Beyond the Hype: Distributed ledger technology in the field of public administration

Preprint · March 2018

DOI: 10.13140/RG.2.2.26483.43042

2 authors, including:

Niklas Kossow
Hertie School of Governance
5 PUBLICATIONS **2** CITATIONS

SEE PROFILE

- DRAFT -
Beyond the Hype

Distributed ledger technology in the field of public administration

Niklas Kossow *
&
Victoria Dykes †

April 3, 2018

Following the increasing attention the topic received over the last years, this paper is looking at the use of distributed ledger technology (DLT) in public administration and, in particular at its most prominent example: Blockchain technology. While offering a gentle introduction to the topic, the paper establishes an overview of the attributes and potential use cases of DLT in the context of public administration and bureaucracies. As a technology establishing a decentralised, high-trust data management system, DLT has potential to be used for the storage of administrative data and for increasing the effectiveness and efficiency of administrative data management. While potential uses are wide-ranging, this paper offers a simple typology of these. Furthermore, it offers a critical view of the challenges and drawbacks that the technology currently poses to public officials looking at using DLT in their processes. Ultimately, this paper takes the view that DLT can be a potentially valuable tool for public administrations to make use of, but the drawbacks and difficulties associated with this technology are often not discussed or acknowledged as often or as thoroughly as needed, giving a false picture of how easy it would be for governments to use this technology successfully.

Keywords: distributed ledger technology; blockchain; data mangement; public administration; bureaucracy; state capacity.

*PhD Candidate, Hertie School of Governance, kossow@hertie-school.org
†Researcher, Technologiestiftung Berlin, dykes@technologiestiftung-berlin.de

1 Introduction

In 2017, the hype surrounding blockchain technology reached a new high. While the prices for bitcoin arguably the most successful digital currency to date were soaring, many people began thinking about new ways to use its underlying technology: blockchain. The excitement surrounding the technology became indeed so big that adding the term to the title of a company was able to rise its stock price more than threefold (Pal 2018). This enthusiasm has also reached the field of public administration, as governments and analysts alike hail the possibilities that the technology holds for bureaucratic processes. While Estonia embraced blockchain technology early on, other countries have followed their example over the last couple of years: the UK government published studies on it and started their pilots in 2016 (Walport 2016), the Dutch government supported a broad range of projects[1] and the Lithuanian government recently launched a dedicated platform to support start-ups in this context (Higgins 2018). Governments are eagerly watching the space - the European Commission (2018) even launched a blockchain observatory.

Blockchain is a type of distributed ledger technology (DLT). While the disambiguation of this term will be discussed below, this paper will use blockchain technology and DLT largely interchangeably, as almost all DLT use cases to date use some form of blockchain. The lack of successful use cases is indeed a challenge when analysing the potential of DLT. Many applications are still in their proof-of-concept phase, and very few have been rolled out in full scale. This is especially true for the field of government and public administration. The aim of this paper is to sift through information on current applications of DLT in this field. In doing so, we want to show both the potential of DLT, but also provide a sober view on its challenges and applicability in the context of public administration. This paper provides both a starting point for the coming research on the usability of blockchain in the governmental context and a realistic counter view to publications claiming that blockchain will revolutionise just about everything.

To build its argument, the paper will rely on an analysis of primary literature and project description on relevant DLT projects in the context of public administration. It will supplement this with data collected in a series of expert interview from the field of blockchain and public administration respectively. The paper will offer a brief literature review, as well as an explanation on the functioning of blockchain technology and its particular attributes. It will show the potential of these attributes and functionalities for different applications in the context of public administration and provide a classification of these based on current use cases and ongoing projects. Having highlighted the potential of the technology and the positive effects assigned to it, the paper will go on to offer an extensive discussion on the drawbacks and challenges of DLT use in public administration. Weighing this optimistic and the more sceptical point of view up against each other, the paper wants to provide a realistic assessment of DLT use in public administration.

[1] See: `https://www.blockchainpilots.nl/home-eng`

2 Research Approach & Literature Review

As solid academic work on used cases is still hard to find, this paper wants to lay ground for an an analysis of the use of blockchain in public administration. For this purpose, it will first provide a brief review of literature by looking at which academic works have already considered the idea of using DLT in the context of public administration or governmental work. In doing so it will argue for a gap in literature and a more realistic assessment of the potential of DLT in this field.

Building on this literature, this paper will analyse data provided by three sources. First, it considers several non-academic reports, primarily by private companies and key actors in the blockchain field. It also takes into account website and blog entries, as well as discussions on platforms such as *Reddit*. As DLT is still in its cradle, these are the most reliable first-hand resources providing information on the development of this technology. Developers exchange views and ideas through white papers, blog posts and forums. Private companies, in particular large consultancies, analyse the market and publish information for their customers. As such, analysing these data sources provides a good starting point for this paper and provide a good overview of use cases which are still mostly in its proof-of-concept phase.

Second, the paper looks at documented use cases of DLT in the context of public administration. In doing so, we rely on our own research, examples illustrated in the resources outlined above and use cases listed in an ongoing collection effort of Stanford University students collecting examples of DLT use cases in the context of international development, many of which touch upon functions of public administration.[2]

Furthermore, we conducted several semi-structured qualitative interviews with experts in the field. Interview partners were public administration practitioners, in particular those dealing with innovation and technology, as well as DLT specialists from a variety of companies and backgrounds and public administration experts. Taking into account this variation of experts helps this paper to provide a wide perspective and strike a balance between appreciation for the opportunities offered by DLT and a healthy scepticism with regards to the feasibility of the implementation of this technology.

