applied sciences

MDPI

Article

Possible Blockchain Solutions According to a Smart City Digitalization Strategy

Ivica Lukić *, Kruno Miličević, Mirko Köhler and Davor Vinko

Faculty of Electrical Engineering, Computer Science and IT Osijek, J.J. Strossmayer University of Osijek, 31000 Osijek, Croatia; kruno.milicevic@ferit.hr (K.M.); mirko.kohler@ferit.hr (M.K.); davor.vinko@ferit.hr (D.V.)
* Correspondence: ivica.lukic@ferit.hr; Tel.: +385-91-224-6108

Abstract: With advances in Information and Communication Technologies (ICT) in convergence with blockchain technology, cities have been given the opportunity to improve their services, efficiently use resources, and, thus, become Smart Cities. The main properties of blockchain technology like decentralization, immutability, transparency, consensus, and robustness are qualities needed for Smart City. In this paper, we propose a digitalization strategy for the City of Osijek. Smart City digitalization strategy aims to solve problems of emerging urbanization, improve administration by reducing energy and water consumption, carbon emissions, pollution, and city waste management. To develop an information system based on blockchain technology, the administration structure and the current state of information systems are analyzed, and new solutions are presented.

Keywords: blockchain technology; digitalization; IoT; Smart City; smart contracts

check for updates

Citation: Lukić, I.; Miličević, K.; Köhler, M.; Vinko, D. Possible Blockchain Solutions According to a Smart City Digitalization Strategy. *Appl. Sci.* **2022**, *12*, 5552. https://doi.org/10.3390/app12115552

Academic Editor: Gianluca Lax

Received: 29 April 2022
Accepted: 29 May 2022
Published: 30 May 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Today cities tend to become Smart Cities and improve life quality in every city area. The characteristics of a Smart City are innovative public services such as Smart Governance [1], Smart Health, Smart Economy, Smart Mobility, Smart Environment, Smart People, and Smart Living [2]. Smart Mobility implies that Information and Communication Technology (ICT) is used to support and integrate transport and logistics systems. It requires that the users have relevant and real-time public information about the public services (such as emergency services, public transportation, water supply network, waste management, etc.) and vice versa to improve commuting/collection efficiency, save time, and reduce costs and CO_2 emissions. Smart City strategy aims to solve the problems of emerging urbanization and rising population growth by reducing energy and water consumption, carbon emissions, pollution, traffic jam, and city waste. IEEE has already developed standards for different components of Smart Cities like smart grids, IoT, Healthcare, and Intelligent Transportation Systems (ITS). ISO 37120 standard defines 100 performance indicators for education, economy, education, energy, and environment. City governance should use these indicators to grade their services and compare them to other cities.

A Smart City produces an immense amount of data at a particular time about all public services. Up to date information is crucial to improve public services and provide feedback to its users. A Smart City should ensure an interactive information system to create different participation methods in public life and call citizens to become active users. The active users should be able to provide their real-time data to the Smart City information system and be involved in decision making [3]. To acquire up-to-date information about the public services, it is important to have a good information system for collection and to store relevant data, such as traffic data, air quality, water resources, high-density populated areas, areas inaccessible to certain infrastructure, status of city infrastructure, etc.

In the digitalization strategy for city governance, implementing IoT sensors and devices is an excellent way to collect data and improve public services management as

shown in Figure 1. IoT devices can be integrated into the information system to increase city governance transparency, include citizens in political decisions and city problems, improve healthcare, the well-being of the city, and other aspects of human life [4]. To achieve these goals, trust in city governance and transparency is mandatory; thus, we propose blockchain technology to store and maintain public service data. Blockchain technology has desired properties for this task, such as decentralization, reliability, transparency, and security. There are numerous blockchain solutions that are helpful for different Smart City tasks, such as authentication and trust management [5], healthcare [6,7], waste management [8], and IoT sensors [9]. However, existing literature does not offer a comprehensive overview of the whole city system; it just showcases particular solutions (Table 1).

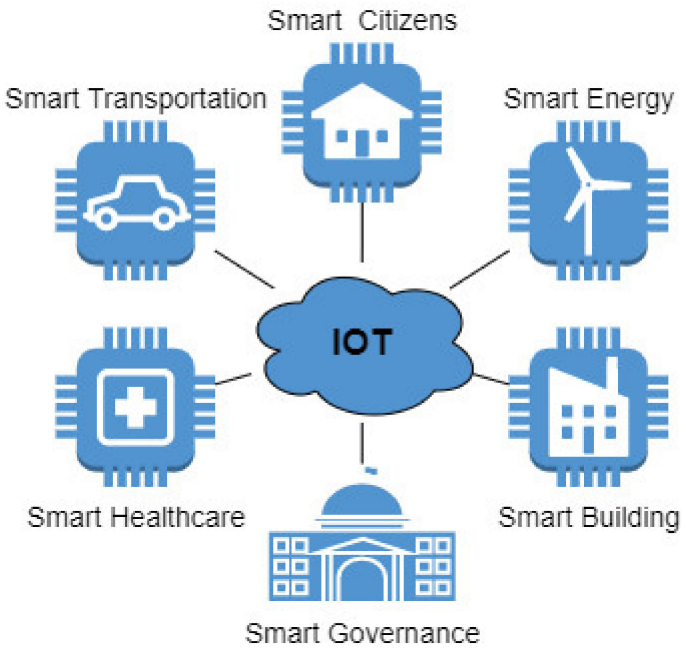

Figure 1. Smart City digitalization strategy goals.

Table 1. Literature overview for blockchain as a Smart City solution.

Literature	Blockchain as a Smart City Solution
[5]	Authentication and trust management
[6,7]	Healthcare
[8]	Waste management
[9]	IoT sensors
[10–14]	Drone applications for Smart City surveillance
[14,15]	Smart contracts
[16]	Online insurance
[17]	Legal and technical adoption issues for Smart City
[18,19]	Blockchain oracles problem
[20–23]	Blockchain consensus type overview
[24–31]	Security of data sent by oracles
[32–35]	Interplanetary File System for data storing
[36–38]	Smart City interoperability
[39–42]	Data consolidation and GDPR

Thus, the contribution of this paper is a presentation of the whole topic of the digital transformation of a city and the peculiarities of possible application of blockchain in each instance. In doing so, it was beneficial to collaborate with the City of Osijek, with a goal to define the digitalization strategy document as the basis for later implementation.

2. Blockchain in Smart City Solutions

Blockchain technology has needed properties and solutions for the most technical challenges of digitalization strategy and transformation of a Smart City. Thereby, it is also possible to combine technologies, like using drones for remote regions where IoT devices face network scarcity and potential cyber threats [10], or in case of needed supervision [11]. Drones can be used in all aspects of Smart City safety like traffic monitoring, emergency disaster monitoring, safety and violation monitoring [12,13].

One of the many solutions are blockchain smart contracts, which were first introduced in [14] and further improved and popularized through Ethereum and similar blockchain technologies [15]. Smart contracts are distributed computer programs on a blockchain network that have various terms and conditions, and actions which should be made by a smart contract. Smart contracts are automatically executed without human intervention when the defined terms and conditions are fulfilled. This functionality is useful for many Smart City functions where an automated and active system is needed [16]. However, there are possible legal problems in the case of a dispute because of legal and technical adoption issues [17]. Smart contracts could be used for automated decision making in the digitalization strategy, such as automated warning systems, automated reports, automated agreement execution, payment, etc.

Using blockchain technology, city governance can be decentralized and distributed among all parties involved in a decision about Smart city sociodemographic problems. Problems like water supply management, pollution, social inequalities, healthcare services, transport, education, and safety need new and better solutions. Blockchain is a platform that can help solve these problems by involving citizens in participation, democracy, and transparency. Smart City should have more services than cities before, where the main services were trash collection, streetlights, and road repair. It was a vertical government, but today cities have horizontal responsibilities:

- Information sharing is needed because citizens are connected using mobile devices and want new information.
- Constant updates with new data which should be verified.
- Intermediates between citizens and governance, which add complexity to city governance.

For example, blockchain has its advantages when it is necessary to decentralize the distribution of the trust, or when you want to avoid a trusted third party in the verification of agreements (which have elements of a contract) between two or more parties through the so-called smart contracts. Since the city itself, through its function, legally often has the role of a third-party trust, the blockchain cannot be widely used for all data services. However, the application could be considered when an additional level of trust is sought, i.e., when the city voluntarily (if legally possible) renounces the role of the third party of trust, e.g., in the case of involving citizens in decision-making through various voting processes and decision making as showed for waste management, healthcare, and resource sharing applications.

The true value of blockchain is the possibility to share only the information that is important to citizens and they wish to know, while everything else can be encrypted and inaccessible by unauthorized users. Information is stored in blockchain, and cryptography is used to prevent manipulation, modification of information, and privacy violations. In this paper, the digitalization strategy for the City of Osijek is presented to transform it into a Smart City, improving the quality of life for all citizens.

2.1. Data Collection Using IoT Sensors as Oracles

The blockchain ecosystem can be provided with data in different ways, and we must trust in data provided by the blockchain network. To ensure trust, we need oracles, which are trustable entities that collect information from the external world. The oracles are IoT devices connected to the blockchain on one side and take on several key functions [18]:

- Monitoring the blockchain network to check for incoming user or smart contract requests for measured data.
- Performing some type of computation before sending data to the blockchain network.
- Verifying and sending measured or calculated data to the blockchain to be processed by the smart contracts or directly written in the blockchain network.

