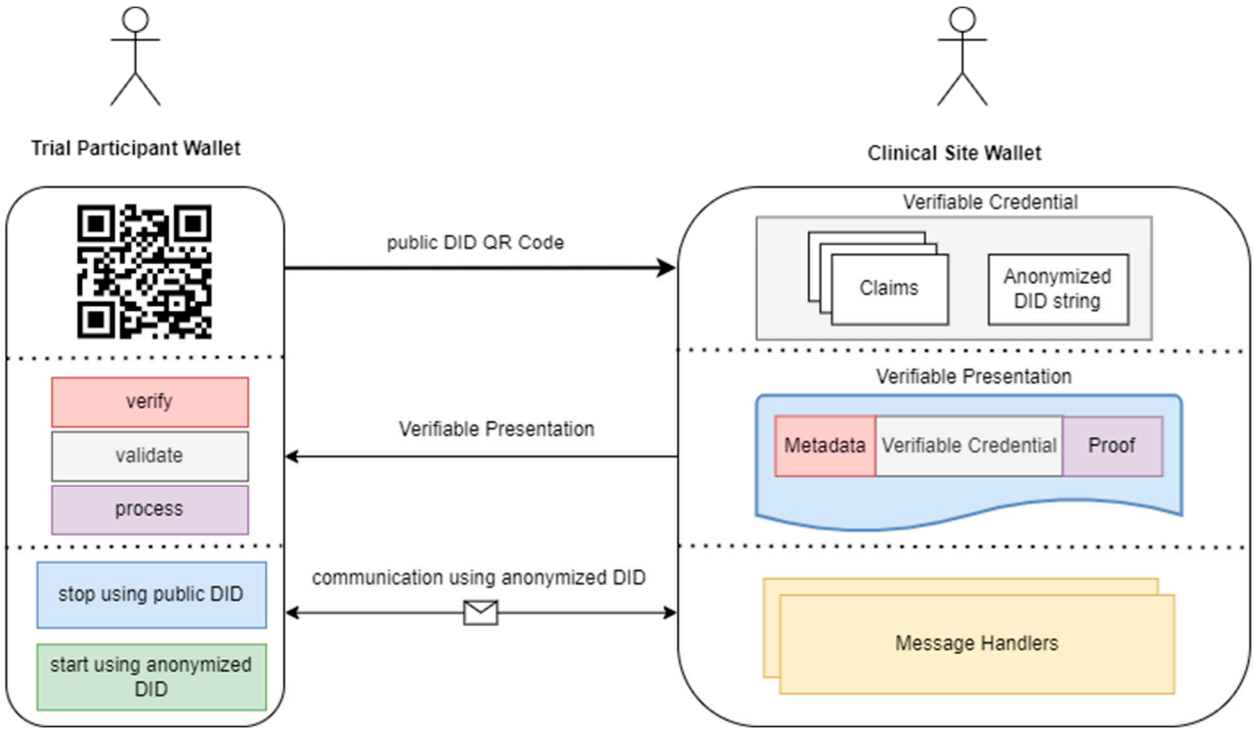

Figure 3. Verifiable presentation for anonymised DID creation (Source: PharmaLedger 2022 [88]).

To avoid composition techniques that can converge to unique digital and identifiable fingerprints, clinical sites should act carefully when working with the private data of patients. Some privacy-by-design techniques have, in the meantime, been developed to ensure anonymised personal information and to ensure that anonymised health data trial sponsors (e.g., pharma companies) are able to work with vast amounts of data.

Here, we provide here a simple illustration. In Figure 4, we present how the patient information is split into multiple DSUs and the HCP enclave. Furthermore, when health data records should also be written by a different actor (e.g., an IoT adapter), a new DSU is added and mounted in the patient's DSU to achieve the granularity of data access so that the privacy-by-design mechanism is fully functional.

The IoT adapter may be integrated as an intermediate tool able to communicate and exchange information between actors and external systems. Additionally, the adapter has the function of storing the data locally, accessing and communicating with external databases (e.g., clinical databases) and creating the DSUs to share information with the actors. The IoT adapter receives data from the IoT devices, transforms IoT device data into a globally accepted medical form and then stores it in a hospital database to expose various stakeholders through secure application programming interfaces (APIs), which comprises a set of defined rules that explain how computers or applications communicate with one another.