2.1 Review of literature

As it was already pointed out above, the body of academic literature on use cases DLT and blockchain technology is, so far, rather small. It becomes even smaller when going away from the context of digital currencies and their implementation and when taking a focus on public administration and government services. The larger body of research is published in the form of reports. Yet, we will start by providing a brief review of the

[2]This information is collected via crowdsourcing using a Google spreadsheet: `https://docs.google.com/spreadsheets/d/14BPQIqnDUTyinkp9eJ7bwYwsg22RJz0AVU9vOSSU94o/edit\#gid=1835238919`

academic literature at hand in order to argue why there is a need for further research on the topic.

An early seminal text on the uses of blockchain technology that goes beyond bitcoin is (D. Tapscott and A. Tapscott 2016). Their book *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world* provides a good introduction to the technology as well as a large variety of use cases. D. Tapscott and A. Tapscott also extensively look at uses of DLT in the context of government, providing insights into potential applications and early experiences. It is notable that they are looking both at financial services and fields such as the internet of things, before turning to government. Here they do not go into many details, but rather provide an overview of potential use of blockchain in service delivery and in the context of democratic elections. In the final part of their book, D. Tapscott and A. Tapscott give a decent overview of limitations and argue that blockchain, for numerous reasons, is not ready yet. Still, the tone of their work remains very enthusiastic about the potential of DLT.

Even more convinced of the potential of blockchain technology is Atzori (2015). He considers the argument that blockchain technology might enable decentralised governance, making centralised state institutions irrelevant in the long run. His overall argument runs against this claim, asserting that state institutions are here to stay. Yet, his opinion remains that blockchain might contribute to the decentralisation of the state. A fairly concise overview of DLT applications in financial and non-financial areas is provided by Crosby et al. (2016). They strike a fairly balanced tone which remains optimistic about the disruptive nature of the technology. Non-financial applications also include several potential use cases in public administration. Crosby et al. stress the obstacles that are in the way of wide-scale adoption of blockchain technology and predict a slow adoption rate that will take 10-20 years. An even shorter overview of financial and non-financial applications of blockchain technology is provided by Nofer et al. (2017). They call for some caution, but overall also argue that blockchain technology is likely to disrupt an array of industries, including government. Meijer (2016) analyses the UK governments approach to blockchain technology and lauds it for its balanced approach of non-excessive regulation of the space while recognising the potential of blockchain technology. Davidson, De Filippi, and Potts (2016) argue that blockchain is even more than just a disruptive new technology. They call it an "institutional technology of governance" (ibid., p. 2) and liken its implications to "the invention of the joint stock company" (ibid., p. 24).

Interesting contributions to the field are provided by Svein Ølnes. Ølnes, Ubacht, and Janssen (2017) provide a critical assessment of the potential of blockchain applications in e-government. They argue for a need-driven rather than a technology-driven approach in the application of blockchain technology and point at the exaggerated expectations for the impact of the technology. Their paper provides a great overview of literature and of the different benefits and promises assigned to blockchain technology in government. They also distinguish between governance of the blockchain technology, referring to the determination how the technology operates and how users can engage with it, and governance by blockchain, meaning the use of DLT in government work and the provision of

a blockchain architecture by the government (Ølnes, Ubacht, and Janssen 2017, pp. 4-5). Ølnes and Jansen (2017) analyse the use of blockchain in as an underlying technology for e-government provision. They argue that there is potential to use blockchain in a wider field of government applications and that it is already suitable for use in the authentication of many types of persistent government documents. Ølnes (2016) provides a type of meta-study, reviewing literature on blockchain in the context of e-government. He argues that the technology holds potential, but that it is widely under-researched in its application to e-government. A similar meta-study is put forward by Yli-Huumo et al. (2016) who look more generally at the research provided on blockchain technology. They find that the majority of research still focuses on the bitcoin system and only increasingly looks at other blockchain applications. Their paper gives a comprehensive overview of the challenges in applying blockchain to a bigger variety of applications and outline a research agenda to address these challenges and monitor use-cases. Finally, Glaser (2017) provides an ambitious ontology to introduce a common terminology, core concepts and features of blockchain technology. While not directly dealing with the context of public administration and government, his paper still provides a good starting point for research into blockchain applications.

Academically, this paper wants to build upon these previous research items. It wants to give a realistic and sober assessment of the use of DLT in public administration. It thus provides both a perspective on the potential of DLT, but also extensively discusses challenges and pitfalls in the introduction of this technology in the field of public administration. As it was pointed out above, the body of research published in non-academic publications will feed into this analysis and was thus not considered in the literature review above. Having laid the foundations for our analysis, we will now go on to look closer at DLT itself, its attributes and potential, as well as potential and actual use cases.

3 Defining Blockchain and different types of DLT

The concept of blockchain technology was first published as part of the bitcoin white paper by Satoshi Nakamoto (2008). While it is still unknown who exactly Satoshi Nakamoto is, the technology has by now been much more widely used.

Digital currencies face the crucial question of how to avoid their value being spent twice at the same time. How can trust in the value of a currency be established? The blockchain was designed to solve this double spending problem without relying on a trusted third party. It introduces a storage system which, rather than storing data on a centralised server, stores them in a type of decentralised, distributed ledger. A blockchain is thus also referred to as a type of distributed ledger technology (DLT). This is why this paper will refer to this technology primarily under the DLT umbrella term. However, in order to create an understanding of its functioning and how DLT is seen as a relevant technology for public administration, we will first describe the way blockchain technology works and how it can be distinguished from other DLT.

Data on the blockchain is stored on a decentralised computing system that consists of nodes communicating with each other. Data that is stored on the blockchain is simultaneously stored on all devices within the system that function as full nodes. These can be any type of device with an IP address able to run a program that validates transactions on the blockchain (Drake 2017). Data on these nodes is stored in blocks. These were conceived to store data on bitcoin transactions. However, these blocks can in theory store any kind of data, which is why the applications of blockchain technology can be so varied (Walport 2016).