According to [19], data provided to the blockchain by oracles are:

- Web content.
- Sensor data.

Both data sources are significant for digitalization strategy. Web content data includes data about city companies, city employees, documents, certificates, agreements, citizens, etc. Other sources are data collected by various sensors across the entire city like air quality sensors, cameras, traffic monitoring, smart home sensors inside buildings, user wearable devices, etc. Oracles can be divided into different types depending on their role [20]:

- Software oracles—collect web content for the blockchain network.
- Hardware oracles—physical devices which provide sensor data.
- Inbound oracles—collect data from the external world as inputs for smart contracts.
- Outbound oracles—send information from blockchain network to the outside world.
- Consensus-based oracles—data provided to blockchain network are consensus from multiple sensors.

2.2. Validation of the Data That Oracles Provide to Blockchain-Based Applications

The digitalization strategy should include blockchain in different city procedures because the blockchain for data verification does not need intermediaries or central authority [21]. Blockchain network is based on a consensus among the blockchain users, and some parts of city governance can benefit from the consensus among citizens. The goal of Bitcoin as the first blockchain network was to enable online payments without financial institutions so a city can use it for some service payments, taxes, etc. The most used consensus types are Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Authority (PoA) [22,23]. There are many alternative consensus approaches, and all have the same goal to avoid frauds and make it unprofitable. In the PoW consensus, verifiers invest high amounts of computing power, and it is not profitable to invest it for false verification, while the PoS verifiers invest their stake and risk losing them if they verify false data. The PoA is a consensus where some actors in the blockchain network can validate transactions and stake their identity, so if they undertake some malicious activities, they will lose their reputation and active role in future transaction validation.

Due to the Smart City hierarchical structure, PoA is the best mechanism for transaction validation. In this case, the blockchain loses distributed consensus-based transaction validation, but it keeps other specific properties, like distributed and immutable data storage. Thus, a consensus type should be made regarding specific applications in a Smart City; considering different requirements, the Proof-of-Reputation also could be an alternative [23].

2.3. Security of Data Sent by Oracles

As one of the ultimate goals, a mobile application (Android and iOS) was identified to unite all individual services and processes for city companies, institutions, and city users. To ensure the security of transfer, data from oracles should be encrypted. The blockchain network infrastructure can provide all that is necessary for data security [24,25]:

- Integrity, authenticity, and non-repudiation of legally relevant information (WELMEC Software Guide 7.2, Measuring Instruments Directive 2014/32/EU, 2020).
- The blockchain stores and attests public keys from IoT devices.
- The solution does not depend on a trusted third party.

Additionally, the oracles should send data using secure IoT communication protocols to ensure anti-tampering protection [26–28]. To ensure the true values of the measured data

it is important to prevent tampering, which can happen at the software level, hardware level [29,30], and tampering sensor input level [31].

2.4. The Interplanetary File System for Data Storing

The Interplanetary File System (IPFS) is a decentralized file system for building the next generation of the Internet. Some call it a hard drive for blockchain and Web3, although its power extends much further. IPFS stores data, applications and websites and provides access to them through a decentralized P2P infrastructure. IPFS works on the principle of content addressing in which it uses cryptographic algorithms called "fingerprint algorithm", to generate a unique CID (Content ID), i.e., content identity. IPFS can remove duplicates in its decentralized repository and generate only one fixed CID, which means one fixed document. In this way, we also eliminate any possibility of change or digital impact on the document, because each change will generate a new CID and, therefore, will not match the required. IPFS allows NFT to be generated by uploading a digital copy of a document to a P2P network and saving it forever. Although IPFS is a public blockchain, it can also be applied to privacy-seeking systems and specific participants. Due to its capabilities and technological functionalities, it is ideal for determining the ownership and change of documents in case of credibility of information and taking responsibility. It can be used as a peer-to-peer (P2P) file system in blockchain [32]. The blockchain is not suitable for storing large files since all data should be replicated on many nodes and it leads to price increasing for data storage. The IPFS can be used to store data, and it can be modified to share private data with trusted parties using smart contracts to maintain access [33–35].

The Interplanetary File System is suitable for Smart City applications and data storage, as shown in Figure 2. Official documents of the city governance, formal letters, images, documents of citizens, and data collected from the sensor can be saved in IPFS. In the next step, a file hash is generated, and a smart contract can be called if necessary. The data can be encrypted using various algorithms and saved in the blockchain. Access to data (public, private, etc.) can be determined very easily; data are secured and not in readable format due to the encryption and cannot be changed without consensus because of file hash.

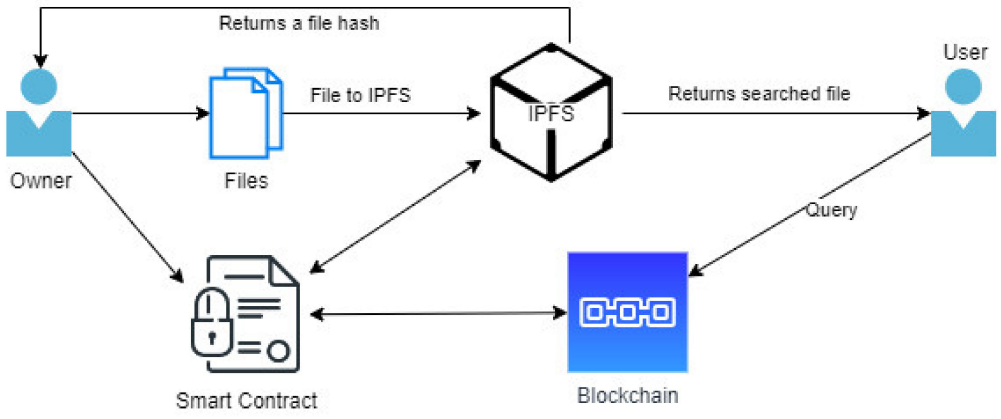

Figure 2. The IPFS for a Smart City.

3. Digitalization Strategy of City Governance

For the development of an information system that will meet all the city administration's needs, it is necessary to have a holistic approach. Namely, partial solutions have often the disadvantage of lacking interoperability [36–38]. Thus, the first goal is to analyze the administration structure and the current state of information systems. In the case of the City of Osijek, the analysis was conducted based on a several meetings with the city administration and data collected for the processes of all City Departments:

- Internal audit of the City of Osijek
- Mayor's office
- City Office

- Administrative Department for Communal Economy, Transport, and Local Self-Government
- Administrative Department of Economy
- Administrative Department for Social Activities
- Administrative Department for European Union Programs
- Administrative Department for Finance and Procurement
- Administrative Department for Social Welfare, Pensioners, and Health
- Administrative Department of Urbanism
- Administrative Department for Property Management and Ownership Relations
- Administrative Department for Construction, Energy Efficiency, and Environmental Protection

Each department submitted the business processes, which involve so-called external stakeholders: citizens, city companies, and other City Departments. After the surveys and meetings, items relevant to the information system development strategy emerged, which will be discussed in more detail in the following chapters. In addition to the business processes of the city administration, business processes were collected for ten city companies and various institutions such as water supply company, waste collection company, etc. About 320 relevant business processes required for city management were recorded. When developing the city digitalization strategy, it is necessary to process all relevant items in detail. After the analysis, Strategy is divided into phases. Each phase is responsible for one part of the Strategy, as will be shown in the next subchapters, which represent the main aspects of the digitalization strategy. All Smart City components should be included in the digitalization strategy, as shown in Figure 3.

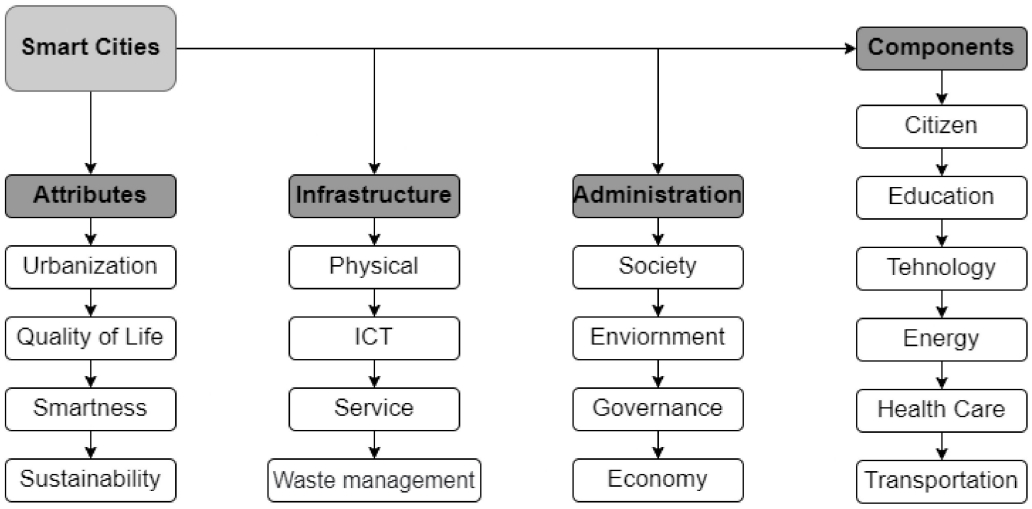

Figure 3. Smart City components included in digitalization strategy.

3.1. Data Consolidation

Consolidation of data is necessary so that all data, whenever possible, are entered only once, through one interface, and written in its original or encrypted form in one place, while other systems will have access to them as needed. It is also necessary to resolve possible unnecessary redundancy and data collisions when consolidating. When this step is properly conducted, there is a possibility to store public data on a blockchain network to ensure data security, transparency, and confidence [39].