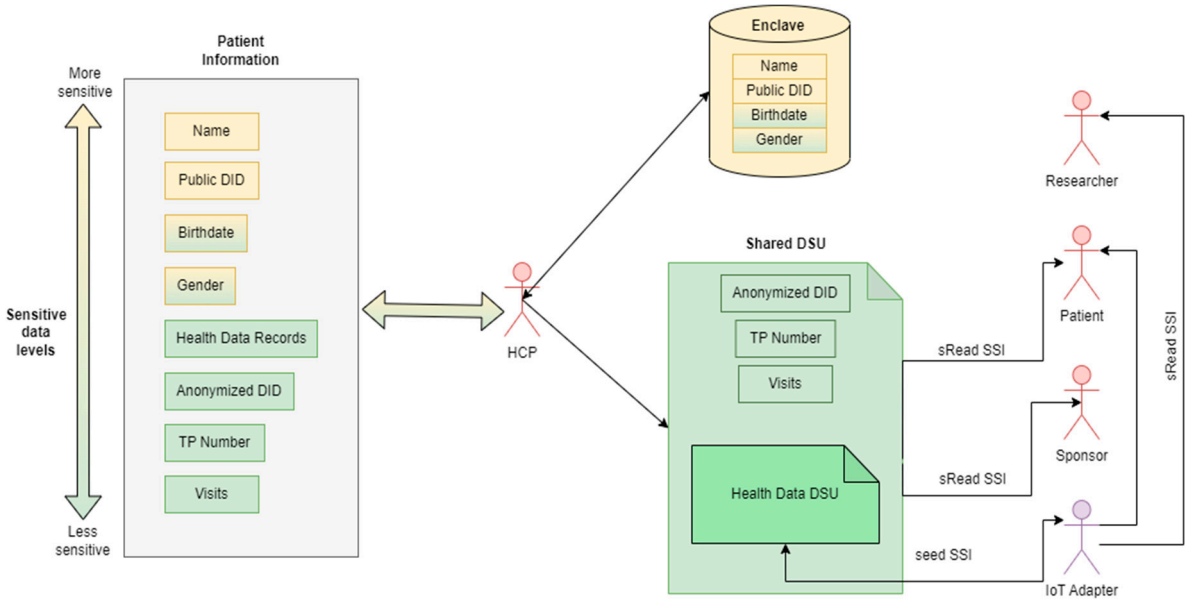

Figure 4. Privacy by design using enclaves and nested DSUs (Source: PharmaLedger 2022 [88]).

The transformed data are stored in the clinical database, far-chain data storage. Furthermore, the IoT adapter helps expose different APIs to external actors by securely utilising the patients' consent. In addition, the IoT adapter stores the trial participant data in the clinical database as observations. The observation process starts after the clinical site assigns a device to a trial participant. In addition, before device assignment, a device must be registered in the IoT adapter. Finally, the researcher can create, update and delete evidence stored in the clinical database.

Furthermore, the IoT adapter shares patient data by creating DSUs locally in the IoT adapter wallet (the owner and the source of trust of the IoT adapter wallet is the hospital) and by sharing patient observations with the clinical site, patient, researcher and sponsor. In addition, the IoT adapter manages the DSU keys and device assignments to the trial participant. Finally, the IoT adapter initiates the data matchmaking process to find candidates for trial participants to share data. The permission process for using such data is complicated and follows predefined rules.

5.3. A Design Perspective

In the PharmaLedger approach, the researcher generates a study from the relevant SSApp and requests a specific type of data (e.g., SPO2). This request is delivered to the IoT adapter, which acts as an intermediate step to facilitate communication between all actors (clinical site, sponsor, researcher and trial participants). The IoT adapter executes another algorithm called "Data Matchmaking" which searches for the data requested and generates potential matches. Each match stores the patient's information, such as their DID and patient number and the device's ID with the available data. The trial participant has a profile with personal settings. If they are allowed to receive invitations to participate in studies and share their data, then the following actions are undertaken. If not, there is no continuation of this algorithm. The matches are sent to each patient candidate found during the previous process. The patient can now see this request as a pending study in the studies menu on their application. The patient can choose to accept or reject sharing the data. In case of acceptance, the patient informs the IoT adapter that they consent to sharing. The IoT adapter reports to the researcher that a new participant has been added to the study. The study object is updated with an array of patients currently sharing data. In any case, the patient can stop sharing/donating data, and the permission is immediately removed from the researcher's study. It is important to note that the data are generated, anonymised and sent to the researcher' SSApp only when the study is completed.