Blocks contain a full history of the data that was stored on them. Each new block of data is linked to the previous block, creating a chain of information: the blockchain. The process of storing data on the blockchain is automated and follows specific rules. Each block is time-stamped and cryptographically sealed. This means that data entered onto the blockchain can be traced back to the exact moment that it was entered and it can not be altered later on. This process uses the SHA-256 hash algorithm. It creates a hash of the transaction: a fixed-length string of text that uniquely represents the data at hand at the exact instant in which the hash was created. Even small changes to the data and a re-application of the hash algorithm would generate a different hash value. The hash of the previous block is included in each newly written block. Tempering with the data would thus be immediately noticed, as hashes would not match up any longer.

To enable the process of linking subsequent blocks, a validation system needs to be established in order to verify that the data is properly stored on the distributed ledgers. This process is referred to as a distributed consensus process (Crosby et al. 2016). The most common of these processes, also applied within the bitcoin blockchain, asks for a provision of a proof-of-work. The hash of each block contains information on the data stored within the block, and also a cryptographic puzzle. This needs to be solved in order to link a new block to a previous block. This requires a certain amount of computing power and effort on behalf of those who want to store data on the blockchain. While the cryptographic puzzle is hard to solve, it can easily be verified: this makes it possible for other participants within the system to verify transactions. Transactions are accepted if they are verified by 51% of all nodes. The process of adding new data to the blockchain is referred to as mining, to reflect that a considerable amount of computing power is needed for it and as digital currencies are distributed as reward for the creation of a new block (Nakamoto 2008). The difficulty of the proof-of-work that has to be provided is automatically adjusted. This makes sure that the number of blocks that can be written stays roughly constant, no matter how many miners participate in the system. In the case of the bitcoin blockchain, a new block can be written every ten minutes.

Proof-of-work algorithms are seen as a secure way to link subsequent blocks and to choose who gets to write these. This is determined by who solves the given cryptographic puzzle first. However, the proof-of-work process also has significant drawbacks: it requires a lot of computing power and thus very high energy consumption, especially with an increasing number of participants in the distributed network (O'Dwyer and Malone 2014). This also creates problems of scalability, as in the bitcoin blockchain, for instance, the time in

which a new block can be added (the block time) and the size of the block are limited. Some blockchain projects thus try to address this problem by increasing block size and aiming for a much shorter block time. Others are trying to use another distributed consensus algorithm altogether. The most well-know attempt in this context is the application of a proof-of-stake algorithm. Here, the participants in the process are called validators. They have to show that they own a certain economic stake in the system, through the digital currency that the system uses. If they do, their assets get locked. If the validator is chosen to add a block to the blockchain, their stake in the system is released together with an interest rate. Most notably, Ethereum, one of the most important and largest public blockchains, announced that they will switch to a proof-of-stake process (Etherum 2018). While many still see problems and vulnerabilities in this new distributed consensus, other highlight the increased scalability and decreased energy use of this approach (Alkan 2017).

Distributed consensus algorithms seem like a complex way of adding data. But it is important to remember that these methodologies have been explicitly designed to ensure that data on the blockchain can be trusted. Once data is successfully entered onto the system, it can be traced back to the point of entry, it cannot be changed later on and it can be verified by all participants in the system. All of these effects are reached without relying on one intermediary and thus the technology avoids one central point of failure. In the development of blockchain technology, the establishment of trust in the data stored on the blockchain was key. It ensured that users can put their trust into bitcoin and thus assign value to it. However, the different attributes that blockchain technology has also have potential positive effects in context far beyond the creation of digital currencies. Before looking in more detail at these attributes, we will first look at distinguish different types of blockchains and other DLT applications.

3.1 From the bitcoin blockchain to distributed ledger technologies

The bitcoin blockchain, as it was described above, is a type of distributed ledger technology referred to as a *public blockchain*. A public blockchain means that, technically, everybody in the world can participate read a blockchain, send transactions to the blockchain, and expect these transactions to be included. Anyone can participate in the consensus process as described above, and no one can be excluded. In a way, this fact democratises the data storing process of public blockchains: it is available to everyone who has the processing power to participate. Entry hurdles are fairly low. Yet, as pointed out above, public blockchains also have significant drawbacks: with many people participating and an increasing number of nodes and blocks, they become hard to manage. They have an enormous energy consumption and high costs. Also, as some data stored on the blockchain might be sensitive (even if encrypted), they raise questions of data security.

Consortium blockchains[3] are distributed ledgers with a fixed or limited number of nodes

[3]These are also called to as permissioned blockchains, in contrast to permissionless public blockchains. In permissioned blockchains, the owner of the blockchain controls who is permitted to write and read

who can participate in the system. These are usually implemented by a limited number of organisations who take part in the system. Examples for these are consortia of banks who cooperate to implement blockchain technology for financial services. Here, the right to read a blockchain might be public, while the right to write on it may not. The ledgers are thus still decentralised, even though only partially. Yet, energy consumption and costs are considerably reduced (Buterin 2015).

Private blockchains are limited to one organisation or entity. It still uses several devices to store data, rather than relying on a centralised server. However, one organisation controls who can read and write data on the blockchain. While this can provide an effective database solution, it also removes some of the key attributes assigned to blockchain technology, which we will discuss further below (Berke 2017).

More recent DLT projects are looking to remove the concept of blocks altogether. IOTA promises to store data in a network referred to as the tangle. While still functioning as a distributed ledger, it stores data in a directed acyclic graph and simplifies consensus algorithms. It is thought to serve especially applications in the field of the so-called internet of things, but has not yet been brought to market (Popov 2017).

4 How and why use blockchain for public administration?

The above description of the functioning of blockchain technology already highlighted some of the attributes generally assigned to DLT. These are outlined below and summarised in Table 1.