Blockchain technology is robust because a single entity does not control it, the network is decentralized, and there is no single point of failure, as shown in Figure 4. Information is distributed across the nodes in the entire network, and failure in one node will not lead to data loss. Data are secured and trusted, while it is almost impossible to change or false verify data. Intruders should have enormous computational power to alter the stored information. If anyone changes the information, it is visible to all participants, transparency

is achieved, and possible tampering is eliminated. All participants in the transaction should have a consensus before the transaction is validated and data stored in the blockchain.

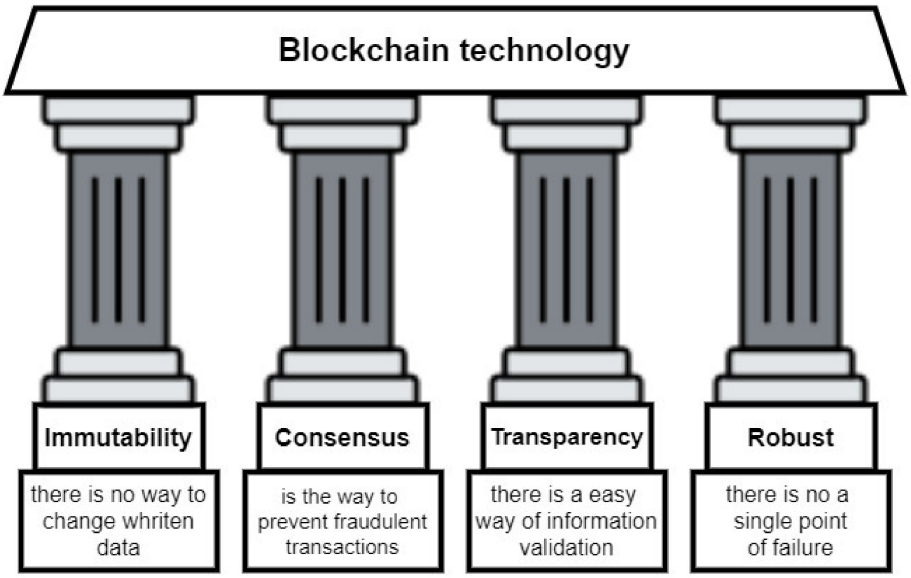

Figure 4. The pillars of blockchain technology.

After the data consolidation process, we divided data into the following separate categories:

- Data on the city system (organizational units, employees, hierarchy).
- Data on users of public services (citizens, associations, companies, crafts, etc.).
- Data on city cases (submitted requests, etc.).
- Sensor data—data obtained by various sensors (mostly IoT), and can be referred to as user data related to the basic public services they receive (e.g., water consumption, waste collection, etc.), to City data related to additional public services, i.e., improvement of existing ones (e.g., smart parking, video surveillance for security purposes, but also additional purposes, etc.), and data related to the quality of life (e.g., air quality, etc.).

We should have in mind and incorporate already existing data:

- Data available in national databases and registers, as will be explained in the next chapters, which can be accessed by appropriate connectors, e.g., through web services or API (Application Programming Interface).
- Data for specific cases depend on business logic, which can be implemented to a greater or lesser extent in software support for individual processes.

3.2. GDPR

Many city governance applications, such as notary service, identity documents, and healthcare require citizens' personal information. Malicious users can use this sensitive information to identify any individual, and, thus, data protection is the main goal and the most important task of any Smart City application. If a malicious user obtains at least 51% of processing power, he can manipulate data stored in the blockchain network. It is necessary to apply the GDPR (General Data Protection Regulation), among other things, when consolidating and merging databases. Blockchain technology is not legalized for some applications in city government affairs, for example, legal documents, licenses, etc. Therefore, using blockchain applications without legalization will raise legal implications, so it is important to ensure new law regulations, as shown in Figure 5.

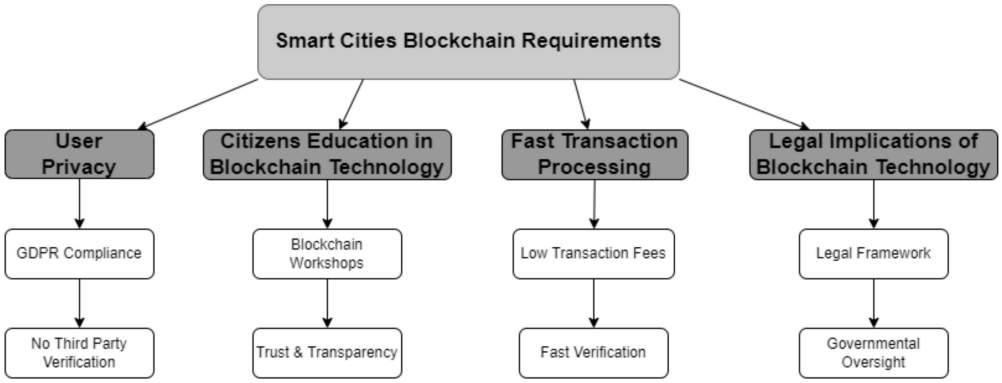

Figure 5. The requirements of blockchain technology.

Smart City platform, which takes GDPR in consideration and data security, is proposed in [40], a platform with a focus on healthcare is presented in [41], and a review of GDPR compliant blockchain systems is presented in [42]. The GDPR requires that the processing of personal data be harmonized with professional regulations governing the field of activity. Although certain processing is not prescribed by law, it may be lawful from the point of view of personal data protection, as processing may be based on contract, official authority of a public body, public interest, vital interest of the individual, legitimate interests, or when the individual has given consent. However, it does not matter which legal basis is used for which processing. Furthermore, the GDPR always places emphasis on transparency, which is achieved by providing layered privacy notices on and off the web. Education is vital; both employees and users have to be educated about their privacy rights and responsibilities because most rights violations occur due to human error. It is also important to take care of the records of processing activities and the data protection officer. Increased attention should be paid to special categories of data, such as data on health, nationality, data on trade union membership, etc. When necessary, a data protection impact assessment should be performed, and information security must be taken into account. Not all employees should be allowed access to all data, confidentiality statements should be signed, and care should be taken of the executors of the processing. The latter are entrusted with specific processing and conclude contracts with them. Individuals are becoming more aware of the right to personal data protection and know that an organization that adheres to personal data protection can be trusted and vice versa.

3.3. Internal Communication

Tailored communication channels, both formal and informal, including the sharing of documents between different parts of the city administration, need to be provided to make mutual cooperation as efficient as possible. Informal communication (inquiries about clarification of individual requests and processes, search and delivery of data that are not necessary for the continuation of the process, etc.) should be strictly distinguished from official communication, which is part of official city procedures (approval of various requests, delivery of data necessary for the continuation of the process, etc.). Official communication should be enabled through DMS (Document management system) software in which the business logic of the process should be embedded or at least through process display BPMN (Business Process Modeling Notation) diagrams to enable users to indicate and track which step a particular document and accompanying communication refers to. For informal communication, it is desirable to take place within the DMS software. Still, it is not necessary, i.e., it is possible through a separate communication software platform (if possible, by connecting the communication to the object defined in the DMS software via a unique case ID). For both types of communication, the systems must be common to the entire city system (administrative departments of the city, city companies and institutions). Special attention should be paid to the simplicity of communication because otherwise (especially for informal communication), employees of the city system will resort to simpler

ways of communication (phone call, e-mail, etc.), which is not optimal in the long run, given the digitalization strategy, data tracking, and security.

The blockchain solution for Smart City is divided into three parts; the first part comprises all city applications such as waste management, healthcare, traffic, and other applications important for city governance, as shown in Figure 6. The second part is network devices (IoT) and communication networks responsible for collecting and data sharing. The final part is the blockchain network for data storage after reaching a consensus among the trusted nodes in the network depending on selected consensus protocols. For each node on the network, smart contracts are defined, and if a node agrees with the rules in smart contract, information is stored in the blockchain [43].

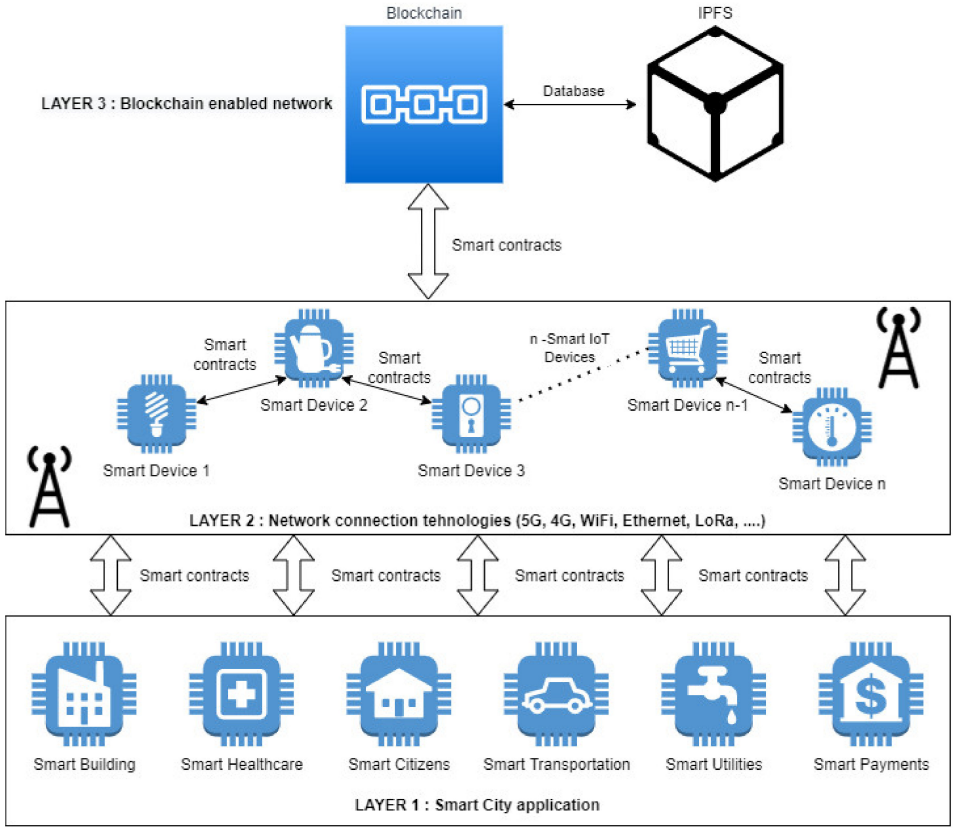

Figure 6. The blockchain solution for Smart City.

