computers

MDPI

Review

The Use of Blockchain Technology in e-Government Services

Ioannis Lykidis [1], George Drosatos [2] and Konstantinos Rantos [1,*]

[1] Department of Computer Science, International Hellenic University, 65404 Kavala, Greece; iolykid@cs.ihu.gr
[2] Institute for Language and Speech Processing, Athena Research Center, 67100 Xanthi, Greece; gdrosato@athenarc.gr
* Correspondence: krantos@cs.ihu.gr; Tel.: +30-2510-462611

Abstract: e-Government services have evolved significantly over the last decade, from a paper-based bureaucratic procedure to digital services. Electronically processed transactions require limited physical interaction with the public administration, and provide reduced response times, increased transparency, confidentiality and integrity. Blockchain technology enhances many of the above properties as it facilitates immutability and transparency for the recorded transactions and can help establish trust among participants. In this paper, we conduct a literature review on the use of blockchain technology in e-government applications to identify e-government services that can benefit from the use of blockchains, types of technologies that are chosen for the proposed solutions, and their corresponding maturity levels. The aim is to demonstrate blockchain's potential and contribution to the field, provide useful insights to governments who are considering investing in this innovative technology, and facilitate researchers in their future activities in blockchain-enabled e-government services.

Keywords: blockchain; distributed ledger technology; e-government; review

Citation: Lykidis, I.; Drosatos, G.; Rantos, K. The Use of Blockchain Technology in e-Government Services. *Computers* **2021**, *10*, 168. https://doi.org/10.3390/computers10120168

Academic Editor: Wenbing Zhao

Received: 1 October 2021
Accepted: 3 December 2021
Published: 10 December 2021

1. Introduction

Blockchain technology was initially introduced in cryptocurrency applications. Blockchain are transparent, tamper-resistant, digital ledgers, implemented in a distributed network of peer-to-peer nodes in which transactions are made securely and usually without the approval of a central and trusted authority [1]. The information of every transaction is stored hashed in blocks; each block also contains the hash of the previous block and this chain of blocks is called the ledger. This allows a community of users to record transactions in a shared ledger so that these transactions cannot be changed after adding it to the blockchain. Thus, blockchains allow peer-to-peer nodes that do not have a trust relationship to exchange data without third parties or intermediaries. This data could correspond to money, contracts, land titles, medical and educational records, certificates, purchase and sale of goods/services, or any other transactions or assets that could be digitised.

Blockchain technology, as in many other fields, has been explored by e-government to promote public administration transformation and facilitate the provision of transparent and secure public services. The main purpose of adopting this technological approach is to avoid the use of a central authority for citizens'/businesses' transactions with government authorities, to decentralise the collection, storage and processing of data, and to ensure data integrity and immutability.

However, the use of blockchain technology raises many privacy concerns, as many e-government services involve personal data that needs to be properly protected so that blockchain is not the target of adversaries gaining unauthorised access to citizens' data. Thus, the proposed solutions have to take into account legal restrictions, such as those imposed by the General Data Protection Regulation (GDPR) [2] and respect the privacy of users when publishing transactions in the ledger, while providing the necessary authorised access to public administration parties and other stakeholders.

Many efforts have been made by governments to adopt and implement blockchain technology in some of their public services, although the majority of them are still at an early stage. The aim of this paper is to provide a literature review on the use of blockchain technologies in Government-to-Government (G2G), Government-to-Business (G2B) and Government-to-Citizen (G2C) services in order to simplify the administrative procedures, as well as to enhance the security, transparency and privacy of e-government services. In this context, we explore areas such as e-contracts, e-voting, authentication, data sharing and land registry.

The main contribution of this paper is to present a literature review with case studies of e-government services that have adopted blockchain technology between 2015 and 2020, description of each blockchain framework and its characteristics and the maturity level of the proposed solutions. A two-level screening process was conducted using eligibility criteria in an attempt to narrow down the results and gain insight into a corresponding group of research questions regarding the use of blockchain technology in e-government services. The results of our research provided us with a yearly distribution of the blockchain state-of-the-art solutions that enabled us to demonstrate its potential and contribution to the field.

The rest of this paper is organised as follows. Section 2 provides an introduction to blockchain technology and e-government services. The research methodology for our literature research and analysis is presented in Section 3, while related works are provided in Section 4. Section 5 analyses the proposed use of blockchain in e-government services, while Section 6 discusses the findings of this research. Finally, in Section 7, we come to our conclusions.

2. Background

2.1. Blockchain Technology

The first appearance of blockchain technology was in October 2008 with the Bitcoin digital currency platform by Satoshi Nakamoto [3]. Executed transactions are hashed and stored in blocks. Each new block contains not only the stored transactions information, but also the hash of the previous block. Figure 1 illustrates this sequence of blocks that form a blockchain. The hash is also used to identify and integrate information. The hashing method is a way to secure data in a blockchain [4].

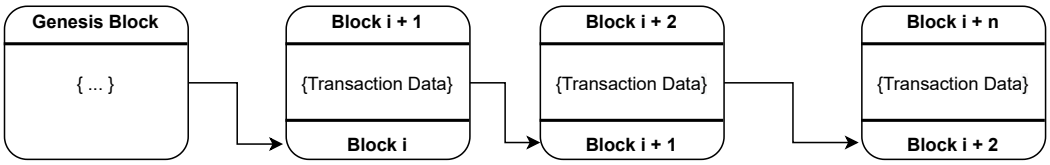

Figure 1. Generic blockchain model.

The blockchain consists of a peer-to-peer network, in which transactions are executed between nodes securely without the need for the approval of a central authority [5]. Each node in the network is able to hold a full copy of the ledger. Each transaction is validated through the consensus mechanism, which is the procedure of an asynchronous messaging communication between a number of nodes in the network, such as an announcement of a transaction representing an event in the system or the creation and broadcasting of a block that contains information of the transaction. Afterwards, each node should validate by checking the consistency of the transaction sequence of the new block [6]. Some of the consensus mechanism are Proof-of-Work [7] and Proof-of-Stake [8]. Successfully validated transactions are added to the ledger which is updated throughout the network [9].

Another way to execute transactions is with smart contracts [10] that are designed to satisfy contractual conditions that allow the interaction between untrusted nodes and do not require the approval of a central authority [1]. Smart contracts have become more popular as they can be used more easily in information and communication technologies [11].

Blockchain technologies, can be divided into different types, based on requirements for data access and control. These architectures give users the right to read and/or write data, as well as who will participate in the consensus mechanism [12,13]. Examples are public and private blockchains, that determine who has the right to read the existing data. Another categorisation is the permissionless and permissioned blockchain, which determine the ability to add blocks to the chain and participate in the consensus mechanism [14,15].

2.2. e-Government Services

e-Government is an effort by governments to use Information and Communications Technology (ICT) to automate public services and facilitate their use by citizens (G2C), businesses (G2B) and intergovernmental (G2G), such as secure data transfer, e-procurement, filling tax returns, identity management, electronic voting, etc. The purpose of this effort is to integrate public services electronically, in which the service of citizens and businesses to be done safely, transparently and with trust in a decentralised way without the involvement of public authorities and to eliminate bureaucracy.