Arguably the most important feature of DLT is its decentralised nature and the resulting *disintermediation*. DLT directly connects all users in its network. It does not rely on one centralised server system or one authority to verify and confirm transactions. Its consensus-building process, as described above, enables transactions and data to be recorded in a decentralised fashion while establishing trust in the system and thus the data stored within it. Disintermediation results in two key attributes assigned to DLT:

- *Security*: avoiding a trusted third party and a single point of failure through decentralisation provides a substantial increase in security with regards to storing transactions. We can differentiate between two different types of security provided by DLT. *Internal security* refers to how DLT in cases of both private and public blockchains prevents participants in the network from tampering with transactions and changing data entries without being noticed. It thus provides protection against fraud. We also see increased *external security*, as distributed ledgers are

data and transactions on the blockchain.

less vulnerable to outside attack, such as distributed denial of service (DDoS) attacks (Rodrigues et al. 2017).[4] Similar to internal security, external actors would find it almost impossible to tamper with data without being noticed. Of course, the system still depends on accurate data being entered onto the blockchain in the first place, an issue that is also true for other data storage solutions.

- *Efficiency*: removing a third party and thus the middle-man makes it possible to create a direct link between two or more participants in the respective DLT environment. This can lead to significantly faster transaction rates as data is immediately shared and stored on all participating nodes. This can also lead to lower transaction costs, as in theory, no intermediary needs to be paid for its services. To date, however, these effects are limited in the context of public blockchains. Both bitcoin and ethereum, arguably the most important blockchains to date, experienced slow transaction rates in times of strong demand. Bitcoin transactions also became increasingly expensive throughout 2017, as more and more transactions were recorded (Lee 2017). Efficiency gains could potentially increase with more efficient distributed consensus algorithms in the context of consortia or private blockchains that limit the number of full nodes within the system.

Another important attribute of DLT applications is the *immutability* of data and transactions stored on the distributed ledgers. In the case of blockchains, every block that is written is cryptographically sealed and time stamped. This makes it possible to track all data entries to who entered data onto the blockchain and when data this was done; it also prevents data from being changed at any later point. This contributes to idea of security highlighted above. Due to immutability, data and transactions cannot be tampered with once they have been successfully recorded on the blockchain. This contributes to another important attribute:

- *Accountability*: a common misconception about DLT is that it anonymises transactions. This contributed to fears that digital currencies can be used for crime and even to finance terrorism. For some digital currencies and their underlying blockchains this is true. ZCash or Monero are designed to keep users anonymous.[5] However, generally speaking, DLT does not anonymise users, but in most cases offers pseudonyms to them. Transactions can thus be assigned to the device and/or the person who entered specific data to a specific block at a specific time (Woodward 2016). This, of course, depends on the design of the DLT system. If designed correctly, DLT thus has the potential to increase accountability in data storage. A full record of all transactions is kept, including information on who added data or transactions to the blockchain. In the case of fraudulent data, it is possible to

[4] DDoS attacks are coordinated attacks of a large number of computing devices who all try and access a service (often an internet server) at the same time, causing it to crash due to the overload and thus making its data unavailable.

[5] The degree of anonymity of these, and other digital currencies, is a subject of debate in many online forums. See for instance: `https://www.reddit.com/r/Monero/comments/7ongx5/is_monero_truly_100_anonymous/`.

trace who provided this data. Depending on the design of the blockchain application, attribution and thus accountability can be easier in consortia or private blockchains.

Another related attribute of blockchain technology is transparency. All nodes within DLT systems can at least read the data stored in the blockchain. In its initial conception, the bitcoin blockchain was specifically designed to be transparent and open to the public. Everybody was supposed to be able to participate in blockchain transactions either by writing onto the blockchain or by reading and thus monitoring transactions on the blockchain. In this sense, using DLT can thus increase the inclusiveness of data storage (Maupin 2017). Rather than making potential participants in a data storage system reliant on one intermediary, they can all participate in the system themselves. This also has potential implications for the governance of DLT systems. It is possible to democratise governance of DLT systems and let participants vote on critical decisions within the system (Atzori 2015). Naturally, these attributes are less pronounced in consortium blockchains and even more so in private blockchains. Transparency and inclusiveness only extend to those who are able to write and/or read data and transactions on the blockchain. In the case of consortia, however, blockchains can increase transparency and inclusiveness between different parties taking part in the DLT data storage system.

Due to these attributes, blockchain is seen to have a potential impact on public administration and provide a variety of use cases. Two key added benefits can be identified in this context:

As it was already pointed out above, DLT potentially offers significant efficiency gains. These are particularly pronounced in the context of recorded cross-border transactions, which in many cases are still highly reliant on third party intermediaries (Guo and Liang 2016). Even within a given country, however, blockchain technology can help improve data sharing and entry from different constituencies or different participating government agencies. This has a significant potential for cost savings and efficiency gains, as security concerns are moved into the background. Another concept that is frequently brought up in this context are smart contracts. These are self-enforcing contracts that are automatically executed when the terms of the contract are met (Walport 2016). Governments might use smart contracts for executing payments or enforcing actual contracts, for instance in the context of public procurement. They can also be used to regulate certain types of procedures and promise efficiency gains in these context (Cheng et al. 2017),

Similarly, as highlighted before, DLT applications can create trust in data storage systems. Especially in environments in which trust in government is low and corruption is high, DLT offers a way to record data and transactions that does not rely on a single government actor. Decentralising data storage and making it more transparent and accountable can help citizens to regain trust into data held by the government. It can thus potentially even help to prevent corruption by making it impossible to tamper with data and change data entry (Kossow and Dykes 2018). With the help of the correct system design, data storage using DLT can help citizens to make claims and prove them using data in the blockchain.