The solution has numerous heterogeneous devices that are participants in information exchange. These devices should be oracles to ensure trust in exchanged information. A large number of cryptographic keys should be secured to identify each device properly. Keys can be stored locally, in password-protected storage, offline key storage, or on a third-party service, as shown in Table 2.

Table 2. The key management proposal.

Approach	Description	Pros	Cons
Local storage	Private keys are stored in a local device with password protection, which can be accessed through application-based software	Quick access	Prone to online hackers and installation of malicious malware on local devices
Offline storage	Private keys are secured by storing keys in offline media	Secure from attack	No fast access to keys
Third party storage	Services from cloud-neutral providers	Fast and easy	Trust to third party

3.4. Repetitive Subprocesses

Although the Strategy is oriented to processes that have input and/or output from the outside world (i.e., city companies and institutions and users of public services), much of the process has a significant part of the sub-processes within the city administration. They require the harmonization of these internal sub-processes (e.g., archiving documentation, contract records at the end of the calendar year, procurement procedures, contract writing, delivery, and analysis of materials on working bodies as well as feedback information, etc.) so that all the city administration would take place in the same way, i.e., whenever possible through the same applications or the same modules that different applications will use in their work.

The Event Condition Action (ECA) method belongs to a group of rule-based systems. Therefore, it can be used for dynamic management in blockchain systems, as shown in Figure 7. The ECA model, in combination with the blockchain, fully enables dynamic management. As such, it does not require the implementation of logic and the development of program code for a specific case of use in smart contracts. In an intelligent transportation system to share critical information among all participants, blockchain can be used, and smart contracts mechanism can react to events like road accidents and emergency events [44]. Smart contracts are software units in blockchain systems that execute a certain logic. Managing and changing smart contracts is more complex than traditional systems. In the case of official digital documents (diplomas, contracts), it is not possible to allow systems to be offline due to the constant dynamic change in regulations, legal articles, and laws. That is why we can use the ECA approach for a rule-based engine:

- Event—an event is a content that needs to be checked and harmonized with the rules within the blockchain network. Content always comes from external, centralized, synchronized systems.
- Condition—a condition is a predefined business rule that lives on a blockchain system that is directly related to business rules and uses them to check the content and its compliance.
- Action—action is the last step of checking in which we have defined what, according to a certain situation, must happen or what business process must be started.

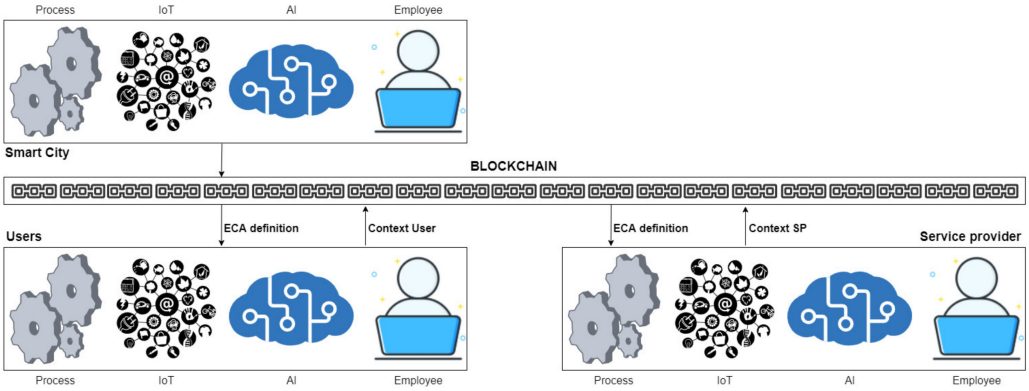

Figure 7. The ECA model and blockchain technology.

The Event Condition Action (ECA) method belongs to a group of rule-based systems. Therefore, it can be used for dynamic management in blockchain systems. The ECA model in combination with the blockchain fully enables dynamic management because, as such, it does not require that all actions should be executed manually. Big data technologies and machine learning can be used to detect the occurrence of different events by analyzing a big collection of data and taking action upon these events [45].

3.5. Existing Applications and Common Users Application

At the meetings with the city administration, it is necessary to analyze in more detail the existing software solutions (DMS, Social Care Software, Water supply software, etc.) as well as individual steps in general. For example, it has been found that DMS does not have built-in business process logic, which, on the one hand, gives great flexibility in process implementation, but on the other hand has a reduced level of process automation. In these cases, RPA (Robotic Process Automation) or RBE (Rules Based Engine) could be an acceptable and cost-effective solution, as stated in the previous chapter.

As one of the ultimate goals, a mobile application (Android and iOS) was identified that would unite all individual services and processes for city companies and institutions and users of city services. Upon completion, all services would be added to the application according to the priorities defined in the Strategy. Therefore, the services must be implemented modularly, following the principles of interoperability. Each data source should be used as much as possible, i.e., with as many different purposes as possible. For example:

- Consolidated data as explained in Section 3.1 should be used for different types of analysis to plan and optimize the effectiveness of city administration decisions.
- Videos from installed public cameras should be used for security surveillance of public spaces, but also for recognizing free parking spaces (so-called smart parking), etc.
- In data processing, one should be careful about the GDPR, as explained in Section 3.2.

3.6. Healthcare Application

The healthcare system consists of hospitals that are under a central authority and are, therefore, subject to a single point of failure [46]. Hospitals do not have enough resources, and citizens demand better service, and here we come to a disparity between the requirements and the available resources. As a solution, decentralized blockchain technology is offered, which enables the improvement of services by offering smart hospitals, vehicles, and urgent responses to customer requests. Decentralized Application (DApp) for transparent, secure, and anonymous transactions in a healthcare system is proposed in [47] and proved that blockchain is the right solution for a decentralized healthcare network. The technology allows doctors to access patient data at remote locations to treat patients on the spot [48]. Below are the steps that need to be taken to introduce blockchain technology into the health system [49] as shown in Figure 8:

- IoT sensors collect patients' health information like sugar, heart rate, respiratory information, blood pressure, body temperature, etc.
- The collected data are used to create a patient's report.
- The doctor analyses the report and recommends the treatment.
- The treatment reports can be shared using a distributed database with other doctors for further analysis.
- The reports should be shared in an encrypted format.
- Patients can easily request their treatment records from the Cloud Service Provider (CSP).
- After successful validation, the encrypted file is sent to the patient.
- The patient decrypts the received file with his private key.

3.7. Intelligent Transportation System Application

Blockchain technology can be used in smart transportation to improve vehicle safety and travel efficiency, reduce travel costs, and ensure secure transport for drivers and their passengers. Blockchain can improve coordination among transportation parties, documents sharing, security, and privacy of the Intelligent Transportation System (ITS) [50]. Blockchain technology improves efficiency, lowers costs, and ensures secured delivery of goods to the end-users [51]. In modern smart cities, electric vehicles are very popular as green transportation systems. These vehicles should be charged in charging stations that are in urban areas with a high-density concentration of electric vehicles. Lightning Network

and Smart Contract (LNSC) are proposed to secure trading between charging stations and electric vehicles [52].

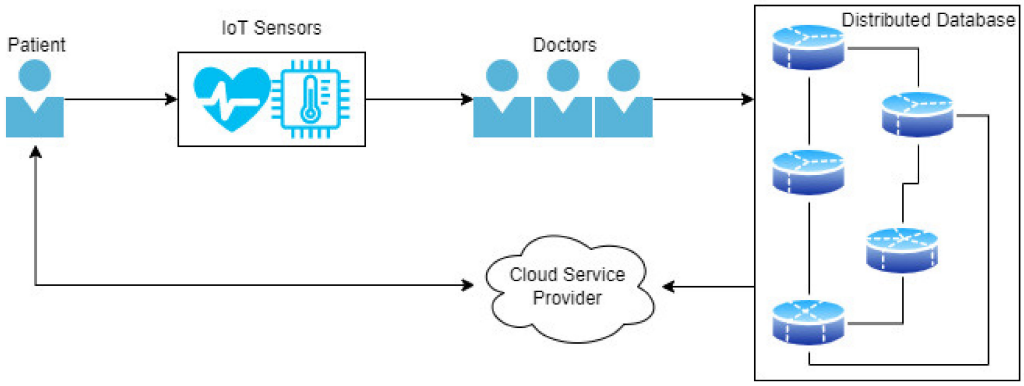

Figure 8. The process of securing patients' treatments in blockchain healthcare network.