The OpenDSU architecture is designed around the concept of signed code and data stored in data-sharing units (DSUs), which provides a secure foundation for integrating new privacy techniques. This is because the signed code and data in DSUs are tamper evident, meaning that any unauthorised modifications to the code or data can be detected. This tamper-evident architecture provides a high degree of confidence that the data stored in the DSUs is accurate, reliable and secure. As a result, it encourages the further integration of new privacy techniques that can enhance the security and privacy of the system. Furthermore, the modular architecture of OpenDSU allows for the easy integration of new privacy techniques and technologies as they emerge. This means that the system can evolve over time to support new privacy-enhancing techniques without requiring major re-architecting or redesign. Overall, the use of signed code and data in DSUs provides a strong foundation for integrating new privacy techniques into the OpenDSU architecture, which, in turn, promotes the continued evolution and enhancement in the system's privacy and security capabilities. These methods, supported by the OpenDSU architecture, allow the construction of new solutions for confidentiality and privacy issues in a way to create the benefits needed for specific application environments. If the environment is stable and if the actors and the way information is shared between actors are known, one can analyse the issues and risks of attacks on confidentiality and privacy and develop and adopt proper solutions.

The OpenDSU approach is based on the idea that a single blockchain technology or deployment cannot cover all use cases of an industry efficiently or cost-effectively.

Attempting to use a single blockchain technology or deployment to cover all use cases would require a significant amount of resources and would likely result in a complex, inflexible and difficult-to-manage system. This is because different use cases have different requirements and may require different blockchain technologies or deployment models.

The OpenDSU approach recognises this and provides a modular, extensible and flexible architecture that allows for the integration of different blockchain technologies and deployment models as needed. This approach enables developers to choose the appropriate blockchain technology or deployment model for each use case, resulting in a more efficient and cost-effective system.

Overall, the OpenDSU concept recognises the limitations of attempting to use a single blockchain technology or deployment to cover all use cases and provides a more flexible and adaptable approach that can better meet the needs of different use cases and industries.

OpenDSU provides a unified architecture that enables the reuse of code where possible but does not fix the blockchain technologies or deployment patterns that can be employed. This allows OpenDSU to be implemented in different ledgers with tailored capabilities, depending on the specific use case and requirements.

Moreover, the flexibility of the OpenDSU approach enables it to be deployed in different ways, which is particularly important to ensure the privacy and security of sensitive data. Even with the most advanced privacy-preserving technology available, it may not always be necessary or desirable to share data, anchors, zero-knowledge proofs or anonymised transactions if there is no real business or technical requirement for sharing. Therefore, the main aim of the OpenDSU approach is to facilitate secure and auditable data sharing while preserving privacy to the best extent possible in the context of the sharing economy or platform cities. The OpenDSU concept aims to solve coordination and confidentiality issues in off-chain and near-chain storage.

In most cases, the DSU-anchoring model [89–92] of OpenDSU can avoid or mitigate the need to reveal any type of data to the entities which generate or provide the software; the OpenDSU approach shifts the computation off-chain to wallets or agents controlled by participants, rather than utility providers. While OpenDSU's validation at the anchoring level may not be sufficient, as it can be susceptible to spamming attacks where an attacker creates multiple versions of DSUs to block business processes. Such attacks are usually noticed quickly in practice. It goes without saying that smart DSU solutions in various industrial sectors (such as the pharma-medical sector) need the seedbed conditions of

platform cities: DSUs do not operate in isolation. Our experiments with this approach have shown that this proof of concept is very promising.

6. Concluding Remarks

Digital technology is often seen as a spearhead technology in the domain of the emerging Industry 4.0. The handling and coordination of an abundance of data in both the private and public sector have become a major challenge for both the research and policy communities. Smart platforms are increasingly becoming the vehicles for a sharing economy based on the design of efficient information gathering and exchange among multiple actors. This megatrend has induced the development of a great variety of many new products and services in the urbanised world, as is witnessed by a wealth of new novel e-services, including supporting digital network constellations such as intelligent platforms. A novel recent development is the rising popularity of blockchain systems and self-sovereign trust systems. Thus, urban density and proximity provide a stimulus for a new generation of advanced digital services. This trend is documented and illustrated in our study on the basis of advanced digital platforms in the healthcare sector.