<table>
<tr><td rowspan="2">Disintermediation</td><td>Security</td><td rowspan="2">No single central point of failure
More resistant to attacks
Higher transaction rates
Lower transaction costs
Depends on scalability of DLT application
Slightly different for private/consortium blockchains: data is potentially less vulnerable to outside access, data storage is made even more efficient, but security effects through disintermediation are diminished.</td></tr>
<tr><td>Efficiency</td></tr>
<tr><td>Immutability</td><td>Accountability</td><td>Time stamped transactions that can be tracked
Record of full transaction history
Reduced possibility of tampering with data
Attribution potentially easier in consortia/private blockchains</td></tr>
<tr><td>Transparency</td><td>Inclusiveness</td><td>Enable broad participation
Allow access to the public
Limited in private blockchains</td></tr>
</table>

Figure 1: Key Attributes of DLT

To this date, many of these attributes are not shown in proven use cases. However, there are already a number of cases which have gone through a proof-of-concept process and which are likely to launch for prototyping in 2018 or beyond. For the purpose of this paper, we collected a number of these cases and tried to derive a typology for public administration.

4.1 Potential applications

Over the last years, several hundreds, if not thousands, of DLT based projects were developed. They are hard to count as some projects are publicised early on during their conceptualisation, whereas others do not have a proper web presence until after their proof-of-concept phase. One indication of the increasing number of blockchain based projects is the rising number of digital currencies.[6] To date, the majority of DLT based applications uses digital currencies, often in forms of tokens, for their purposes.

[6]Often also referred to as cryptocurrencies, due to their reliance on cryptography.

These are needed to make consensus algorithms work and offer rewards to miners. They are thus a necessary part of the majority of blockchain based systems. At the time of writing, 1564 publicly traded digital currencies exist.[7] Looking at a variety of sources, we considered use cases that support the work of public administration. We realise that classifying these is not an easy task. Government and public administration touch upon all DLT applications. Even if they do not concern public service delivery, they still require regulation, as for instance the digital currency space (Doles 2017).

For the purpose of this paper though, we are interested in how public administration uses DLT in providing services and interacting with its constituents. We reviewed several reports and collections of DLT use cases in public administration and found five distinct categories of actual or potential applications. These are summarised in Figure 1, and will be outlined below.

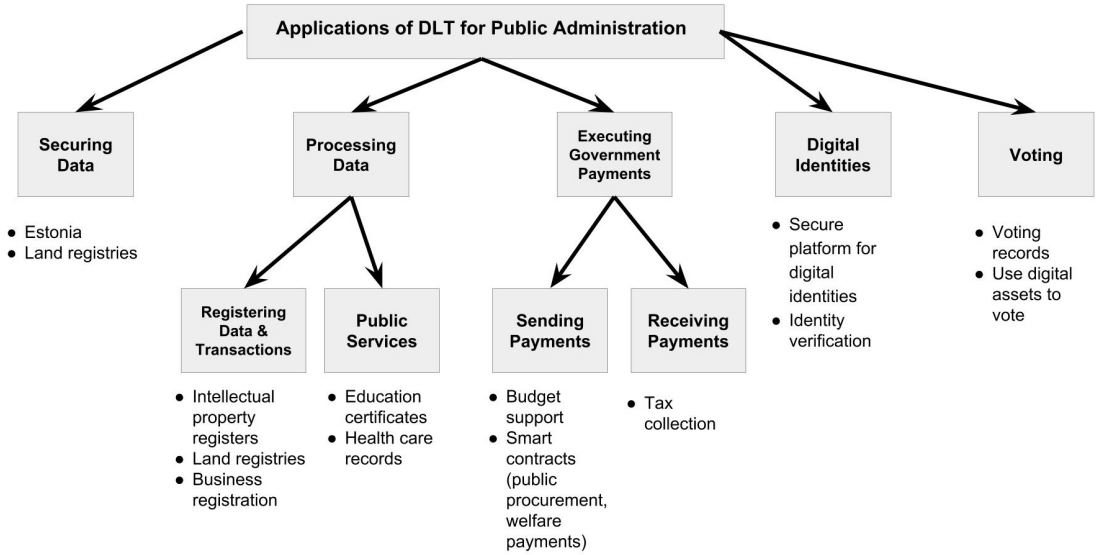

Figure 2: Applications of DLT for Public Administration

Securing Data: as it was highlighted above, security is one of the key features of blockchain technology. Storing data in a distributed ledger removes the dangers attached to having one central point of failure. For governments, blockchain technology thus can provide efficient, affordable and safe data storage. Using blockchain can become an advantage in this context if critical government data is stored digitally. Estonia has become the first country to use the technology in this context. Rather than storing data itself on a blockchain, Estonia uses blockchain technology to verify the integrity of data. It does so by creating a cryptographic hash of the original data, time-stamping and securely storing it. As any other version of the data would result in a different hash

[7] As listed by Coinmarketcap.com, a website listing cryptocurrencies and their market value: `https://coinmarketcap.com/all/views/all/`

value, the Estonian system can easily detect fraudulent data. While attempts to delete or change data cannot be prevented, the system can however detect any wrongdoing. This works as Estonias permissioned blockchain is built into the countrys advanced data infrastructure. Securing data is possible, as it uses *data-at-rest*, referring to data that is not in use at the time it is being hashed (Martinovic, Kello, and Sluganovic 2017).

Similar projects have been piloted in the context of land registries. Countries such as Bermuda, Costa Rica, Dubai, Georgia,[8] Honduras, Sweden & Ukraine have all launched project to secure their land registries using blockchain technology (Reese 2017). Similar to the Estonian example, hashes of land registries are time-stamped and added to a blockchain. This move is seen as a way to establish greater trust into the data and in helping to prevent corruption.