3.8. Water Resource Management Application

Another example of the use of blockchain technology is water resource management to improve the quality of urban life [53]. The solution consists of collecting data using IoT sensors, storing data in the cloud and sharing information with users. Citizens can take an active role and participate in decision-making regarding water resource management. The app uses smart contracts, and contract execution depends on decisions made publicly by the community. In this way, access to information and involvement of citizens in making correct and transparent decisions is ensured.

3.9. Waste Management Application

Waste management should be organized to improve human health, protect water systems, reduce air pollution, and ensure the quality of life. However, today's waste management systems are centralized, mostly manual and becomes a single point of failure. Furthermore, waste management history is not traceable, not transparent, and can be manipulated. Thus, it is necessary to involve and explore blockchain technology in managing waste within smart cities [8]. Blockchain waste management can include real-time tracking of waste, efficient human and resources management, document protection, and citizens in decision-making. Different IoT devices (sensors, radio frequency identification, etc.) can be used to monitor and collect city environment information. IoT devices can collect information from every aspect of city activities and are used in waste management models [54]. The authors proposed a design that uses different truck sizes for different waste types and IoT devices for communication among parties involved in waste management. Another approach is the design of smart waste management bins [55], which have sensors for waste weight measurement and the waste level inside the container.

As shown in Figure 9, the waste collection must consider materials suitable for recycling, and they should be disposed of or recycled in waste recycling plants. The smartphone devices contain lithium, gold, cobalt materials which can be reused [56]. Some materials and consumables like smartphones, tires, and accumulators have an expiry date and should be recycled [57]. Today's solutions are centralized and incapable of providing trust, traceability, and active waste operations. The blockchain technology and smart contracts can increase the cooperation and coordination among parties in waste management, increase citizen's trust and make them active parties. It can ensure only authorized users can view the data and enable them to visualize, monitor, and make decisions about waste management. Consumers can return waste after purchasing and using products and make payments from their wallet [58,59]. A smart contract can be used to calculate and transfer fund to users based on returned waste and make them produce less waste and recycle more waste [60].

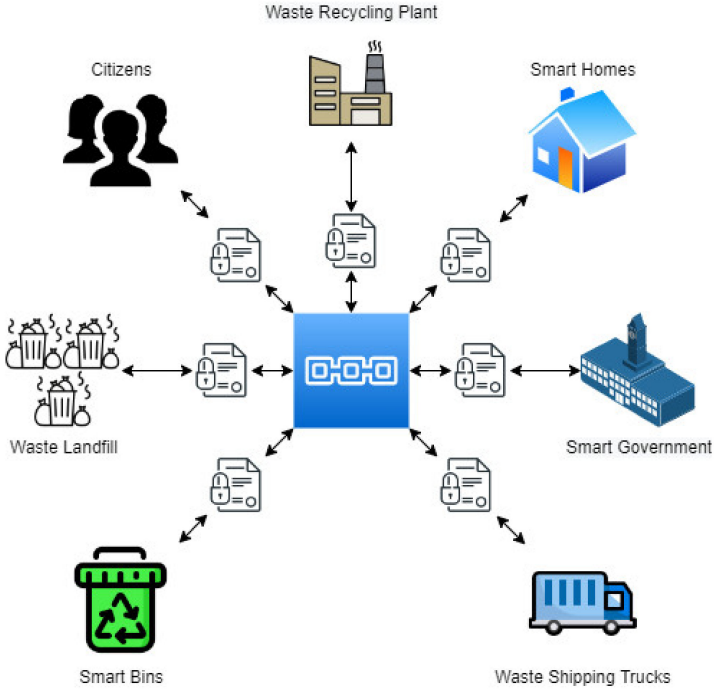

Figure 9. The waste management using blockchain.

3.10. Resource Sharing Application

As resource sharing is becoming more important to increase efficiency, it is necessary to define a software system for this purpose, which would enable potential users to use city resources in a simple and transparent way (usually for one-time short rent), e.g., use of sports halls, conference halls, office space, means of transport (car/bike sharing, electric scooters, etc.). Resource sharing can improve life quality and manage shared resources. The current resource sharing is centralized and, thus, is vulnerable to many threats like theft, lack of spatial data, traceability, etc. Blockchain technology can prevent various risks because it is decentralized and tamper-resistant. Using blockchain smart contracts Smart City resource sharing system can provide all necessary for secure and transparent resource sharing [61]. The blockchain can enable distributed authentication, registration, IoT device management, scalable and secure instantiation of IoT networks, and payment management [62]. Each registered device status can be monitored; data are collected and stored for future decision making about resource sharing, as shown in Figure 10.

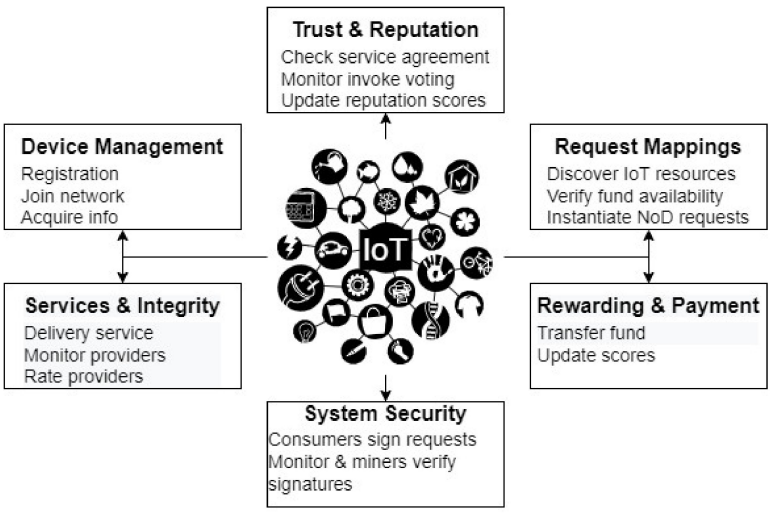

Figure 10. Resource share architecture.

3.11. Geoinformation System

Spatial data are inseparable from most urban processes. Therefore, special attention should be paid to the procurement of integrated GIS (Geographic Information System), which would, as far as possible, include all relevant data for the processes in question, i.e., avoid the procurement of partial solutions. To collect geolocations in Osijek, we created an application for collecting geolocations using parameters such as the name of the city and street number [63]. To visualize collected data, geolocations were plotted, resulting in the contour of the City of Osijek, as shown in Figure 11. These data can show population density in different places around the city and manage city services upon them.

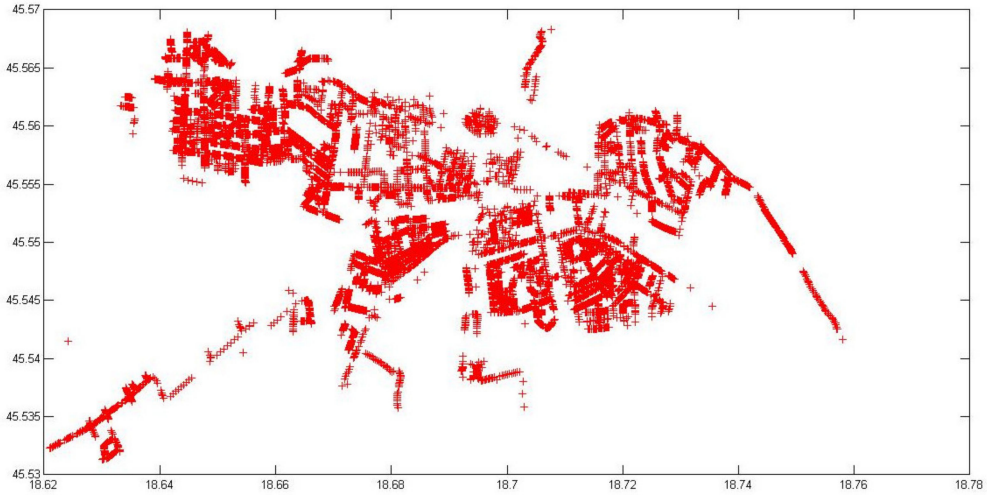

Figure 11. The collected geo-coordinates in the City of Osijek.

Geolocation data can minimize the costs and travelled distance by locating public services in high-density areas to fulfil the tasks efficiently. The tasks are completed efficiently, and predictions can be made using previous data, such as predicting the needs for exceptional situations that can dramatically change the future requirements and share these data with users. Drones can use geolocation data for city regions to identify the location of the supervised area and collected data [11], location of the emergency disaster, traffic jams, and safety violations [12,13]. Different internet platforms and companies like Google, Uber, Amazon, and Airbnb base their services on geolocation. User identity in a Smart City will be online, and geolocation can be used to improve their experience of Smart City applications. It is important to identify the area of services and offer services and products specifically for users' geographical location. For example, Google Maps show the closest shops, restaurants, pharmacies, etc., and services are based on geolocation. Knowing the real-time user and car position in resource sharing applications and transportation applications like Uber is essential. Collected data can be used to identify the area in a Smart City with traffic jams and traffic accidents rate and to improve traffic control. Users have mobile devices which are aware of their location, and if users share their data, it is helpful for Smart City governance to improve the quality of their services. In Figure 11 are shown geo-coordinates in the City of Osijek, which can be provided for any city on the same way. The digitalization strategy for the City of Osijek, which is presented in this paper, can be transformed into any other city. Geolocation can be used for resource sharing like e-bikes in the City of Osijek to locate every bike location and share information with users. Information can be stored in the blockchain to gain traceability, transparency, and trust.