Due to the increasing demand for online services from citizens and the need for reducing bureaucracy, more and more governments are turning their services to electronic forms. Electronic services are all time available and accessible from everywhere, and easy to use. The European Commission, recognizing the demands of citizens, businesses and governments for having access to e-government services, has been working on an e-government action plan. This action plan has based on the e-government benchmark for the period 2016–2020, which collects data on an annual basis from online stakeholders for new proposals for the future action plan [16] The action plan envisages user-friendly public administrations to reduce administrative burdens through digital services, cross-border services through connecting public administrations across Europe, opening up government data, services and procedures to create better or new services and improve policies. Four principles define the action plan: digital-by-default, cross-border by default, once-only principle and inclusive by default. Furthermore, the e-government benchmark measures progress in four areas, called top-level benchmarks: user-centricity, transparency, key enablers and cross-border mobility [17]. For user-centricity as technology evolves, upcoming technologies such as blockchain, augmented and virtual reality, and AI, are expected to be part of the digital services improvement [18].

Many researches were made in which ways blockchain will benefit as an infrastructure in e-government services, and the challenges that this approach can have [13].

3. Research Methodology

The research methodology that has been followed in this review paper included an initial search on Scopus (www.scopus.com, accessed on 15 January 2021) to identify published works related to the use of blockchain technology in e-government services. The search query that was used for this purpose, looking at the title, abstract and keywords of the papers, is as follows:

```
TITLE-ABS-KEY(("e-governance" OR "smart governance" OR "smart government"
      OR "e-government") AND (blockchain OR "distributed ledger"))
```

Our search was conducted in January 2021, and included 131 results until the end of 2020. We have worked on a two-level screening process, as shown in Figure 2. Therefore, we set the following eligibility criteria: the paper, (i) presents a solution that uses blockchain technology exclusively in e-government services, (ii) is published in peer-reviewed journals or conferences, (iii) is written in English and (iv) has the full-text available. On the first level, we have looked at the title, abstract and keywords of the papers and excluded those papers that did not meet our eligibility criteria. From this process, we excluded 84 papers and the remaining papers were 47. On the second level of the screening process, we have looked at the full-text of the papers taking into consideration the same eligibility criteria and the results were 19 papers.

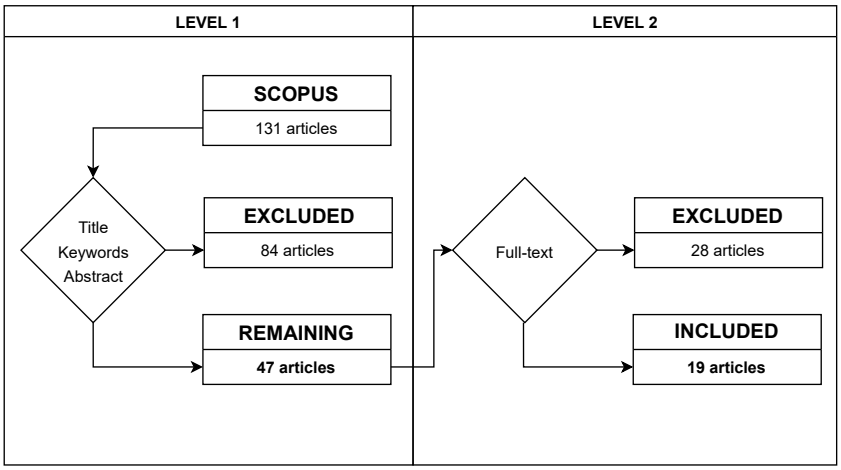

Figure 2. Two-level screening process.

Figure 3 shows the yearly distribution of the retrieved papers compared to the papers included in our literature review. As can be seen in this chart, there has been an increase of scientific interest in the use of blockchain in e-government applications in 2019.

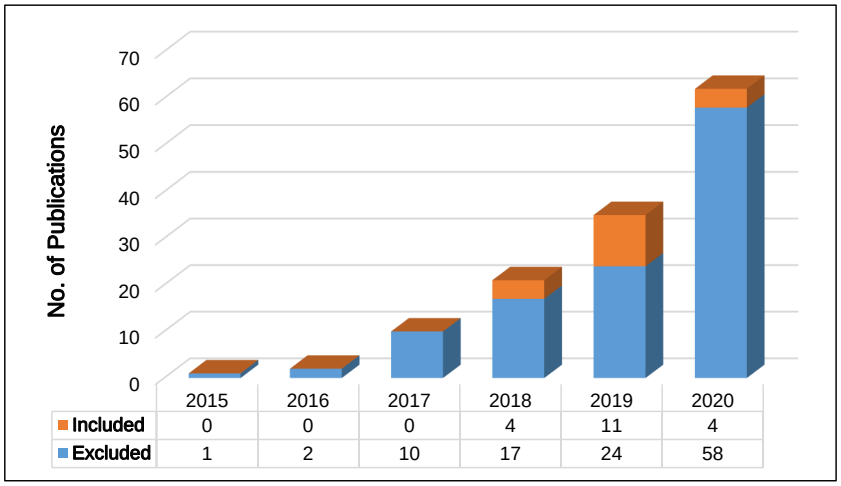

Figure 3. Yearly distribution of the included/excluded papers.

The research questions that we will try to answer in our research are the following:

RQ1. Which type of e-government service is provided?
RQ2. Which blockchain technology frameworks are used and with what characteristics?
RQ3. What is the maturity level of the proposed solution in e-government?
RQ4. What is the case study of the proposed solution?

4. Related Work

In this section, we present previous literature reviews on the use of blockchain technology in e-government services. During our research, three literature reviews were identified and included publications up to the year 2018.

Franciscon et al. [15] focused on a systematic review of the types of software architecture used in public services based on blockchain technology. However, several publications have not articulately described their architecture. Their research was conducted for publications made in the years from 2016 to 2018.

Batubara et al. [19] researched the state of the art solutions and addressed the challenges faced by the adoption of blockchain technology in e-government services. Their analysis mainly included system architecture, conceptual frameworks, system analysis, design, development and evaluation and was limited to publications that use blockchain

technology exclusively in e-government services. The systematic literature review was conducted for publications made until the end of 2017.

Alexopoulos et al. [20] first started by conducting a literature review in general on the types and features of blockchain technology to gather the benefits and obstacles of this technology, then they researched for projects that used blockchain technology in e-government services, and, finally, they conducted semi-structured interviews with experts to validate their findings. Their research was performed for publications made until the year 2018.

In this paper, we have included publications until the end of 2020, as shown in Section 3. Additionally, we have focused on the implementations of the proposed solutions, the utilised blockchain technology and its characteristics, and the maturity level of the given solutions.

5. Blockchain-Enabled e-Government Applications

In this section, we have categorised the papers that remained from the screening process, by the type of e-government services they have provided or supported, and we present each of these solutions based on this categorisation. The categorisation is also shown in Table 1 accompanied by the answers to the research questions given in Section 3.

Table 1. Research papers included in the review and their characteristics.