Processing Data: the potential for using blockchain in handling data, however, also includes the treatment of *data-in-use*, meaning data that is being processed (Martinovic, Kello, and Sluganovic 2017). This would mean registering data and transactions on the blockchain with potentially several authorised partners being able to access the data. Pilots to use DLT in data processing are already under way and some have passed their proof-of-concept phase. These ideas include storing health care records[9] and education certificates on the blockchain. Going back to the example of land registries, it could result in land sales being executed via a blockchain using smart contracts (Shin 2017). Furthermore, intellectual property registries could be moved onto the blockchain and several companies are currently developing solutions for this idea (TaylorWessing 2017). The US state of Delaware is developing an incorporation service that is supposed to use smart contracts and blockchain technology. It could be used to make incorporation more efficient and to ensure compliance with rules in the process (Cheng et al. 2017).

Disintermediation holds potential for the use of blockchain technology in these contexts. As many government services today involve data storage, using this technology for this purpose could result in significant efficiency gains. However, so far, storing data-in-use by means of DLT still faces significant challenges. While new DLT applications such as IOTA (Popov 2017) might address some of these with regards to scaling, other issues will still remain significant for several years to come. These will be outlined in more detail below.

Executing Government Payments: several DLT pilots have looked at how the technology can be used in the execution of government payments. Given the risks for fraud and corruption in this context, experts see an opportunity to secure payments using blockchain to create an immutable and accountable record of transactions (Cheng et al. 2017; White, Killmeyer, and Chew 2017). Blockchain based payment mechanisms were already introduced in a refugee camp in Jordan, in order to support the distribution of funds through the World Food Programme (2017). The German Development Bank KfW (2017) is piloting *TruBudget*, a blockchain based application to administer budget

[8] See, for instance: `https://exonum.com/napr`
[9] See, for instance: `https://medicalchain.com/en/`

support for aid projects. Further projects are also looking at the use of such applications to administer tax payments to the government (Walport 2016). In these context DLT can be used to keep accurate records of payments and to make them accessible to partners with a central point of access. However, payments can also be administered using a digital currency. In the context of public procurement, the use of smart contracts has been raised as an idea to make procurement process more efficient and to protect them from fraud (Santiso 2018). Likewise, there are ideas to use blockchain-based smart contracts to administer welfare payments (Walport 2016).

Digital Identities: a common problem in internet-based economies is the need for secure digital identification. These are rarely fully implemented to due security concerns. Several companies are currently working on DLT based solutions for this problem. Their idea is to store digital identities on a blockchain, in order to protect them against attacks, make them immutable and keep a record on how they are used. This is supposed to increase trust in their usage. While there are significant challenges to the wide scale implementation of digital identities, pilots have been very promising and are likely to be extended in 2018 (Aitken 2018).

Voting: another common use case for DLT is voting procedures. Voting processes of any kind is common place in most democratic societies. Equally often they are subject to fraud. Using blockchain technology might help to address this issue. Voting could take place using digital assets, with records being kept secure through blockchain technology. Voters could identify themselves through cryptographic key, biometric data or digital identities. Several pilots were launched in a variety of concept and blockchain voting applications are moving out of their proof-of-concept phase. Recently, a DLT based application was piloted for voting in Sierra Leones election, however, it was not yet used to govern the entire election (Kazeem 2018).

As shown above, many pilots and use cases exists that show the potential for the use of DLT in a variety of contexts.[10] However, the widescale implementation of any of such projects should also be greeted with a healthy amount of scepticisim. Several challenges and considerations have to be taken into account.

5 Challenges & Considerations

Like any technology, blockchain is not a panacea nor does it come without its own unique set of challenges and drawbacks. Understanding what these are is crucial to being able to meaningfully assess the potential this technology has for governments in the modern era.

[10] A large number of projects were also found in the energy sector and in the management of supply chains. We found that these sectors, however, were less directly linked to the provision of services by public administration. Equally we did not include fundraising efforts and the distribution of non-governmental funds in this context.

Regardless of the field of application, one of the most considerable challenges associated with blockchain technology is that of scalability. As has already been touched upon in previous sections, to date all of the popular blockchain consensus protocols in use require every node in the network to process every transaction (Kasireddy 2017). This means adding new information to a blockchain will demand increasingly more computer processing power as both the number of nodes and the length of the blockchain increase over time. The end result is that adding information to the blockchain becomes more inefficient and resource-intensive over time. There are alternative consensus models currently being explored and tested (such as proof of stake and the Tangle from IOTA, both of which were mentioned earlier in paper), but generally, scalability remains a concern with public blockchains. Private blockchains, however, can avoid this problem to some extent, since they can limit the number of nodes required to update a blockchain (Buterin 2015).

Another consideration for blockchain technology in any context is to what extent the technology actually stands to solve fundamental issues of trust is different environments. Certainly, blockchain technology provides a high level of oversight over changes to information published on a blockchain, as well as assurances that a central authority is not bending rules and regulations according to their whims. But blockchain technology still cant guarantee information was correctly entered in the first place the same limitation any database solution faces. Thus while blockchain can in theory promote greater trust in the integrity of information entered into it, other mechanisms and processes outside of blockchain are necessary to resolve trust issues that extend beyond whether information is tamper-proof once it has been entered. Given that trust and the ability to combat fraud is one of the key selling points of blockchain technology (Ølnes, Ubacht, and Janssen 2017), its important to maintain a grounded understanding of what benefits this technology can actually bring about.

In addition to these two broad concerns, there are also several areas where public administrations may face unique challenges when deploying blockchain technology. Again, it is worth noting that many times, private or otherwise restricted blockchains can either solve or at the least mitigate many of these issues, although this does erode some of the transparency and decentralized trust gains from public blockchains, as has been discussed in earlier parts of this paper.

5.1 Legal Challenges

The use of blockchain technology, particularly in a governmental context, opens up a host of complex legal questions with no obvious answers; governments will have to grapple with these questions and consider how blockchain fits into existing legal frameworks, or whether existing frameworks should be changed to accommodate blockchain technology.