Some smart applications can retrieve relevant information about users and their surroundings to create location-aware city services based on data from IoT devices [64]. Geographical data can be stored in the cloud and used for spatial data purposes, where each data is connected with spatial origin. For example, if some sensors detect smoke, it is easy to locate the fire area from a sensor's spatial data. Spatial data can be used to monitor

older people's data using wearable devices, outdoor sensors, and smart city systems to ensure better healthcare, monitor physical activity, and base interventions on collected data to reduce frailty risks [65].

3.12. Existing Resources on National Level

Existing state databases, registers, services, and applications should be used as much as possible, e.g., NIAS (National Identification and Authentication System), OIB register, register of residence, vehicle register, citizens' master data, records of income and receipts, register of real estate transactions, register of companies and crafts, records of communal infrastructure, Central Register of State Property, e-Tax, e-Permits, e-Newborn, e-Fees, e-Authorizations, e/m-Signature and time stamp, e-Consulting, and various e-services from different ministries departments. Moreover, as much as possible, it is necessary to use available hardware and infrastructure resources available at the state level, such as the SSC (Shared Services Center).

3.13. Regulation on Office Operations and Trends at National Level

Given the legal obligation to apply the National Regulation by the January of the year 2023, the City Administration should, regardless of the development of the Strategy, adjust its processes and applications in order to meet at least the minimum required by the Regulation. Among other things, enable electronic signing of documentation, for which it is necessary to have digital certificates and an application solution that will enable the implementation of signatures on documents [66].

The National Regulation, i.e., its Technical Specification [67], provides for the following. The technical specification is intended for public bodies and companies that develop digital solutions for public administration, as well as for all other interested stakeholders who cooperate with public bodies. It serves as a basis for public law bodies that have developed solutions for the digitalization of office business processes to upgrade existing systems. It also serves as a basis for public law bodies that do not have digitized office business processes to announce requests for procurement of necessary solutions. The technical specification contains a sufficient level of detail to be used without additional intervention as an annex to the public procurement procedure for all standard procedures in the office operations of public bodies. However, although the Technical Specification is designed to cover all key processes that occur in the office operations of public bodies, each public body can supplement the requirements in the procurement process required in their business processes if any, especially if special procedures regulate some processes.

The digitalization strategy of the city administration will focus on supplementing the requirements in the process of procuring the necessary software solutions in accordance with the data collected on the processes. It is also essential to adhere as much as possible to the standards for the development of public e-services in the Republic of Croatia [68] and the National Plan for the Development of Public Administration from 2021 to 2027 [69]. In addition, communication with the Association of Cities can be very useful to compare possible problem-solving approaches that are often the same for all cities, even throughout the possibility of developing application solutions at the state level, for example through national SSC hardware and software and using Government Service Bus [70].

4. Overview of Blockchain for Different Smart City Applications

Table 3 presents the advantages and disadvantages of blockchain technology as a technical solution in different Smart City applications. When developing a blockchain network, there are different security issues that should be considered and prevented when developing blockchain applications [50]. It is necessary to prevent 51% attack, phishing, routing and Sybil attacks, and endpoint vulnerabilities. A 51% attack can occur when a malicious entity collects more than half of the hash rate. It can be prevented by improving mining pool monitoring, increasing hash rate, or avoiding proof-of-work (PoW) consensus procedures. The goal of a phishing attack is to steal the user's credentials by entering login

details via a fake link, and gain access to their wallet. Having access to a user's wallet is an attack that gives access to sensitive information. A phishing attack can be avoided by educating users, improving browser security, and installing antivirus software. In a blockchain network, large amounts of data are transferred to an internet service provider, and an attacker can intercept data. In a routing attack, users are usually unaware of the attack because they do not monitor data transmission. To prevent routing attacks secure routing protocols and data encryption should be implemented. The blockchain network endpoint attack is oriented on users' interaction with the blockchain and monitors user's devices to steal the user's private key. To prevent endpoint vulnerabilities, private keys should be encrypted on users' devices and antivirus software installed. In the Sybil attack, numerous fake network nodes are created to obtain majority consensus and take control over a network like in a 51% attack. To prevent Sybil attacks, an appropriate consensus algorithm should be used to monitor network nodes behavior [71].

Blockchain technology is robust, decentralized, and not controlled by a single entity, and there is no single point of failure. Data are immutable, transparent, and traceable, and consensus among involved parties is needed to prevent fraudulent transactions. Some blockchain solutions have a limited number of transactions per second and transaction sizes; however, new blockchain solutions are developing every day to increase transaction size and speed. The GDPR requires that the processing of personal data be harmonized with professional regulations and without legalization will raise legal implications, so it is important to ensure new law regulations that include blockchain technology to secure user's data using encryption, authentication, and authorization. Smart contracts can be used to define terms and conditions, and if all involved parties agree with the rules in the smart contract, action is taken, and information is stored in the blockchain. Smart contracts enable users to define their rules on how to process their data and decisions; repetitive processes can be automated and executed when conditions are met. In this paper, blockchain is presented as a solution for different Smart City applications such as healthcare, waste management, water resources, resource sharing, etc. National standards and legislation are going toward including blockchain solutions in e-services like documents signatures, EBSI network, etc. Blockchain technology can be used for visualization of data, representing the view through history, and users can have trust in data due to the transparency and immutability of the blockchain. However, to achieve all these goals in the City of Osijek, to become the true Smart City, significant resources, new legislation, effort, and time are required.

Table 3. Blockchain pros and cons for digitalization strategy.

Digitalization Strategy	Pros	Cons	Consensus Considerations	Security Issues
Data Consolidation	Blockchain technology is robust Not controlled by a single entity Data are transparent and trusted	Constrictions on the number of transactions per second and transaction size	Proof-of-Authority (PoA)	51% attack, phishing, routing and Sybil attacks, endpoint vulnerabilities
GDPR	User's data are secured Data are encrypted, and a private key is needed for decryption	Requires new legislations	Proof-of-Authority (PoA)	Phishing attack
Internal Communication	The consensus among the trusted parties Traceability of communication	No	Proof-of-Authority (PoA), Proof-of-Stake (PoS)	Phishing attack
Repetitive Sub-processes	The Event Condition Action Smart contract for automated execution of repetitive tasks	Requires new transaction for every insertion of data	Proof-of-Authority (PoA)	Phishing attack
Existing Applications and Common Users Application	Application in healthcare, waste management, resource sharing Citizens are included in decision making	Transfer existing databases to blockchain Amount of data to be stored in blockchain	Proof-of-Stake (PoS)	51% attack, phishing, routing and Sybil attacks, endpoint vulnerabilities
Healthcare Application	Distributed data, transparency and immutability of data, easy permissions management	Development cost, the data cannot be deleted, lack of expert knowledge	Proof-of-Authority (PoA), Proof-of-Stake (PoS)	51% attack, phishing, endpoint vulnerabilities
Intelligent Transportation System Application	Trust, data immutability, efficiency because all members see data, transparency	Permissions about sensitive data, human error is not easy to correct, transaction scaling and costs	Proof-of-Authority (PoA), Proof-of-Stake (PoS)	51% attack, phishing, endpoint vulnerabilities
Water Resource Management Application	Distributed data, transparency and immutability of data, easy permissions management	Permissions about sensitive data, human error is not easy to correct, lack of expert knowledge	Proof-of-Authority (PoA), Proof-of-Stake (PoS)	51% attack, phishing, endpoint vulnerabilities
Waste Management Application	Distributed data, transparency and immutability of data, easy permissions management	Permissions about sensitive data, human error is not easy to correct, lack of expert knowledge	Proof-of-Authority (PoA), Proof-of-Stake (PoS)	51% attack, phishing, endpoint vulnerabilities
Resource Sharing Application	Enhanced security, transparency, instant traceability of shared resources, automation and efficiency	Number of transactions for large systems	Proof-of-Stake (PoS)	51% attack, phishing, endpoint vulnerabilities
Geoinformation System	Distributed data storage and access, data can be used for different Smart City applications	Non-existing or just developing blockchain architecture	Proof-of-Authority (PoA)	51% attack, phishing, endpoint vulnerabilities

Table 3. *Cont.*

Digitalization Strategy	Pros	Cons	Consensus Considerations	Security Issues
Existing Resources on National Level	Signatures on documents National standard for the development of e-service Croatia is part of EBSI network	Non-existing or just developing blockchain architecture	Proof-of-Authority (PoA)	Phishing attack, endpoint vulnerabilities
Regulation on Office Operations and Trends at National Level	Distributed data, transparency and immutability of data, easy permissions management, automation, efficiency, citizen's trust	Non-existing architecture and legalization, GDPR about sensitive data	Proof-of-Authority (PoA)	Phishing attack, endpoint vulnerabilities

5. Additional Considerations for Digitalization Strategy

The Strategy will, among other things, define the priorities, i.e., the order of digitalization of all recorded processes. As defined by the Strategy plan, the proposed order of digitalization will be based on measurable criteria such as frequency of use of the process, number of users, and implementation complexity. Of course, the final realization of priorities will be limited by the financial possibilities of the City of Osijek, depending on the annual city budgets reserved for digitalization processes.