No.	Author	Year	Blockchain	Consensus Algorithm	Maturity of Solution	Case Study
Authentication (Section 5.1):						
1	Chen et al. [21]	2019	Consortium Blockchain, Hyperledger Fabric	Kafka Consensus	Experimental	PKI system using Blockchain
2	Khan et al. [22]	2019	Consortium Blockchain, Hyperledger Fabric	-	Conceptual	Dubai Economic Department's Unified Corporate Registry
3	Batubara et al. [23]	2019	Public Permissioned Blockchain	-	Proposal	Indonesian Land Registry
4	Pinter et al. [24]	2019	-	-	Conceptual	Austrian SVN-G Law
5	Páez et al. [25]	2020	Private Blockchain	Tournament Consensus Algorithm, Proof-of-Luck	Prototype	Biometric e-ID System
Data Sharing (Section 5.2):						
6	Liu et al. [26]	2018	Private Blockchain	-	Conceptual	Privacy protection in governmental data sharing
7	Ghanem and Alsoufi [27]	2019	Consortium Blockchain, Ethereum	-	Proposal	A unified portable citizen's public and private records using blockchain technology
8	Zhang et al. [28]	2019	Consortium Blockchain	-	Conceptual	Data sharing between government departments
9	Xu et al. [29]	2019	Consortium Blockchain, Hyperledger Fabric	-	Experimental	Electronic certificates catalogue sharing in China
10	Naing [30]	2019	-	Proof-of-Work, Proof-of-Authority	Conceptual	Data sharing between government departments
11	Elisa et al. [31]	2019	Consortium Blockchain, Ethereum	Proof-of-Stake	Experimental	Information sharing services
e-Voting (Section 5.3):						
12	Hjalmarsson et al. [32]	2018	Private Blockchain, Go-Ethereum	Proof-of-Authority	System evaluation	Blockchain-based e-voting system
13	Yavuz et al. [33]	2018	Private Blockchain, Ethereum (Rinkeby)	-	Prototype	Small-scale polls and elections
14	Khan et al. [34]	2020	Private Blockchain, MultiChain	Proof-of-Work	Experimental	Blockchain-based e-voting system
Land Property Services (Section 5.4):						
15	Alketbi et al. [35]	2020	Private Blockchain, Hyperledger Fabric	Kafka Consensus	Conceptual	Housing rental in Dubai
16	Nguyen et al. [36]	2020	Private Blockchain, Hyperledger Fabric & Sawtooth	-	Experimental	Land Management e-gov application framework in Vietnam
e-Delivery Services (Section 5.5):						
17	Payeras-Capella et al. [37]	2019	Consortium Blockchain, Ethereum	Proof-of-Work	Prototype	Multiparty registered e-Delivery system
Human Resources Management (Section 5.6):						
18	Neiheiser et al. [38]	2019	Any Blockchain with built-in cryptocurrency and Smart Contracts	-	Prototype	Applicants selection process
Government Contracting (Section 5.7):						
19	Diallo et al. [39]	2018	Public Blockchain	Proof-of-Work	Conceptual	Distributed Autonomous Organisation based on the U.S. Small Business Administration Policies

5.1. Authentication

Chen et al. [21] proposed a blockchain-based trust-transferring scheme using different PKI systems to enhance trust when users need cross-domain access. They have worked to solve at a national level the trust service problem of PKI using blockchain consensus. The authors have proposed a consortium blockchain, which includes users of a particular group and a limited number of regulatory parties. Some of the nodes can be named to mutually maintain the ledger and block generation. Alternative PKI systems services participating in the consortium can be used by users. When a user wants to have access to a service, she needs to be validated by presenting her certificate. An authentication request is sent to the blockchain for the presented certificate to validate whether the certificate is active or revoked. As a security enhancement, the blockchain scheme uses the traditional Online Certificate Status Protocol (OCSP) [40,41], which returns the status of the certificate to the blockchain in real-time. Following that, the blockchain sends for each certificate its information and time to the server. The final step is for the server to confirm the information and pass the verification.

Khan et al. [22] suggested that full integration of e-business services and e-government services could be achieved by using blockchain technologies. This could make the government's processes faster and more secure. Also, data synchronisation between departments could easily be achieved. In their paper, they explore the evolution of e-government services in the U.A.E. and specific in one of the government's departments in Dubai. A consortium blockchain technology was adopted for developing a Unified Corporate Registry which will allow authenticated users to create and update license information though the blockchain. For this implementation the Hyperledger Fabric platform was used. The registry is integrated with other nodes in the network such as public registries, and other business entities. Each node pushes to the corresponding business activity entity the license information whenever there is an new issue or renewal or modification or cancellation. There are three types of members in the united registry, the nodes that publish data to the registry, the data subscribers and the service providers, the nodes that subscribe data from the registry for any business activity transaction, and the nodes that manage registry's indexes.

Batubara et al. [23] evidenced the existence of improvement in transparency and accountability in e-government services when using blockchain technologies. As a case study for their work, they used the land registry and how blockchain technology could improve transparency and accountability. The use of cryptographic pair of keys is not enough. The user's authentication needs supreme perquisites for the system to function properly, enforcing an electronic identity prerequisite on all members of the blockchain. If members want to validate only users that have confirmed their real identity to the relevant authority that manages their transaction, then a public permissioned blockchain is adequate. Therefore, the electronic identity is needed. By this, the legal status of all members that transact is guaranteed and at the same time the transparency is preserved since the information on the ledger is public and everyone can read it. In case of land registry, the smart contract could be utilised as support of the system. Specific rules and prerequisites could be enclosed into the smart contract; the results are added to the blockchain. Each block of the chain is being transmitted to the network in order for the nodes to validate it. After the block is validated it will be appended to the previous block of the ledger. The authentication is made by using asymmetric cryptography that means that the specific member is authorised to work on it. In addition, by the presence of a large number of nodes and by the consensus algorithm in the communication between all nodes for the validation of the transaction, the whole network accepts the transactions.

Pinter et al. [24] suggested that e-government services, such as e-ID, could be enhanced by using blockchain technology. The main concept is to avoid a centralised model where only one authority could authenticate users. A decentralised model also helps to enhance security layers against attacks. Another matter that needs to be considered, is data protection because data is stored publicly on the blockchain. An approach to avoid data

protection breaches is to store only technical references to the blockchain, all the other data could be stored locally. In the privacy-by-design framework, multiple identities should allow if needed for each user. Using blockchain helps to confirm the user's identities by the signature of their public keys. Their proposed architecture is based on the SVN-G draft law. For the identification of users. The user has to log on to an ID portal, where he can choose one of the authorised Know Your Customer (KYC) [42] providers, to identify himself. When the KYC completes the verification of the user's identity, the information is stored in the public blockchain. After that, the user is provided with a signature from the KYC which helps him to log on without revealing his personal data in any service that trusts the KYC provider. The connection between a public key and other offline data such as ID number is stored with the KYC provider in a private database. In case of illegal activities, the corresponding information is provided to the authorities. The advantage of using the blockchain in the process of the KYC provider helps to protect against the DoS attacks.