In many cases, the information processing challenges have a geographical connotation, as is witnessed in recent advances in geoscience, geodesign, spatial dashboards, digital twins, etc. A particularly important sector where the exchange of geographically bound information is often critical is the pharmaceutical and medical sector, given the need for up-to-date information on patients, medical treatments, pharmaceutical products, etc. In light of the privacy-sensitive nature of medical information, the design of information-sharing mechanisms calls for a systematic and comprehensive digital data architecture, which was sketched out in the present study. The various steps and the lessons from a proof-of-concept experiment based on the PharmaLedger project are described in this paper.

The medical–pharmaceutical sector is one of the most prominent and advanced sectors faced with strict privacy and confidentiality requirements; hence, it is a promising sector for a proof-of-concept design of digital data access technology. In many cases, the spatial action radius of patients and their treatment is limited to the urban or regional scale, so spatial platforms (e.g., in the form of platform cities) provide a natural focus for an advanced and digitally driven data exchange architecture.

OpenDSU is a technology that supports the future development of sharing securely private and confidential data. Given that OpenDSU relies on the concept of signed codes and signed data housed within data-sharing units (DSUs), it appears conceivable that the architecture of OpenDSU will facilitate the future incorporation of additional privacy methodologies.

OpenDSU was validated and adopted in our paper for various business use cases in the pharma ecosystem and is easily scalable to different industries. The spectrum of use cases selected for the PharmaLedger project proved the general applicability of OpenDSU technology in different industries and scenarios.

Individual solutions for different business use case implementations are relatively easy to implement, given the actual development of data libraries with new features regarding confidentiality methods. These methods, supported by the OpenDSU architecture, allow for the construction of new endeavours for confidentiality and privacy to create the benefits needed for specific application environments.

Additionally, it is worth noting that, in enterprise settings, there are instances where the need for transparent auditability and the ability to censor and regulate an organisation's infrastructure may result in the utilisation of less stringent confidentiality measures. One of the major insights acquired from the PharmaLedger project is that, when assessing matters of confidentiality, it is crucial to maintain a balanced perspective, and all conflicting aspects should be considered. The test experiments in the PharmaLedger project proved that, based on the particularities of the selected use case, OpenDSU might support different special methods to address data confidentiality issues.

Platform organisations (including smart cities) may become the foci of advanced digital technology applications (as was demonstrated in our medical–pharmaceutical

study), but they require a careful and actor-oriented consensual architecture, not only from a data–technology perspective, but also from an institutional user perspective.

Author Contributions: Conceptualization, A.B. and P.N.; methodology, K.K.; software, A.G.T.; validation, A.B., K.K. and P.N.; formal analysis, A.B.; investigation, A.G.T.; resources, A.B.; data curation, K.K.; writing—original draft preparation, A.B.; writing—review and editing, A.G.T.; visualization, K.K.; supervision, P.N.; project administration, A.B.; funding acquisition, P.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data supporting reported results can be found in the deliverables of PharmaLedger project. Part of the results is confidential to the members of the Pharmaledger consortium.

Acknowledgments: Ana Balan and Andi Gabriel Tan would like to thank the partners from the PharmaLedger project consortium and from the PharmaLedger Association (https://pharmaledger.org/ (accessed on 1 June 2022)), a non-profit organisation which continues and moves further the work started during the PharmaLedger project with the aim to support collaborative innovation in a healthcare digital trust ecosystem (DTE). Peter Nijkamp and Karima Kourtit acknowledge the grant from the Romanian Ministry of Research, Innovation and Digitisation, CNCS—UEFISCDI, project number PN-III-P4-PCCE-2021-1878, within PNCDI III, project—Institutions, Digitalisation and Regional Development in the EU.