For one, the decentralized and permissionless nature of a public blockchain or distributed ledger means the nodes that make up the blockchain and which provide the consensus necessary to add new blocks can be added at an individual's whim and conceivably be located anywhere in the world. This creates a uniquely muddied jurisdictional landscape if a transaction conducted on a blockchain is later legally disputed, it could conceivably fall under jurisdiction of every nodes location and it could also be problematic if governments have specific regulations around where and how data can be stored (for example, that it should not be stored outside of the country or outside of a specific region) (McKinlay et al. 2018; Finck 2017). This issue can conceivably be avoided by simply making use of private or otherwise restricted blockchains whereby the blockchains administrators can control what nodes are part of the blockchain (and thus ensure the only nodes able to write to the blockchain in question are located within the permissible area).

Another consideration specific to the functioning of public blockchains reflected in the literature as well as in our interviews is the fact that they cant simply be turned off when their usefulness has ended (McKinlay et al. 2018). The government can cease contributing to their blockchain, but as long as other nodes remain active, they can continue to keep the blockchain active and functioning. Here it would remain to be clarified at what point and on what legal basis the government can claim the blockchain in question is no longer in official, government use and thus should not be considered the legal and/or authoritative record. This is largely unexplored territory, given that there are very few examples of successful blockchain-based projects to begin with we hardly know how to start them, let alone end them.

There are also potential legal implications related to data protection ordinances and the storing of personal data on blockchains, as is currently playing out in Europe. The European Union will enact its General Data Protection Regulation in May 2018. Among its sweeping changes are new rights for citizens to demand their personal data be modified or permanently deleted. This flies in the face of one of the key functionalities of blockchains, immutability meaning data cant be deleted or otherwise modified retroactively. There will always be a record of that information having existed and thus the risk that the country responsible for maintaining the blockchain in question will be accused of non-compliance with the GDPR (Finck 2017). Again, however, this issue is potentially resolved by making use of a private blockchain rather than a public one. Information published to a blockchain can theoretically be rewritten if someone creates a new version of that blockchain that is treated as authoritative (i.e., they create a fork that reflects the desired status quo). This action is possible to complete if a majority of the nodes in the network agree to the change a task that is feasible in a private blockchain where there is a limited number of nodes whose participation has already been vetted, but which is much more difficult on a public blockchain with potentially a huge number of nodes whose consensus needs to be secured (ibid.).[11]

Finally, as it was pointed out above, another possible application of blockchain technology

[11]Those interested in learning about other ways blockchain technology and the GDPR will be at odds with each other are highly encouraged to read Fincks entire paper.

is the use of smart contracts. However, in most public administrations, allowing smart contracts to function the same way as a traditional legal agreement would require at times changes to the frameworks that govern what can constitute a legal agreement and such changes are not always trivial to enact. For example, a contract completely concluded via a blockchain may not satisfy a given countrys signature requirements (since digital signatures may not always be accepted), or it the process may not have satisfied requirements for how parties should be informed about the terms of the contract (i.e., were parties given thorough information on how the contract was structured, or were they simply given a broad description of terms and the option to click Agree) (Norton Rose Fulbright 2016; O'Shields 2017). None of this is meant to imply that existing legal codes and smart contracts cant be reconciled, but the compatibility of these contracts with existing legal frameworks needs to be established prior to committing to the use of smart contracts in public administration.

5.2 Bureaucratic Hurdles

In general, implementing new technologies and/or processes into an existing, well-established bureaucracy tends to present significant challenges. Blockchain is, of course, no exception to this.

For one, bureaucrats are often highly resistant to change, preferring not to have to learn new skills or workflows regardless of whether there is a provable benefit to be won from this shift (Dunleavy et al. 2006). Certainly strategies can be employed to make these changes seem more palatable or less intimidating, but this could be particularly difficult to do with regards to blockchain technology, given how poorly understood and difficult to explain it tends to be even for individuals who are otherwise experienced in matters of IT.

But a larger concern for meaningfully implementing blockchain technology in government is the lack of qualified personnel to undertake the task. Governments in general struggle to recruit and keep IT professionals and other technologically skilled individuals (ibid.). Some countries have been more successful than others in mitigating this problem and establishing governmental bodies focused on the technological advancement of the public administration (such as the UKs Government Digital Service or Estonias extensive e-Estonia administration); regardless, most countries continue to struggle with this on a large scale. Further, the novelty of blockchain technology makes it difficult to even attempt to recruit individuals with actual experience implementing blockchain-based solutions there simply arent enough individuals experienced with blockchain technology to go around.

This lack of internal experience puts governments in a challenging position. They can try to move forward with their possibly-lacking in-house capabilities and risk developing a solution with a higher chance of failure due to lack of expertise and experience. To a certain extent, this would be a preferable option, since experimentation and thus, a

willingness to fail is seen by many public sector innovation experts as a key component for successful innovation (OECD 2009). However, the risk of failure presents new challenges for governments looking to adopt blockchain technology it could lead to a sort of chilling effect on future technological innovation. For example, if the society in question is not already used to the idea of the government experimenting with new technologies that may or may not work out, a failure could be seen as reflecting poorly on the governments competence as well as on the viability and desirability of pursuing blockchain-based solutions.[12] This means an initial failure could kill public and governmental support for future experimentation and reduce the likelihood that the government takes such a chance with blockchain or other emerging technologies again, limiting possibilities for future innovation in public administration.

As an alternative to relying on their own capabilities, public administrations can of course seek out the services of private companies or consulting services specializing in blockchain solutions. However, these companies interests tend to lie more heavily with selling governments as many services as possible, rather than with creating a cost-effective, user-focused solutions. Thus, such an approach is less likely to produce outcomes than actual focus on user needs the way successful digital tools usually should (this approach to digital public services is expanded upon in the next section). Further, the lack of government expertise around blockchain puts governments at a disadvantage: they are not able to operate as intelligent customers who can decisively articulate what services they do and do bot need and instead are at the mercy of the vendors (alleged) expertise.[13]

In short, faced with a lack of in-house expertise (and a low likelihood of recruiting new expertise), governments have to weigh the merits of experimentation with the real likelihood of failure versus relying on potentially cost-ineffective third party service providers.