Páez et al. [25] proposed a blockchain-based architecture and a new consensus algorithm for digital identification of citizens by using biometric information. The proposed Colombian national e-ID system uses a blockchain to manage citizens' transactions, where users are authenticated and their transactions are validated using fingerprint and iris recognition. The blockchain network architecture uses a private, permissioned blockchain where only notaries and registries can be part of it. Two types of nodes can be part of the network. One of these two are in charge of issuing an identity document when it is requested by the citizens and they are located in the registration offices. These nodes are the only ones that can generate any digital certificate with its public and private keys by using each citizen's personal identification number. After the above-mentioned procedure is finished and the digital certificate is issued, the citizen can digitally sign any document and perform any transaction. Notary offices are the other type of nodes, which are responsible for maintaining citizen's civil status, validating the correspondence of citizen's identity and the relevant document for citizen's proof of identity. When a new node wants to participate to the network, it sends a request to every node in the network. If it is confirmed as an authorised node, it receives a copy of the ledger and has the right to create a transaction and add blocks to the chain. The network uses the Tournament Consensus Algorithm (TCA) in order to choose which node will add the next block to the chain. TCA sends a request for choosing a number between 0 and 1 to everyone who is connected to the network every random time. The node that has collected all random numbers, finds the bigger number and sends back to the node who sent it a winner's vote. The node that collects the majority of the votes will be the one that has the right to add the next block. In order to avoid the loss of time and energy for mining the block, the Proof-of-Luck (PoL) characteristics [43] were used to allow anyone to solve it quickly unlike the Proof-of-Work (PoW) [44].

5.2. Data Sharing

Liu et al. [26] proposed a data-sharing framework that focuses on data protection breaches when sharing data between different government departments and they describe how to protect data breaches during the transaction. Sharing information between nodes is made using private blockchains, this authenticates the nodes on the network and enables them to trust each other. At the same time, it establishes the data's fundamental features and decreases the data framework disorder. The system could also query the data according to the criteria, collects the names of departments that possess the data and exchange the request. The blockchain also sort the aggregated user message and process user data anonymously to ensure anonymity. The data in the blockchain-based privacy framework includes three layers: (1) the database layer, which the primary database that contains the raw data and the privacy database the privacy processed data, (2) the server layer, which processes the data, and (3) the blockchain layer, which stores each node's data directories and the node that possesses the data. After the completion of the procedure, the data

directory will expand and recorded on the blockchain, which they believe it is difficult to have data protection breach. When there is a data request, the first step, is to locate the requested information and sends the request to the node. When the request is accepted, a specific process runs to store the requested data to the privacy server, then the request is confirmed and the data sharing starts. The role of the blockchain is to authenticate each user and prevent the counterfeit of the data. The validation is made using the PoW consensus algorithm.

Ghanem and Alsoufi [27] have used as a case study an e-service provided by the e-government portal through the creation of an interoperable network between involved organisations in the transaction. Their framework facilitates information exchange in G2C, G2B and C2C services and improves their collaboration. The e-government portal provides citizens with an e-Key which is used for requesting services securely and authenticate them. It is the citizens' obligation to maintain their e-Keys. The role of the blockchain is to specify the proper smart contract which is associated with the corresponding service to check for the necessary documentation to complete the requested service. The collection process has to be validated by the citizen. After the essential documents are completed, the smart contract empowers the relevant service provider to collect a copy of the documents in order to complete the operation defined by the smart contract. Once a new document is issued, it is added to the blockchain where all parties of the network need to validate it by the mining process. The initial document will be reserved on the service provider's storage for availability and authenticity for the granted user. Even though all users keep a copy of the ledger they can only preview the document in order to complete the service. On the other hand, citizens will have access to the documents anytime and anywhere since the service is provided on the web and mobile devices. The control of allowing joining nodes for the mining process is made by using a consortium blockchain. For the implementation, an existing platform is considered such as Ethereum or the e-government's network.

Zhang et al. [28] have considered blockchain as the fundamental technology to create a government model for sharing information among different government departments, including fiscal, legal, tax, educational and medical departments, and solve security and reliability problems. The authors set out the implementation strategy based on a consortium blockchain and providing solutions for government information sharing. Blockchain technology is based on a peer-to-peer network, where the content of the nodes is immutable, while using a consensus plugin guarantees the synchronisation of the data, and also ensures the safety of data. The network accomplishes the data synchronisation of the nodes with protocols such as Proof-of-Stake (PoS) or Proof-of-Work (PoW). Information routing is accomplished through consensus and smart contracts. All data sharing information is hashed inside the sharing platform. The blockchain will verify the ciphertext data, while reading the stored information in order to reduce the instability of the node by storing the reading records in order to trace errors when self-audit. Their framework of information exchange uses a three-level software architecture that connects the data and presentation layer through a blockchain-based layer. The data layer contains information stored in a blockchain, such as information exchange using Internet and Internet-of-Things (IoT) devices. The blockchain-based layer scattered storage, smart contracts, consensus algorithm and others combining the data and presentation layer. Finally, the presentation layer is the interface of government service application.

Xu et al. [29] proposed a trusted and flexible Electronic Certificate Catalog Sharing (ECCS) system which is the first analysis solution about electronic certificate register sharing services that differ from other existing discoveries. ECCS segregates the network into a channel where each channel represents authorised participants to access data for the smart contract that have been deployed to the channel. Their scheme designs and simulates a pioneer blockchain system based on a three-level electronic certificate architecture. Therefore, the electronic certificate register sharing system is based on a consortium blockchain that uses smart contracts to record and review every usage of electronic certificate automatically and independently. Therefore, transactions about catalogue sharing or request of electronic

certificates are kept private from other entities which have not joined the channel. In other words, those entities authorised by the ROOT-CA node or intermediate CA node has permission to access the ledger. All Ledger data on each peer is encrypted via file system encryption to achieve the privacy of data related to electronic certificates. Moreover, data that are transmitted among peer nodes, ordering nodes and CA nodes are encrypted via TLS (Transport Layer Security). ECCS builds an access control pattern in the smart contract to restrict data access to certain roles which can meet the requirements for e-government service. Whoever, electronic certificates or catalogue sharing service requests will be added successfully to the blockchain without any human interference. This can provide trusted audit and trace when a dispute occurs. The blockchain-based system is a universal solution for the shared service of the digital certificate. That is to say, entities that want to cooperate on certain business but do not trust each other can use the blockchain-based system to achieve sharing services of data. The implementation was made by using the Hyperledger Fabric to demonstrate the functionality and practicality. The preliminary results showed that the work and functionality could meet all prerequisites of e-government.

Naing [30] proposed a generic model of an open blockchain framework that could be used for all types of e-government services, Government to Employee, Government to Citizens, Business to Business and Government to Government to ensure security, reliability and robustness of the e-government services. The use of a common data framework between all the authorities will also increase interoperability. Previous form the implementation, e-government strategies were reviewed from several other countries in Asia, East Asia and the EU. The proposed generic framework is based on a distributed blockchain with five layers: (1) Development Platform for e-gov services Layer, which includes front-end services and UI, application and data templates. (2) Blockchain Technology Service Layer, this layer is the most important because it includes services such as smart contracts, cryptocurrency, consensus algorithms such as Proof-of-Work (PoW) and Proof-of-Authority (PoA), Cybersecurity and many other services. (3) Data Standardisation and Distribution Layer, in this layer various data from different ministries or authorities are stored. (4) Data Storage Service Layer, this layer supports data centres services. (5) Secure and Distributed Infrastructure Layer, which supports secure communication for the blockchain network.