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

References

1. ESPON. *The Territorial and Urban Dimensions of the Digital Transition of Public Services*; ESPON: Luxembourg, 2020.
2. Savastano, M.; Suciu, M.-C.; Gorelova, I.; Stativă, G.-A. How smart is mobility in smart cities? An analysis of citizens' value perceptions through ICT applications. *Cities* **2023**, *132*, 104071. [CrossRef]
3. Peppard, J.; Ward, J. *The Strategic Management of Information Systems*; John Wiley: New York, NY, USA, 2016.
4. Ladley, J. *Data Governance*; Elsevier: Amsterdam, The Netherlands, 2012.
5. Berson, A.; Dubov, L. *Master Data Management and Data Governance*; McGraw Hill: New York, NY, USA, 2011.
6. Bhansali, N. (Ed.) *Data Governance*; CRC Press: Boca Raton, FL, USA, 2014.
7. Cuppini, N.; Frapporti, M.; Pirone, M. When cities meet platforms: Towards a trans-urban approach. *Digit. Geogr. Soc.* **2022**, *3*, 100042. [CrossRef]
8. Ferber, J. *Multi-Agent Systems*; Addison Wesley: Boston, MA, USA, 1999.
9. Chamoso, P.; González-Briones, A.; Rodríguez, S.; Corchado, J.M. Tendencies of Technologies and Platforms in Smart Cities: A State-of-the-art Review. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 3086854. [CrossRef]
10. Repette, P.; Sabatini-Marques, J.; Yigitcanlar, T.; Sell, D.; Costa, E. The Evolution of City-as-a-Platform: Smart Urban Development Governance with Collective Knowledge-Based Platform Urbanism. *Land* **2021**, *10*, 33. [CrossRef]
11. Blok, A.; Courmont, A.; Hoyng, R.; Marquet, C.; Minor, K.; Nold, C.; Young, M. Data Platforms and Cities. *TECNOSCIENZA Ital. J. Sci. Technol. Stud.* **2018**, *8*, 175–220.
12. Oztemel, E.; Gursev, S. Literature Review of Industry 4.0 and Related Technologies. *J. Intell. Manuf.* **2020**, *31*, 127–182. [CrossRef]
13. Dalenogare, L.S.; Benitez, G.B.; Ayala, N.F.; Frank, A.G. The Expected Contribution of Industry 4.0 Technologies for Industrial Performance. *Int. J. Prod. Econ.* **2018**, *204*, 383–394. [CrossRef]
14. Ghobakhloo, M.; Fathi, M.; Iranmanesh, M.; Maroufkhani, P.; Morales, M.E. Industry 4.0 ten years on: A bibliometric and systematic review of concepts, sustainability value drivers, and success determinants. *J. Clean. Prod.* **2021**, *302*, 127052. [CrossRef]
15. Bernholz, L.; Landemore, H.; Reich, R. (Eds.) *Digital Technology and Democratic Theory*; University of Chicago Press: Chicago, IL, USA, 2021.
16. European Commission. The Digital Economy and Society Index (DESI). 2023. Available online: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed on 1 June 2023).
17. Couture, S.; Toupin, S. What does the notion of "sovereignty" mean when referring to the digital? *New Media Soc.* **2019**, *21*, 2305–2322. [CrossRef]
18. Chander, A.; Le, U.P. Data Nationalism. *Emory Law J.* **2015**, *64*, 677–739.
19. Hill, J.F. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U. *S. Policymakers and Industry Leaders. Lawfare Res. Pap. Ser.* **2014**, *2*, 1–41.
20. Panday, J.; Malcolm, J. The Political Economy of Data Localization. *Partecip. E Confl.* **2018**, *11*, 511–527. [CrossRef]
21. Selby, J. Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? *Int. J. Law Inf. Technol.* **2017**, *25*, 213–232. [CrossRef]
22. European Commission. *Trends in Electronic Identification: An Overview, Value Proposition of eIDAS eID, CEF eID SMO, Version 1.1*; European Commission: Brussels, Belgium, 2023; ISBN 978-92-861-5541-3 (PDF/EN). [CrossRef]