5.1. Process Visualization

The digitalization strategy will also catalogue the processes presented in the BPMN diagrams. Due to their clarity, they should be the basis for visualizing the process in later software solutions, i.e., visually showing in the application which steps have been completed and which are still to come. As stated in previous chapters, Smart Cities have an increased amount of data coming from IoT devices. The event detection, monitoring, and prevention process requires visualization of collected data. To prevent different hazards like fires and traffic jams, Smart Cities need adequate visualizations that will enable city administration to make decisions, especially in real-time situations. Furthermore, a Smart City has heterogonous users and heterogeneous data sources and proper visualization methodology and complex dashboards are needed [72,73].

5.2. Business Logic Model and Advanced Technical Solutions

Business logic, i.e., process steps built into software support for individual processes, has the advantage of complete process automation and process status information for all relevant stakeholders. However, since business logic largely depends on the legal framework subject to change, the normal functioning of the city administration would require relatively more significant interventions in software support or the built-in logic of the process. Therefore, it is necessary to require the software provider to update the business logic according to the legal framework.

If the software does not have built-in business logic, and it is estimated that it is not effective to implement (too complex processes, too frequent process changes, the existing software solution does not allow the implementation of business logic), and switching to another solution with built-in logic would not be profitable, should be built into existing software or a new process visualization solution should be developed, as explained in Section 3.8, in which users can manually indicate which process step has been completed or is in progress. Although very popular in Smart City concepts, it is necessary to rationally introduce advanced technological solutions such as artificial intelligence methods.

Artificial intelligence methods are very useful [74–76], e.g., in recognizing certain regularities, optimizing processes/systems, etc. Furthermore, artificial intelligence can be converged with blockchain technology in Smart City network architecture to get the best from both worlds [77]. However, the introduction of such methods shows its great advantage only after the city administration has access to all relevant data as explained in Section 3.1, and all possibilities of simple analytics are exhausted through the visualization of basic indicators.

6. Conclusions

This paper presents blockchain technology as a technical solution in different Smart City applications like healthcare, waste management, resource sharing, and citizens' involvement in decision making. The blockchain has properties that correspond with the digitalization strategy of the City of Osijek, like decentralization, transparency, robustness, security, and overall citizens' trust in city government. The digitalization strategy is divided into phases, and each phase has benefited from blockchain technology. The main obstacle in implementing blockchain is the legal framework that should be changed to legalize blockchain usage in governance procedures, such as legal documents, licenses, etc.

Therefore, using blockchain applications without legalization will raise legal implications, so it is important to ensure new law regulations. After law regulations, Smart contracts could be used for automated decision making, such as automated warning systems, automated reports, automated agreement execution, payment, etc. This paper aims to develop a digitalization strategy that can be a path for the City of Osijek to transform city governance for the future and become a Smart City, which will improve quality of life, include citizens in city governance, and make transparent and trustworthy relations among all included parties.

In the future, the authors will continue to work on the digitalization strategy. The first step is focused on integrating IoT devices into blockchain protocols to reach trust in collected data, which can be used by city governance to conduct the next step in digitalization.

Author Contributions: Conceptualization, I.L. and K.M.; methodology, I.L.; software, D.V. and M.K.; validation, I.L. and M.K.; formal analysis, K.M. and D.V.; investigation, I.L. and K.M.; resources, K.M., I.L. and M.K.; data curation, D.V., I.L. and M.K.; writing—original draft preparation, I.L.; writing—review and editing, I.L. and D.V.; visualization, I.L. and M.K.; supervision, K.M., I.L. and M.K.; project administration, K.M., I.L. and M.K.; funding acquisition, I.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the ESIA—Expert System for Intelligent Agriculture (KK.01.1.1.07.0036).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Acknowledgments: This work results from implementing research activities on the project Development of an expert system for food production and processing management (ESIA-Expert System for Intelligent Agriculture KK.01.1.1.07.0036). The authors gratefully acknowledge the contribution of the City of Osijek, its management and employees for cooperation and allowance to use the data for this paper.

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

References

1. Ministerial Declaration on eGovernment—The Tallinn Declaration. Available online: https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration (accessed on 20 April 2022).
2. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consum. Electron. Mag.* **2016**, *5*, 60–70. [CrossRef]
3. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
4. Jin, J.; Gubbi, J.; Marusic, S.; Palaniswami, M.S. An Information Framework for Creating a Smart City Through Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 112–121. [CrossRef]
5. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors* **2022**, *22*, 2604. [CrossRef]
6. Dammak, B.; Turki, M.; Cheikhrouhou, S.; Baklouti, M.; Mars, R.; Dhahbi, A. LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring. *Sensors* **2022**, *22*, 1497. [CrossRef]
7. Li, C.-T.; Shih, D.-H.; Wang, C.-C.; Chen, C.-L.; Lee, C.-C. A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System. *IEEE Access* **2020**, *8*, 173904–173917. [CrossRef]
8. Ahmad, R.W.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Omar, M. Blockchain for Waste Management in Smart Cities: A Survey. *IEEE Access* **2021**, *9*, 131520–131541. [CrossRef]
9. Alkhateeb, A.; Catal, C.; Kar, G.; Mishra, A. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors* **2022**, *22*, 1304. [CrossRef]
10. Islam, A.; Al Amin, A.; Shin, S.Y. FBI: A Federated Learning-Based Blockchain-Embedded Data Accumulation Scheme Using Drones for Internet of Things. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 972–976. [CrossRef]
11. Islam, A.; Rahim, T.; Masuduzzaman, M.D.; Shin, S.Y. A Blockchain-Based Artificial Intelligence-Empowered Contagious Pandemic Situation Supervision Scheme Using Internet of Drone Things. *IEEE Wirel. Commun.* **2021**, *28*, 166–173. [CrossRef]
12. Lv, L.; Yang, Z.; Zhang, L.; Huang, Q.; Tian, Z. Multi-party transaction framework for drone services based on alliance blockchain in smart cities. *J. Inf. Secur. Appl.* **2021**, *58*, 102792. [CrossRef]
13. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling Drones in the Internet of Things with Decentralized Blockchain-Based Security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [CrossRef]

14. Szabo, N. Smart Contracts. 1994. Available online: http://www.fon.hum.5uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed on 20 April 2020).
15. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper. 2014. Available online: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf (accessed on 20 April 2020).
16. Chen, C.-L.; Deng, Y.-Y.; Tsaur, W.-J.; Li, C.-T.; Lee, C.-C.; Wu, C.-M. A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology. *Sustainability* **2021**, *13*, 9386. [CrossRef]
17. Drummer, D.; Neumann, D. Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *J. Inf. Technol.* **2020**, *35*, 337–360. [CrossRef]
18. What Is the Blockchain Oracle Problem? Available online: https://blog.chain.link/what-is-the-blockchain-oracle-problem/ (accessed on 20 April 2020).
19. Mammadzada, K.; Iqbal, M.; Milani, F.; García-Bañuelos, L.; Matulevičius, R. Blockchain Oracles: A Framework for Block-chain-Based Applications. In *Business Process Management: Blockchain and Robotic Process Automation Forum, Proceedings of the BPM 2020 Blockchain and RPA Forum, Seville, Spain, 13–18 September 2020*; BPM Lecture Notes in Business Information Processing; Asatiani, A., García, J.M., Helander, N., Jiménez-Ramírez, A., Koschmider, A., Mendling, J., Meroni, G., Reijers, H.A., Eds.; Springer: Cham, Switzerland, 2020.
20. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 30 March 2022).
21. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry* **2021**, *13*, 1363. [CrossRef]
22. Puthal, D.; Mohanty, S.P. Proof of Authentication: IoT-Friendly Blockchains. *IEEE Potentials* **2019**, *38*, 26–29. [CrossRef]
23. Manolache, M.A.; Manolache, S.; Tapus, N. Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Comput. Sci.* **2020**, *199*, 580–588. [CrossRef]
24. Moni, M.; Melo, W.; Peters, D.; Machado, R. When Measurements Meet Blockchain: On Behalf of an Inter-NMI Network. *Sensors* **2021**, *21*, 1564. [CrossRef]
25. Melo, W.; Machado, R.C.S.; Peters, D.; Moni, M. Public-Key Infrastructure for Smart Meters using Blockchains. In Proceedings of the 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, Roma, Italy, 3–5 June 2020; pp. 429–434. [CrossRef]
26. Shamsi, K.; Afzal, M. IoT implementation using secure communication protocols. *Int. J. Comput. Eng. Sci.* **2017**, *7*, 2250–3005.
27. Dragomir, D.; Gheorghe, L.; Costea, S.; Radovici, A. A Survey on Secure Communication Protocols for IoT Systems. In Proceedings of the 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, 26–30 September 2016; pp. 47–62. [CrossRef]
28. Nguyen, K.T.; Laurent, M.; Oualha, N. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Netw.* **2015**, *32*, 17–31. [CrossRef]
29. Immler, V.; Obermaier, J.; Konig, M.; Hiller, M.; Sig, G. B-TREPID: Batteryless tamper-resistant envelope with a PUF and integrity detection. In Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; pp. 49–56. [CrossRef]
30. Weiner, M.; Manich, S.; Rodriguez-Montanes, R.; Sigl, G. The Low Area Probing Detector as a Countermeasure Against Invasive Attacks. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2017**, *26*, 392–403. [CrossRef]
31. Kim, T.; Park, T.-H. Extended Kalman Filter (EKF) Design for Vehicle Position Tracking Using Reliability Function of Radar and Lidar. *Sensors* **2020**, *20*, 4126. [CrossRef] [PubMed]
32. Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 2652–2657. [CrossRef]
33. Steichen, M.; Fiz, B.; Norvill, R.; Shbair, W.; State, R. Blockchain-Based, Decentralized Access Control for IPFS. 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. 1499–1506. [CrossRef]
34. Kumar, R.; Tripathi, R. Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain. In Proceedings of the 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, 15–17 November 2019; pp. 246–251. [CrossRef]
35. Zheng, Q.; Li, Y.; Chen, P.; Dong, X. An Innovative IPFS-Based Storage Model for Blockchain. In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 3–6 December 2018; pp. 704–708. [CrossRef]
36. Koo, J.; Kim, Y.-G. Interoperability requirements for a smart city. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing (SAC '21), Virtual Event, 22–26 March 2021*; Association for Computing Machinery: New York, NY, USA, 2021; pp. 690–698. [CrossRef]
37. Buchinger, M.; Kuhn, P.; Balta, D. Towards Interoperability of Data Platforms for Smart Cities. In *Handbook of Smart Cities*; Augusto, J.C., Ed.; Springer: Cham, Switzerland, 2021. [CrossRef]
38. Brutti, A.; Frascella, A.; Gessa, N.; De Sabbata, P.; Novelli, C. Interoperability in the Smart City: A Semantic Approach for Merging Flexibility with Strictness. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 434–439. [CrossRef]

39. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. *IEEE Netw.* **2020**, *34*, 8–14. [CrossRef]
40. Badii, C.; Bellini, P.; Difino, A.; Nesi, P. Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. *IEEE Access* **2020**, *8*, 23601–23623. [CrossRef]
41. Enler, E.; Pentek, I.; Adamko, A. Building Smart City Solutions with Focus on Health Care and GDPR. In *Handbook of Smart Cities*; Augusto, J.C., Ed.; Springer: Cham, Switzerland, 2021. [CrossRef]
42. Haque, A.B.; Islam, A.K.M.N.; Hyrynsalmi, S.; Naqvi, B.; Smolander, K. GDPR Compliant Blockchains—A Systematic Literature Review. *IEEE Access* **2021**, *9*, 50593–50606. [CrossRef]
43. Abuhashim, A.; Tan, C.C. Smart Contract Designs on Blockchain Applications. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–4. [CrossRef]
44. Dwivedi, S.K.; Amin, R.; Vollala, S.; Chaudhry, R. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. *Comput. Electr. Eng.* **2020**, *86*, 106719. [CrossRef]
45. Suma, S.; Mehmood, R.; Albeshri, A. Automatic Event Detection in Smart Cities Using Big Data Analytics. In *Smart Societies, Infrastructure, Technologies and Applications, SCITA 2017, Proceedings of the First International Conference, SCITA 2017, Jeddah, Saudi Arabia, 27–29 November 2017*; Mehmood, R., Bhaduri, B., Katib, I., Chlamtac, I., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Switzerland, 2018; Volume 224, p. 224. [CrossRef]
46. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Kumar, N.; Das, A.K.; Saxena, N. LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. *IEEE Commun. Mag.* **2018**, *56*, 24–32. [CrossRef]
47. Zhang, P.; Liu, Z.; Han, S.; He, L.; Müller, H.S.; Zhao, T.; Wang, Y. Visualization of rapid penetration of water into cracked cement mortar using neutron radiography. *Mater. Lett.* **2017**, *195*, 1–4. [CrossRef]
48. Kuo, T.-T.; Kim, H.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef]
49. Vora, J.; Nayyar, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018.
50. Bernardini, C.; Asghar, M.R.; Crispo, B. Security and privacy in vehicular communications: Challenges and opportunities. *Veh. Commun.* **2017**, *10*, 13–28. [CrossRef]
51. Sharma, P.K.; Chen, M.-Y.; Park, J.H. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access* **2017**, *6*, 115–124. [CrossRef]
52. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [CrossRef]
53. Bracciali, A.; Chatzigiannakis, I.; Vitaletti, A.; Zecchini, M. Citizens Vote to Act: Smart contracts for the management of water resources in smart cities. In Proceedings of the 2019 First International Conference on Societal Automation (SA), Krakow, Poland, 4–6 September 2019; pp. 1–8. [CrossRef]
54. Nirde, K.; Mulay, P.S.; Chaskar, U.M. IoT based solid waste management system for smart city. In Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 15–16 June 2017; pp. 666–669. [CrossRef]
55. Wijaya, A.S.; Zainuddin, Z.; Niswar, M. Design a smart waste bin for smart waste management. In Proceedings of the 2017 5th International Conference on Instrumentation, Control, and Automation (ICA), Yogyakarta, Indonesia, 9–11 August 2017; pp. 62–66. [CrossRef]
56. Mingaleva, Z.; Vukovic, N.; Volkova, I.; Salimova, T. Waste Management in Green and Smart Cities: A Case Study of Russia. *Sustainability* **2019**, *12*, 94. [CrossRef]
57. Dasaklis, T.K.; Casino, F.; Patsakis, C. A traceability and auditing framework for electronic equipment reverse logistics based on blockchain: The case of mobile phones. In Proceedings of the 2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA), Piraeus, Greece, 15–17 July 2020; pp. 1–7. [CrossRef]
58. Gupta, N.; Bedi, P. E-waste Management Using Blockchain based Smart Contracts. In Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 19–22 September 2018; pp. 915–921. [CrossRef]
59. Joshi, N. Revolutionizing Waste Management with Blockchain Technology. Available online: https://www.allerin.com/blog/revolutionizing-waste-managementwith-blockchain-technology (accessed on 20 April 2020).
60. Akter, O. Blockchain Leveraged Incentive Providing Waste Management System. In *Emerging Technologies in Data Mining and Information Security*; Springer: Singapore, 2020.
61. Huang, T. Resource Sharing of Smart City Based on Blockchain. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5886024. [CrossRef]
62. Hamdaoui, B.; Alkalbani, M.; Rayes, A.; Zorba, N. IoTShare: A Blockchain-Enabled IoT Resource Sharing On-Demand Protocol for Smart City Situation-Awareness Applications. *IEEE Internet Things J.* **2020**, *7*, 10548–10561. [CrossRef]
63. Lukić, I.; Krpić, Z.; Köhler, M.; Galba, T. Improving Logistics of the Public Services in Smart Cities Using a Novel Clustering Method. *Int. J. Inf. Technol. Decis. Mak.* **2021**, *20*, 1447–1475. [CrossRef]

64. Calderoni, L.; Maio, D.; Palmieri, P. Location-aware Mobile Services for a Smart City: Desing, Implementation and Deployment. *J. Theor. Appl. Electron. Commer. Res.* **2012**, *7*, 15–16. [CrossRef]
65. Bryant, N.; Spencer, N.; King, A.; Crooks, P.; Deakin, J.; Young, S. IoT and smart city services to support independence and wellbeing of older people. In Proceedings of the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 1–23 September 2017. [CrossRef]
66. Regulation on Office Operations. Available online: https://narodne-novine.nn.hr/clanci/sluzbeni/2021_07_75_1415.html (accessed on 20 April 2020).
67. Annex to the Regulation on Office Operations. Available online: https://rdd.gov.hr/UserDocsImages//SDURDD-dokumenti//02_Tehni%C4%8Dka%20specifikacija.pdf (accessed on 20 April 2020).
68. E-Standard Guidelines. Available online: https://rdd.gov.hr/e-standardi/dokumentacija/1824 (accessed on 20 April 2020).
69. National Plan for the Development of Public Administration from 2021 to 2027. Available online: https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=19440 (accessed on 20 April 2020).
70. Government Service Bus. Available online: https://rdd.gov.hr/istaknute-teme/interoperabilnost-sustava-javne-uprave-drzavna-sabirnica-gsb/1873 (accessed on 20 April 2020).
71. Blockchain Security Issues and How to Prevent Them. Available online: https://www.fastcompany.com/90722111/5-blockchain-security-issues-and-how-to-prevent-them (accessed on 24 March 2022).
72. Lavalle, A.; Teruel, M.; Maté, A.; Trujillo, J. Improving Sustainability of Smart Cities through Visualization Techniques for Big Data from IoT Devices. *Sustainability* **2020**, *12*, 5595. [CrossRef]
73. Ji, W.; Xu, J.; Qiao, H.; Zhou, M.; Liang, B. Visual IoT: Enabling Internet of Things Visualization in Smart Cities. *IEEE Netw.* **2019**, *33*, 102–110. [CrossRef]
74. Nikitas, A.; Michalakopoulou, K.; Njoya, E.T.; Karampatzakis, D. Artificial Intelligence, Transport and the Smart City: Definitions and Dimensions of a New Mobility Era. *Sustainability* **2020**, *12*, 2789. [CrossRef]
75. Luckey, D.; Fritz, H.; Legatiuk, D.; Dragos, K.; Smarsly, K. Artificial Intelligence Techniques for Smart City Applications. In *Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, ICCCBE 2020, São Paulo, Brazil, 18–20 August 2020*; Lecture Notes in Civil Engineering; Toledo Santos, E., Scheer, S., Eds.; Springer: Cham, Switzerland, 2021; Volume 98. [CrossRef]
76. Khan, S.; Paul, D.; Momtahan, P.; Aloqaily, M. Artificial intelligence framework for smart city microgrids: State of the art, challenges, and opportunities. In Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018; pp. 283–288. [CrossRef]
77. 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]