Elisa et al. [31] proposed a secure and decentralised e-government consortium blockchain-based system that transforms the traditional paper-based data sharing government system to its electronic counterpart that provides services in a friendly environment for citizens and businesses despite their physical location, also to provide convenience, transparency and efficiency and at the same time to improve quality of the e-gov services. The proposed consortium blockchain-based system architecture it consists of four layers, the services access layer, the consortium blockchain layer, the network layer and the ledger storage layer. The services access layer is composed of e-government users and different devices to provide access, and storage of user's credentials. The consortium blockchain layer is a peer-to-peer network of pre-selected e-government nodes for validating transactions and to authenticate users before joining the network. The consortium blockchain layer is also responsible for the communication between nodes, user management and the consensus. The Proof-of-Work consensus algorithm is used on this network. The network layer provides the connection between all layers. The ledger storage layer is used to store out of the blockchain large files such as documents, images or data that is going to be deleted or amended in the future. The necessity of this layer is due to the immutability of the blockchain.

5.3. e-Voting

Hjalmarsson et al. [32] have implemented an e-voting system that uses a permissioned blockchain. To achieve their goals for privacy and security, they have used a Go-Ethereum private Proof-of-Authority (PoA) blockchain. The consensus mechanism is based on the identity as a stake, which helps to deliver transactions faster. Their implementation consists of two types of nodes: District nodes and Bootnote. The first type of node represents the

voting restricts which manages the smart contracts for the voting and the second type of node represents the institutions with private access to the network, this type of node works as a service that helps the district nodes to communicate with each other. Each voter has his identity wallet for each election he/she participates in. For the election, the administrator of the elections creates a ballot smart contract for each corresponding district node, then the voter can start to vote, after the voter places his/her vote the data of the vote is verified by the bulk of the district nodes and the vote is added to the blockchain. For each voting, the voter receives a voting ID which can be used to verify that his/her vote is listed on the blockchain and counted correctly. The voting transaction on the blockchain does not contain any of the voter's data to maintain the privacy requirements. The authors tested their blockchain-based voting system in different blockchain frameworks such as Exonum, Quorum and Go-Ethereum, to decide which implementation was the best solution.

Yavuz et al. [33] have implemented a small scale e-voting system using a private Ethereum blockchain platform, specifically the Rinkeby network for a secure e-voting system that does not allow duplicate votes and it is completely transparent and at the same time protects the voter's identity. The Ethereum blockchain network was suitable for them because all transactions are made in real-time. As an exchange for adding blocks into the ledger, Ethers, Ethereum's digital currency is given to miners for their work of validating and adding blocks to the ledger. The consensus is made using the PoW algorithm. They have used smart contracts to verify and calculate the votes which are written in the solidity programming language, the contracts are run by the nodes every 15 s, and their activation must have at least 2 validations from other nodes. Also, in the voting procedure, Ethereum accounts can be used for the elections which helps not to reveal the voter's identity because it uses hashed values, but this is not enough for personal authentication of voters, it needs additional ways such as multi-factor authentication methods because account authentication is not enough. For a person to vote using his/her Ethereum wallet has to have also a small number of Ethers, to cast a vote. In their paper, they have excluded individual authentication and legal regulations because are considered different sub-cases. As we have mentioned above, their implementation is limited for small scale voting systems, which means, in a larger-scale voting system may appear different problems.

Khan et al. [34] described the evolution of their primary proposed idea published in 2018 for a secure e-voting system [45]. Their proposed e-voting system was deployed using an open-source Multi-chain Blockchain and its version Alpha 4. They selected this specific version because it has new features which helped them to handle a stream of data along with voting. To investigate the impact on the transaction processing time, size, average and maximum number of processed transactions and average block size, they have experimented with three different voting implementation scenarios based on different settings such as how many voters will participate, candidates and if clients will be local or remote. For the first two cases, they used a permissionless blockchain having voters with the ability to mine. The third case is acting for a public voting model, where a permissioned blockchain was used with specified nodes for the mining and validating procedure. Before the voting starts, the voters have to be registered as unique hashes, this procedure helps to maintain voter's privacy. These hashes will be used by voters to transfer their vote. The voter, have the right to receive from the relevant authority a voting token which will use to cast the vote to his favourite candidate to prevent duplicate voting. The votes are stored in the private blockchain as an asset and also stored to an address that works as an authority that transfers votes to the candidates. The validation for the casted votes is succeeded by using the PoW consensus algorithm. The consensus is succeeded from a pool of trusted user that work as miners and they are responsible for accepting or not the voting transaction, if a voting transaction is accepted, then it is being added as a block to the ledger.

5.4. Land Property Services

Alketbi et al. [35] have researched and analysed real estate in Dubai as a case study by identifying the involved entities, exploring the real estate process running in Dubai and also identifying the challenges, the impact of using blockchain technology on the real estate market. In this research, they have used a permissioned blockchain structure for enhancing the transparency of the transactions, minimising the cost and making easier the processes of real estate. During their research, they have based on the Hyperledger Fabric platform and its smart contacts. Since selling or renting land properties includes multiple participants, the main objectives for using blockchain technology in real estate is the automation of the property cycle by using smart contracts, management of digital assets by using tokens for properties and real estate in real-time by having predefined policies for instant settlement of transactions. The main roles of participants in the blockchain network are the network administrator, who configures the network policies and installs the consensus services, the operator node, who is responsible for monitoring and managing consensus in cluster nodes, the architect node, who is responsible for the blockchain architecture, and policies definition, the blockchain administrator node, who is different from the above-mentioned network administrator and it is responsible for administering nodes and their operations, including smart contract installation, and last the developer node, who is responsible for developing applications. Each node in the blockchain can participate in one or more permissioned networks. The blockchain smart contracts run through applications and after succeeded transactions, the ledgers are updated. For the future, they proposed the application of blockchain with an alternative operating model to other governments for improvements.

Nguyen et al. [36] have experimented and evaluated the use of blockchain for issuing land valuation certificates. They have defined a generic blockchain model for managing procedure integrated with the e-government services framework. Before starting the implementation, they explored the current procedures of issuing land valuation certificates and due to the Vietnamese network security law, all datacenters must be settled inside Vietnam, so any permissionless blockchain network would not be proper. Therefore, for their implementation, they have chosen to use Hyperledger Fabric, by setting up a private blockchain network, even though the network is private the land valuation certificates are accessible from a public endpoint of the network. They ended up using Hyperledger Fabric because it is an open source blockchain platform, it can support large consortium and by comparing with other platforms, it has more stable releases. For the data storage they used the InterPlanetary File System (IPFS) [46] and a scalable database for string big data BigChainDB [47]. This implementation is an extension of the main current service for the e-government framework. The land valuation platform includes the following services: identification of users who can interact with the stored data, these are authenticated and authorised by the Ministry of Natural Resources and Environment to sign the digital certificates. Data mapping, this service is responsible to map different types of data into a key-value form. Smart contracts deployment and installation for every type of transaction. Consensus, for the initial state it includes the packing procedure of transactions into blocks before adding them to the ledger, in the future this may change according to new requirements. Monitoring of system health, application operations, system availability and anything else that will prevent any failure of the blockchain. Deployment and configuration of tools for peers. This experiment implementation meets the requirements of current service procedures for issuing land valuation certificates and also helps to digitise at the same time similar procedures.