23. Balan, A.; Rata, A.; Alboaie, S.; Kourtit, K.; Nijkamp, P. Sustainability, Smart Digital Cities and Decentralized Brands. In *Planning for Liveable Cities*; Girard, L.F., Nocca, F., Kourtit, K., Nijkamp, P., Eds.; Franco Angeli: Milan, Italy, 2023; *in press*.
24. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Mashat, A.; Kumar, A.; Kumar, M. Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. *Mob. Inf. Syst.* **2022**, *2022*, 8930472. [CrossRef]
25. Stokkink, Q.; Pouwelse, J. Deployment of a Blockchain-Based Self-Sovereign Identity. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1336–1342.
26. European Commission: Brussels, Belgium. 2018. Available online: https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/78549570/Trends%20report%20on%20electronic%20identification_for%20publication_v.1.1.pdf?version=1&modificationDate=1551198712785&api=v2 (accessed on 1 June 2023).
27. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A Fistful of Bitcoins: Characterizing Payments among Men with No Names. In Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), Barcelona, Spain, 23–25 October 2013.
28. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
29. Chauhan, A.; Malviya, O.P.; Verma, M.; Mor, T.S. Blockchain and Scalability. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 122–128. [CrossRef]
30. Taş, R.; Tanrıöver, Ö. Building A Decentralized Application on the Ethereum Blockchain. In Proceedings of the 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 11–13 October 2019; pp. 1–4. [CrossRef]
31. Ethereum. Ethereum Whitepaper. 2020. Available online: https://github.com/ethereum/wiki/wiki/White-Paper#applications (accessed on 1 March 2020).
32. Alboaie, S.; Ursache, N.-C.; Alboaie, L. Self-Sovereign Applications: Return control of data back to people. *Procedia Comput. Sci.* **2020**, *176*, 1531–1539. [CrossRef]
33. Pihl, R. Top Benefits of Decentralized Applications (dApps). Retrieved 22 December 2021 from Toshi Times. 2018. Available online: https://toshitimes.com/top-benefits-ofdecentralized-applications-dapps/ (accessed on 1 June 2023).
34. Ethereum. Introduction to Dapps. Available online: https://ethereum.org/en/developers/docs/dapps/ (accessed on 31 May 2023).
35. Atzei, N.; Bartoletti, M.; Cimoli, T. A Survey of Attacks on Ethereum Smart Contracts (sok). In *International Conference on Principles of Security and Trust*; Springer: Berlin, Heidelberg, 2017; pp. 164–186.
36. Alboaie, S.; Cuomo, M.; Ursache, C.N.; Sava, D.; Gheorghiu, A.; Shah, A.; Alboaie, L. OpenDSU Bluepaper (Draft 2.0). 2020. Available online: https://opendsu.com/?home (accessed on 1 June 2022).
37. Coombs, R.; Saviotti, P.; Walsh, V. *Economics and Technological Change*; Macmillan: London, UK, 1987.
38. Maple, C.; Epiphaniou, G.; Gurukumar, N.K. Facets of Trustworthiness in Digital Identity Systems: The Alan Turing Institute—Technical Briefing: London, UK. 2021. pp. 4–9. Available online: https://www.turing.ac.uk/sites/default/files/2021-05/technical_briefing-facets_of_trustworthiness_in_digital_identity_systems.pdf (accessed on 1 June 2023).
39. Cameron, K. The Laws of Identity. *Microsoft Corp* **2005**, *12*, 8–11.
40. Perrin, A. Half of Americans Have Decided not to Use a Product or Service Because of Privacy Concerns. *Pew Res. Cent.* **2020**. Available online: https://www.pewresearch.org/short-reads/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/ (accessed on 1 June 2023).
41. Cusumano, M.A.; Gawer, A. The Elements of Platform Leadership. *MIT Sloan Manag. Rev.* **2002**, *43*, 51. [CrossRef]
42. Valdez-de-Leon, O. Key Elements and Enablers for Developing a Digital Ecosystem for the IoT. Pipeline 2018. Available online: https://pipelinepub.com/network-transformation/iot_ecosystems (accessed on 1 June 2023).
43. Van Alstyne, M. The Opportunity and Challenge of Platforms. In *Platforms and Ecosystems: Enabling the Digital Economy, Briefing Paper, World Economic Forum*; Jacobides, M.G., Sundararajan, A., Van Alstyne, M., Eds.; 2019. Available online: http://www3.weforum.org/docs/WEF_Digital_Platforms_and_Ecosystems_2019.pdf (accessed on 1 June 2023).
44. Van Alstyne, M.W.; Parker, G.G.; Choudary, S.P. Pipelines, Platforms, and the New Rules of Strategy. *Harv. Bus. Rev.* **2016**, *94*, 54–62.
45. Kodali, S.; Swerdlow, F.; Wolken, S. Digitally Impacted Retail Sales. In 2018: Still Only Half Of Retail, Highlights from the Forrester Data: Digital-Influenced Retail Sales Forecast, 2017 To 2022 (US). 2018. Available online: forrester.com/report/Digitally-Impacted-Retail-Sales-In-2018-Still-Only-Half-Of-Retail/RES122907 (accessed on 1 June 2023).
46. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the Frontier Power*; Ingram Publisher Services: La Vergne, TN, USA, 2019.
47. Schroll, R.; Füller, J. The Value of Community-Brands. *Available SSRN 1452622* **2009**.
48. Pohle, J.; Thiel, T. Digital Sovereignty. *Internet Policy Rev.* **2020**, 9. [CrossRef]
49. PharmaLedger. 2020. Available online: https://pharmaledger.eu/about-us/members/ (accessed on 1 June 2023).

50. Glick, T.B.; Figliozzi, M.A.; Unnikrishnan, A. Case Study of Drone Delivery Reliability for Time-Sensitive Medical Supplies With Stochastic Demand and Meteorological Conditions. *Transp. Res. Rec. J. Transp. Res. Board* **2021**, *2676*, 242–255. [CrossRef]
51. Gallacher, D. Drones to manage the urban environment: Risks, rewards, alternatives. *J. Unmanned Veh. Syst.* **2016**, *4*, 115–124. Available online: https://www.researchgate.net/publication/292995153_Drones_to_manage_the_urban_environment_Risks_rewards_alternatives (accessed on 1 June 2023). [CrossRef]
52. Comtet, H.E.; Johannessen, K.-A. A Socio-Analytical Approach to the Integration of Drones into Health Care Systems. *Information* **2022**, *13*, 62. [CrossRef]
53. Azuma, R.T. A Survey of Augmented Reality. *Presence Teleoper. Virtual Environ.* **1997**, *6*, 355–385. [CrossRef]
54. Alzahrani, N.M.; Alfouzan, F.A. Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review. *Sensors* **2022**, *22*, 2792. [CrossRef] [PubMed]
55. Milosavljević, A.; Rančić, D.; Dimitrijević, A.; Predić, B.; Mihajlović, V. Integration of GIS and video surveillance. *Int. J. Geogr. Inf. Sci.* **2016**, *30*, 2089–2107. [CrossRef]
56. Moguel, E.; Preciado, M.Á.; Preciado, J.C. A Smart Parking Campus: An Example of Integrating Different Parking Sensing Solutions into a Single Scalable System. *Smart Cities* **2014**, *98*, 29–30.
57. Díaz, M.; Martín, C.; Rubio, C. State-of-the-art, Challenges, and Open Issues in the Integration of Internet of Things and Cloud Computing. *J. Netw. Comput. Appl.* **2016**, *67*, 99–117. [CrossRef]
58. Achar, S. Cloud Computing Forensics. *Int. J. Comput. Eng. Technol.* **2022**, *13*, 1–10.
59. Zhu, H.; Shen, L.; Ren, Y. How can smart city shape a happier life? *The mechanism for developing a Happiness Driven Smart City. Sustain. Cities Soc.* **2022**, 80. [CrossRef]
60. Al Sharif, R.; Pokharel, S. Smart City Dimensions and Associated Risks: Review of literature. *Sustain. Cities Soc.* **2021**, *77*, 103542. [CrossRef]
61. Caprotti, F.; Chang, I.C.C.; Joss, S. Beyond the Smart City: A Typology of Platform Urbanism. *Urban Transform.* **2022**, *4*, 4. [CrossRef] [PubMed]
62. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
63. Somayya, M.; Ramaswamy, R. Amsterdam Smart City (ASC): Fishing Village to Sustainable City. *WIT Trans. Ecol. Environ.* **2016**, *204*, 831–842. [CrossRef]
64. Toli, A.M.; Murtagh, N. The Concept of Sustainability in Smart City Definitions. *Front. Built. Environ.* **2020**, *6*, 77. [CrossRef]
65. Ramirez Lopez, L.J.; Castro, A.I.G. Sustainability and Resilience in Smart City Planning: A Review. *Sustainability* **2021**, *13*, 181. [CrossRef]
66. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
67. Singh, T.; Solanki, A.; Sharma, S.K.; Nayyar, A.; Paul, A. A Decade Review on Smart Cities: Paradigms, Challenges and Opportunities. *IEEE Access* **2022**, *10*, 68319–68364. [CrossRef]
68. King, W. The 'Healthcare Internet of Things'. *Pharm. Exec.* **2017**, *37*, 34–35.
69. Dash, S.; Shakyawar, S.K.; Sharma, M.; Kaushik, S. Big data in healthcare: Management, analysis and future prospects. *J. Big Data* **2019**, *6*, 54. [CrossRef]
70. Topol, E. *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*; Basic Books: New York, NY, USA, 2019; p. 341.
71. UK Government, Department of Health and Social Care. Code of Practice for Digital and Data- driven Health Technologies. 2021. Available online: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (accessed on 1 June 2023).
72. Beard, L.; Schein, R.; Morra, D.; Wilson, K.; Keelan, J. The Challenges in Making Electronic Health Records Accessible to Patients. *J. Am. Med. Inf. Assoc.* **2012**, *19*, 116–120. [CrossRef]
73. Smith, R.D.; Malley, J.D.; Schechter, A.N. Quantitative analysis of globin gene induction in single human erythroleukemic cells. *Nucleic Acids Res.* **2000**, *28*, 4998–5004. [CrossRef]
74. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2020**, *22*, 177–183, ISSN 1110-8665. Available online: https://www.sciencedirect.com/science/article/pii/S1110866520301365 (accessed on 1 June 2023). [CrossRef]
75. Tan, K.-L.; Chi, C.-H.; Lam, K.-Y. Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization. Computer Science. Cryptography and Security (cs.CR); Distributed, Parallel, and Cluster Computing (cs.DC); Software Engineering (cs.SE). *arXiv* **2022**, arXiv:2202.10069. [CrossRef]
76. Dwork, C.; Kenthapadi, K.; McSherry, F.; Mironov, I.; Naor, M. Our Data, Ourselves: Privacy via Distributed Noise Generation. In *Advances in Cryptology-EUROCRYPT 2006*; Audenay, S., Ed.; Lecture Notes in Computer Science, 4004; Springer: Berlin/Heidelberg, Germany, 2006.
77. Shi, E.; Chan, H.T.H.; Rieffel, E.; Chow, R.; Song, D. Privacy-preserving Aggregation of Time-series Data. In *Annual Network & Distributed System Security Symposium (NDSS)*; Internet Society: Reston, VA, USA, 2011.
78. Rastogi, V.; Nath, S. Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption. In Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data, Indianapolis, IN, USA, 6–10 June 2010. [CrossRef]