5.5. e-Delivery Services

Payeras-Capella et al. [37] have presented two different schemes of an e-Delivery service to reduce the participation of third trusted parties in comparison with the up until now approaches without excluding the EU guidelines for e-Delivery systems. The schemes were based on a private and public e-Delivery system using blockchain and smart contracts

to deliver fair exchanges and reduce the role of Trusted Third Parties. Both schemes follow a three-step exchange: at the beginning, the sender sends an encoded message to a group of receivers, following, the receivers have to accept or reject the message, at the final step, the sender completes the transaction by providing the message and the proof of acceptance from the receivers. The main difference between these two schemes is that on the private approach the communication exchange is made off-chain regarding the public solution that the communication exchange is made on-chain. For the implementation of the two schemes, they have used the Ethereum blockchain and its cryptocurrency for the execution of the communication. To maintain security and privacy during the implementation they have used digital signatures, symmetric and public key encryption, key wrapping and hash functions. Both schemes are available on GitHub (https://github.com/secomuib, accessed on 28 April 2021).

5.6. Human Resources Management

Neiheiser et al. [38] presented an architecture which can be applicable to any blockchain network that uses smart contracts. More precisely, they present an Human Resources Management (HRM) system, where its decentralised process assure transparency and protect both members from malevolent actions. The model includes three types of users which can be verified by their public key: The applicant, the reviewer and the institution. Two types of smart contracts are available in the system, the one with a list of all institutions and the other which keeps the job's position information and its status. When an opened job position is published, it creates a smart contract on the blockchain. This helps applicants to see more information for each job position. When applicants are registered they receive information about the progress of the process. There is a list of professional reviewers that the smart contract selects one of them to review the job application. For a new institution to be added as a member of the network, a significant number of accepts is required. To sustain the privacy of the applicants, construction of a semi-permissioned model connected with a permissionless blockchain is used. When an institution opens a job position, it creates and publishes a smart contract to the blockchain. The job position is now available to the applicants to register, after the deadline is reached the job position is no longer available to the applicants, then a reviewer is elected to evaluate the application and to post the results. For the validation of the transactions a Byzantine Fault Tolerant consensus algorithm is used.

5.7. Government Contracting

Diallo et al. [39] proposed the blockchain-based system that allows real-time monitoring analysis of the e-government services and can be apply to any policy for government contracting. This system offers transparency, accountability and better service management. They introduced a generic blockchain framework for applying any policy of government contracting and they consider as a case study the US Small business Administration policy [48]. The blockchain-based system executes all the transaction and publishes the results to the public. They have used a public blockchain network. There are four categories of steps for contracts, preparation and submission, bidding and selection, execution monitoring and auditing. In the beginning, the system validates that a contract is submitted, after the validation is completed the transaction is added to the blockchain, after that comes the bidding step, the validation of the transaction is made using the PoW consensus algorithm. To become a user of the blockchain-based system, the entity must register. When the registration is completed a certificate is issued by the authority as an identity for the system, the certificate is a pair of keys, a private and a public key which is rooted in a digital certificate. For enhancing transparency, the guidelines of how to use and manage the certificate are rooted in a smart contract. All traditional contracts are transformed into smart contracts and translated into the supported language of the system. The generated contract is digitally signed by the issuing authority and shares with the other members of the system's network. The member of the system's network checks if the issued contract is

regulated and digitally signed using the pair of keys. If everything is confirmed, the contract is available to the public, and the offering procedure starts. All interesting parties can prepare a signed proposal and submit it to the system. Each submitted offer is checked by the parties and those offers that satisfy the regulations will be accepted and written to the blockchain. The winning bidder is the one that its offer meets the regulations, at the whole procedure the winner is kept secret until the bidder proceeds to the next step. The final selection's block is added to the blockchain. In the case of public blockchain security issues are raised since the stored data is publicly available, to reduce this concern, all parties in the system network could negotiate to encrypt and protect the sensitive data, but this could lead to the reduction of the government's transparency.

6. Discussion

Initially, the use of the blockchain was limited to financial transactions using cryptocurrencies. Over the years, blockchain features such as transparency, data security in which data amendments are not applicable when they added in the blockchain [49] and also its decentralised network, have attracted the interest of many researchers to adopt blockchain technology in various other areas besides financial transactions. One of these areas is e-governance for better and secure services for citizens, businesses and governments.

We have seen that from 2018 and onward (see Figure 3) the number of papers is increasing significantly. The majority of the proposed blockchain solutions are at an early stage, as a small percentage of them (see Figure 4) have reached the stage of system evaluation or even prototype implementation.

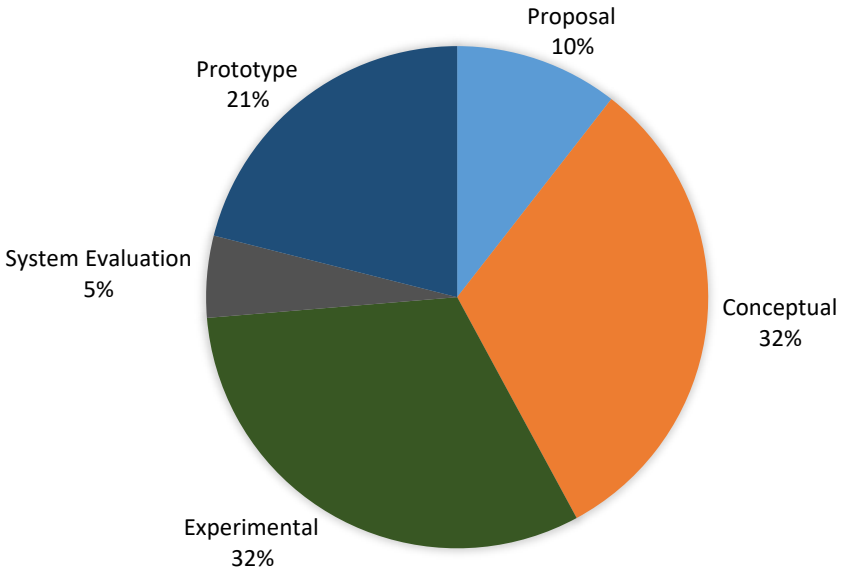

Figure 4. Percentage of maturity provided in the included e-government services.

The bulk of the findings in the conducted review for this paper are related to authentication, data sharing and e-voting services whereas, less of the findings are related to other e-government services. Also, only 4 of the proposed solutions (21%) were implemented as prototypes and on average the maturity of all solutions was between conceptual and experimental level (2.89) (more details in Figure 5).

Our findings show that blockchain as a novice technology in e-government services needs more research for improvement. Most of the studies and their corresponding implementations mainly focuses on security issues as opposed to privacy preservation which needs to be further studied, taking into account the GDPR and the limitations of public data. However, other issues that have to consider when adopting blockchain technology in e-gov services are the integration with other technologies. Such as data storage for reserving files (i.e., certificates and other public documents).