79. Avellaneda, O.; Bachmann, A.; Barbir, A.; Brenan, J.; Dingle, P.; Duffy, K.H.; Maler, E.; Reed, D.; Sporny, M. Decentralized Identity: Where Did It Come From and Where Is It Going? *IEEE Commun. Stand. Mag.* **2019**, *3*, 10–13. [CrossRef]
80. Allen, C. *The Path to Self-Sovereign Identity*; Coin Desk: New York, NY, USA, 2016. Available online: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed on 1 June 2023).
81. Romero Ugarte, J.L. Distributed Ledger Technology (DLT): Introduction. *Banco Espana* **2018**, *19*, 18.
82. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model 1.0 Recommendation. 2019. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 1 June 2023).
83. Barclay, I.; Radha, S.; Preece, A.; Taylor, I.; Nabrzyski, J. Certifying Provenance of Scientific Datasets with Self-sovereign Identity and Verifiable Credentials. In Proceedings of the 12th International Workshop on Science Gateways (IWSG), Online, 10–12 June 2020.
84. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight Blockchain for Healthcare. *IEEE Access* **2019**, *7*, 149935–149951. [CrossRef]
85. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [CrossRef]
86. Ekblaw, A.C. MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2017.
87. Da Fonseca Ribeiro, M.I.; Vasconcelos, A. MedBlock: Using Blockchain in Healthcare Application based on Blockchain and Smart Contracts. In Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020), Prague, Czech Republic, 5–7 May 2020; Volume 1, pp. 156–164. [CrossRef]
88. PharmaLedger. D3.9 Reference Implementation of Advanced Confidentiality Methods—Final Report. 2022. Available online: https://pharmaledger.eu/resources-publications/horizon-2020-pharmaledger-grant-agreement-documents/ (accessed on 1 June 2023).
89. Alboaie, S.; Mastahac, B. Anchoring. 2021. Available online: https://opendsu.com/?openDSU/rfc004.html (accessed on 1 June 2023).
90. Axiologic; PharmaLedger. OpenDSU Concepts: Anchoring (RFC-005). 2022. Available online: https://opendsu.com/rfc005 (accessed on 1 June 2023).
91. Axiologic; PrivateSKY și PharmaLedger. OpenDSU APIHub APIs Anchoring (RFC-121). 2022. Available online: https://opendsu.com/rfc121 (accessed on 9 June 2023).
92. Axiologic; PrivateSky și PharmaLedger. Anchoring (RFC-069). 2022. Available online: https://opendsu.com/rfc069 (accessed on 1 June 2023).