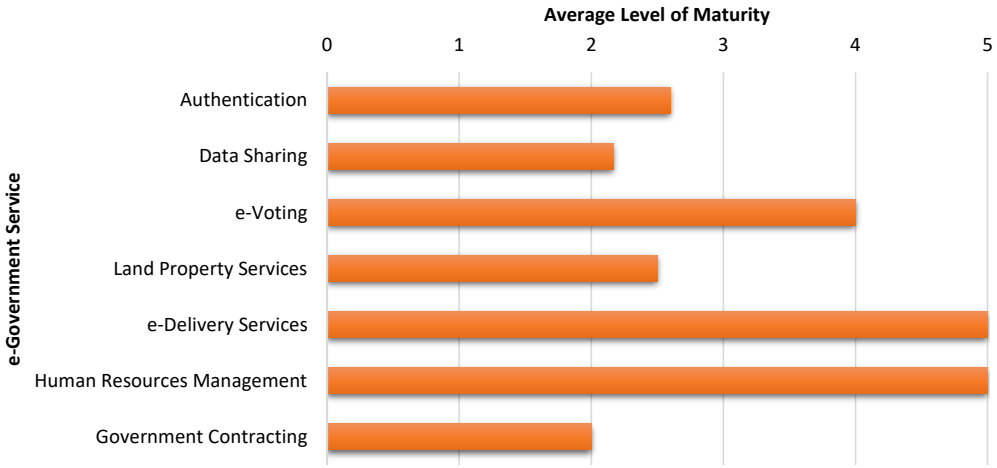

Figure 5. Average level of maturity per e-government service (1 = proposal, 2 = conceptual, 3 = experimental, 4 = system evaluation, and 5 = prototype).

We believe that in the upcoming years there will be an increase in research into e-government services using blockchain technology, as improvements are made to existing blockchain platforms or new ones are developed. The transactions are executed using the minimum computing resources through smart contracts, in contrast to other consensus mechanisms. As a future direction, we believe that it would be useful to create a unified architecture of a blockchain network in which services can be easily integrated without limiting the number of services provided on the network. To this end, the European Union has already stepped up its efforts to digitally transform the public sector [50] by building a pan-European public service blockchain for creating trust in data, allowing citizens and organizations to trust each other to collectively agree without a third-party authority. This effort includes environmental sustainability, data protection, digital identity, cybersecurity and interoperability.

Our main goal is to do a literature review and capture the state-of-art of the use of blockchain technology in e-government services for scientific journals, conference, etc. However, we have not included whitepapers, grey literature, reports, etc., and it is clear that not all of the solutions are being recorded in our work and there might be more available solutions already implemented and in production that are not published in a scientific journal or conference proceedings, such as the projects of the European Blockchain Service Infrastructure (EBSI). The European Union Member States and the European Union Commission have joined forces and formed the European Blockchain Partnership (EBP) and built the EBSI for the creation of cross-border services for public administrations, to verify information and make services trustworthy using blockchain.

7. Conclusions

With the expansion of blockchain technology in areas other than cryptocurrencies, the research efforts have been radically expanding during the past years. Blockchain technology is considered as a revolutionary approach in the area of public services and e-governance, and acts as an enabler for citizens, businesses and governments to easily interact with each other in a transparent way. Its innovation comes from the combination of transparency, integrity, confidentiality and accountability, when accurately designed. Moreover, a distributed blockchain network enhances trust among all participants, as transactions are executed securely without the approval of a central authority.

In this paper, we have conducted a two-level screening process using eligibility criteria to narrow down the results and gain insight into our research questions regarding the use of blockchain in e-government services. Having presented the findings of our research, we have recorded the maturity level of the solutions using blockchain technology in e-government services. The results of our research have been grouped chronologically

according to the type of service, comprising details regarding the blockchain characteristics, the maturity level of the solution and the case study.

Blockchain as a disruptive technology has the potential to significantly contribute towards more robust and transparent e-government services. Research activities in the field have to be intensified and more results have to be produced to draw safe conclusions with regards to the most viable and sustainable blockchain-enabled e-government services.

Author Contributions: Conceptualization, G.D. and K.R.; methodology, G.D. and K.R.; validation, I.L., G.D. and K.R.; formal analysis, I.L., G.D. and K.R.; investigation, I.L., G.D. and K.R.; data curation, G.D.; writing—original draft preparation, I.L.; writing—review and editing, G.D. and K.R.; visualization, I.L.; supervision, G.D. and K.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would also like to thank the MPhil program "Advanced Technologies in Informatics and Computers", Department of Computer Science, International Hellenic University, for facilitating this research study.

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

References

1. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; Technical Report NIST IR 8202; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
2. European Parliament and Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 9 May 2021).
3. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 9 May 2021).
4. Konashevych, O.; Poblet, M. Is blockchain hashing an effective method for electronic governance? *Front. Artif. Intell. Appl.* **2018**, *313*, 195–199. [CrossRef]
5. Zein, R.M.; Twinomurinzi, H. Towards Blockchain Technology to Support Digital Government. *Electronic Government and the Information Systems Perspective*; Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 207–220. [CrossRef]
6. Pîrlea, G.; Sergey, I. Mechanising Blockchain Consensus. In Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2018, Los Angeles, CA, USA, 8–9 January 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 78–90. [CrossRef]
7. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 3–16.
8. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Niyato, D.; Nguyen, H.T.; Dutkiewicz, E. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access* **2019**, *7*, 85727–85745. [CrossRef]
9. Allessie, D.; Sobolewski, M.; Vaccari, L.; Pignatelli, F. (Eds.) *Blockchain for Digital Government: An Assessment of Pioneering Implementations in Public Services*; Technical Report JRC115049; European Commission, Joint Research Centre: Luxembourg, 2019. [CrossRef]
10. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. 2014. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 9 May 2021).
11. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187. [CrossRef]
12. Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger* **2019**, *4*. [CrossRef]
13. Ølnes, S.; Jansen, A. Blockchain Technology as Infrastructure in Public Sector: An Analytical Framework. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, DG.O '18, Delft The Netherlands, 30 May 2018–1 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–10. [CrossRef]

14. Ølnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–364. [CrossRef]
15. Franciscon, E.A.; Nascimento, M.P.; Granatyr, J.; Weffort, M.R.; Lessing, O.R.; Scalabrin, E.E. A Systematic Literature Review of Blockchain Architectures Applied to Public Services. In Proceedings of the IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal, 6–8 May 2019; pp. 33–38. [CrossRef]
16. European Commission. *eGovernment Benchmark Framework 2012–2019: Method Paper for the Benchmarking Exercises (Comprehensive Rules from 2012 to 2019)*; Publications Office of the EU: Luxembourg, 2019; pp. 1–72. [CrossRef]
17. European Commission. *eGovernment Benchmark 2020: eGovernment That Works for the People: Background Report*; Publications Office of the EU: Luxembourg, 2020; pp. 1–199. [CrossRef]
18. European Commission. *eGovernment Benchmark 2020: eGovernment that Works for the People: Insight Report*; Publications Office of the EU: Luxembourg, 2020; pp. 1–49. [CrossRef]
19. Batubara, F.R.; Ubacht, J.; Janssen, M. Challenges of Blockchain Technology Adoption for E-Government: A Systematic Literature Review. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, DG.O '18, Delft, The Netherlands, 30 May 2018–1 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–9. [CrossRef]
20. Alexopoulos, C.; Loutsaris, M.A.; Charalabidis, Y.; Androutsopoulou, A.; Lachana, Z. Benefits and Obstacles of Blockchain Applications in e-Government. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Grand Wailea, Maui, HI, USA, 8–11 January 2019; p. 10.
21. Chen, Y.; Dong, G.; Bai, J.; Hao, Y.; Li, F.; Peng, H. Trust Enhancement Scheme for Cross Domain Authentication of PKI System. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 17–19 October 2019; pp. 103–110. [CrossRef]
22. Khan, S.N.; Shael, M.; Majdalawieh, M. Blockchain Technology as a Support Infrastructure in E-Government Evolution at Dubai Economic Department. In Proceedings of the 2019 International Electronics Communication Conference, IECC'19, Okinawa, Japan, 7–9 July 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 124–130. [CrossRef]
23. Batubara, F.R.; Ubacht, J.; Janssen, M. Unraveling Transparency and Accountability in Blockchain. In Proceedings of the 20th Annual International Conference on Digital Government Research, DG.O 2019, Dubai, United Arab Emirates, 18–20 June 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 204–213. [CrossRef]
24. Pinter, K.; Schmelz, D.; Lamber, R.; Strobl, S.; Grechenig, T. Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms. In Proceedings of the Business Process Management: Blockchain and Central and Eastern Europe Forum, Vienna, Austria, 1–6 September 2019; Di Ciccio, C., Gabryelczyk, R., García-Bañuelos, L., Hernaus, T., Hull, R., Indihar Štemberger, M., Kő, A., Staples, M., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 361, pp. 151–165. [CrossRef]
25. Páez, R.; Pérez, M.; Ramírez, G.; Montes, J.; Bouvarel, L. An architecture for biometric electronic identification document system based on blockchain. *Future Internet* **2020**, *12*, 10. [CrossRef]
26. Liu, L.; Piao, C.; Jiang, X.; Zheng, L. Research on Governmental Data Sharing Based on Local Differential Privacy Approach. In Proceedings of the 2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), Xi'an, China, 12–14 October 2018; pp. 39–45. [CrossRef]
27. Ghanem, M.E.; Alsoufi, A. Interoperable Framework to Enhance Citizen Services in the Kingdom of Bahrain. In Proceedings of the International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 22–23 September 2019. [CrossRef]
28. Zhang, Y.; Deng, S.; Zhang, Y.; Kong, J. Research on Government Information Sharing Model Using Blockchain Technology. In Proceedings of the 10th International Conference on Information Technology in Medicine and Education (ITME), Qingdao, China, 23–25 August 2019; pp. 726–729. [CrossRef]
29. Xu, C.; Yang, H.; Yu, Q.; Li, Z. Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain. In Proceedings of the IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019; pp. 1237–1242. [CrossRef]
30. Naing, T.T. Initiation of Blockchain Technology based Open Framework for e-Government Development in Myanmar. In Proceedings of the Myanmar Universities' Research Conference (MURC 2019), Yangon, Myanmar, 24-25 June 2019; pp. 1–7.
31. Elisa, N.; Yang, L.; Li, H.; Chao, F.; Naik, N. Consortium blockchain for security and privacy-preserving in E-government Systems. In Proceedings of the International Conference on Electronic Business (ICEB), Newcastle Upon Tyne, UK, 8–12 December 2019; pp. 99–107.
32. Hjalmarsson, F.P.; Hreioarsson, G.K.; Hamdaqa, M.; Hjalmtysson, G. Blockchain-Based E-Voting System. In Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 983–986. [CrossRef]
33. Yavuz, E.; Koc, A.K.; Cabuk, U.C.; Dalkilic, G. Towards secure e-voting using ethereum blockchain. In Proceedings of the IEEE 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–7. [CrossRef]
34. Khan, K.; Arshad, J.; Khan, M. Investigating performance constraints for blockchain based secure e-voting system. *Future Gener. Comput. Syst.* **2020**, *105*, 13–26. [CrossRef]

35. Alketbi, A.; Nasir, Q.; Abu Talib, M. Novel blockchain reference model for government services: Dubai government case study. *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 1170–1191. [CrossRef]
36. Nguyen, N.H.; Nguyen, B.M.; Dao, T.C.; Do, B.L. Towards Blockchainizing Land Valuation Certificate Management Procedures in Vietnam. In Proceedings of the International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 14–15 October 2020; pp. 1–6. [CrossRef]
37. Payeras-Capella, M.M.; Mut-Puigserver, M.; Cabot-Nadal, M.A. Blockchain-Based System for Multiparty Electronic Registered Delivery Services. *IEEE Access* **2019**, *7*, 95825–95843. [CrossRef]
38. Neiheiser, R.; Inacio, G.; Rech, L.; Fraga, J. HRM Smart Contracts on the Blockchain. In Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; IEEE Computer Society: Los Alamitos, CA, USA, 2019; pp. 1–6. [CrossRef]
39. Diallo, N.; Shi, W.; Xu, L.; Gao, Z.; Chen, L.; Lu, Y.; Shah, N.; Carranco, L.; Le, T.C.; Surez, A.; et al. EGov-DAO: A Better Government using Blockchain based Decentralized Autonomous Organization. In Proceedings of the 5th International Conference on eDemocracy and eGovernment (ICEDEG), Ambato, Ecuador, 4–6 April 2018; pp. 166–171. [CrossRef]
40. Munoz, J.L.; Forné, J.; Esparza, O.; Soriano, B.M. Using OCSP to secure certificate-using transactions in M-commerce. In Proceedings of the International Conference on Applied Cryptography and Network Security, Kunming, China, 16–19 October 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 280–292.
41. Lin, J.; Yu, J.; CAO, Z.; FENG, D. Implementation of Highly Efficient OCSP Server. *Comput. Eng.* **2005**, *31*, 74–76.
42. Moyano, J.P.; Ross, O. KYC optimization using distributed ledger technology. *Bus. Inf. Syst. Eng.* **2017**, *59*, 411–423. [CrossRef]
43. Milutinovic, M.; He, W.; Wu, H.; Kanwal, M. Proof of Luck: An Efficient Blockchain Consensus Protocol. In Proceedings of the 1st Workshop on System Software for Trusted Execution, SysTEX '16, Trento, Italy, 12–16 December 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 1–6. [CrossRef]
44. Nguyen, G.T.; Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128. [CrossRef]
45. Khan, K.M.; Arshad, J.; Khan, M.M. Secure digital voting system based on blockchain technology. *Int. J. Electron. Gov. Res. (IJEGR)* **2018**, *14*, 53–62. [CrossRef]
46. Nyaletey, E.; Parizi, R.M.; Zhang, Q.; Choo, K.R. BlockIPFS—Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability. In Proceedings of the IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 18–25. [CrossRef]
47. McConaghy, T.; Marques, R.; Müller, A.; De Jonghe, D.; McConaghy, T.; McMullen, G.; Henderson, R.; Bellemare, S.; Granzotto, A. *BigchainDB: A Scalable Blockchain Database*; White Paper; BigChainDB: Berlin, Germany, 2016; pp. 1–66.
48. Denes, T.A. Do Small Business Set-Asides Increase the Cost of Government Contracting? *Public Adm. Rev.* **1997**, *57*, 441–444. [CrossRef]
49. Oliveira, T.; Oliver, M.; Ramalhinho, H. Challenges for connecting citizens and smart cities: ICT, e-governance and blockchain. *Sustainability* **2020**, *12*, 2926. [CrossRef]
50. Baldacci, E.; Frade, J.R. Advancing Digital Transformation in the Public Sector with Blockchain: A View from the European Union. In *Disintermediation Economics: The Impact of Blockchain on Markets and Policies*; Kaili, E., Psarrakis, D., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 281–295. [CrossRef]