5.3 Usefulness & Context-Appropriateness

It is crucial to remember that while blockchain technology can theoretically bring about a range of possible benefits in the public administration context, that does not mean it is the only way of securing those benefits, or even the best way. In many cases, traditional databases are just as sufficient as blockchain solutions for meeting data storage needs (Greenspan 2017). Governments contemplating developing a blockchain-based tool for their public administrations need to consider if this is truly the right technology to use, rather than simply diving blindly into blockchain projects for fear of falling behind the curve. Yet, much of the discussions today of blockchain-based innovations for public administration are technology-driven rather than needs-driven or user-driven; that is, many governments seem to be embracing blockchain technology as an end in itself, rather than a way of solving specific problems (Ølnes, Ubacht, and Janssen 2017). This is in contrast to the current-day prevailing wisdom with regards to designing better public services, which advocates for a user-centred design. This is the idea that services

[12]Interview with an Estonian expert on e-government.
[13]Interview with a UK civil servant with expertise in digital services.

should be designed for the people who will actually use them based on assessments of what the user needs actually are (rather than being based on assumptions of what those needs by bureaucrats and civil servants) (Brown, Fishenden, and Thompson 2014). Government digitalisation experts who we spoke to for this paper repeatedly observed that this emphasis on what users actually want is hugely absent from current discussions about blockchain technology for public administrations. If a compelling user need is not identified, its highly unlikely a blockchain-based solution for public administration would see enough use and positive feedback from citizens to justify the amount of money and resources put into its development.

As has been mentioned, one of the most commonly cited and celebrated benefits of blockchain technology is its ability to provide a greater amount of trust than other most other technologies through the assurance users have that information cannot be tampered with once it has been entered into the blockchain. The thought process many blockchain champions thus have is that more trust is always a net gain and thus if transitioning a service to the blockchain increases the amount of trust it can provide users, then this is a worthy endeavour.

In the context of developed, western countries, however, many areas where blockchain stands to increase trust and combat fraud are simply not areas where rampant concerns with fraud are regularly encountered. For example, a civil servant working on digital transformations in the UK commented that one possible use case for blockchain that has been cited is for verifying university qualifications: degrees could be digitally registered on a blockchain by a trusted party (e.g., the university itself) and then future employers or other universities could verify that a persons stated academic credentials are indeed valid by checking the blockchain record, whose trustworthiness would conceivably be bolstered by the tamper-proof structure of the blockchain. Except, a similar level of trust could also be established using a public key infrastructure, which has been in widespread use for decades. However, efforts to enact such a system in the UK have never gained traction, presumably in part because theres not enough fraud in the system to be worth checking.[14]

Obviously the prevalence of fraud is likely to vary based on the country context of a specific public administration (e.g., countries with higher rates of corruption would probably have a greater need for finding innovative and trust-maximizing solutions for combating fraud). But conversations about blockchain for public administration need to include a realistic assessment of whether specifically focusing on blockchain-enabled is bringing any additional value to would-be users and thus if it represents a wise use of often-limited resources.

[14]Interview with a UK civil servant with expertise in digital services.

5.4 Security Unknowns

Blockchain remains a very new and largely untested technology in general, and especially in the field of public administration. One consequence of this is that the security implications of storing government information on the blockchain is not well-understood. There are of course plenty of known ways to compromise the security of traditional centralized servers, such as DDoS attacks. But, as pointed out by multiple interview partners, there is a certain advantage to knowing what the common methods of attack are and having a legacy of best practice approaches for preventing or fending off such attacks. Security in the context of blockchain technology is a much larger unknown; there arent decades of experience to build off of.

Here public versus private blockchains are important to consider. The traditional image of a blockchain is a public one where the information stored upon it is publicly readable but often encrypted. But, as one interview partner with extensive experience in implementing software systems for government noted, there are constantly advances in decryption technologies, and in this case, having potentially sensitive information stored on a public, encrypted blockchain presents a different set of risks than storing information on a centralized, secured, and non publicly-accessible server. Once the information is published on a public blockchain, this action cant be reversed anyone could make a copy of the blockchain and the information stored on it, and potentially compromise the information held within it should they possess the necessary decryption capability. The likelihood of this happening is currently low, but it cant be discounted, especially as computing processes advance and new risks present themselves (Wood 2010). Private blockchains are less risky in this sense, since the information stored on the ledger would only be accessible to those with access to the private blockchain; the trade-off here is that you lose one of the major selling points of blockchain technology, which is the absence of a central authority to manage the ledger.

In general, these security concerns are not unique to the specific usage of blockchain technology in public administration; they would theoretically exist in any application of it. But when governments are making use of blockchain technology, that means there is the possibility of citizens personal information or other valuable government information being be stored on the blockchain, as well as the possibility that important government functions might be built to rely on the blockchain. If a government-run blockchain were to be compromised, it could have negative effects for a wide swath of the population and potentially disable the government from completing critical operations.

6 Conclusion

The aim of this paper was to look beyond the hype and enthusiasm surrounding the concept of distributed ledger technology and its application in the field of public administration. For this purpose we first gave an introduction into blockchain technology and

DLT, highlighting key attributes of this technology: security, efficiency, inclusiveness and trust in the context of data storage applications. We derived these from the central features of DLT systems, namely disintermediation, immutability and transparency. Based on these attributes and on further research on current and potential use cases, we went on to offer a classification of blockchain use cases in the context of public administration. We distinguished between securing data, processing data, executing government payments, providing digital identities and voting. These categories partially overlap. Yet, they aim to provide some guidance when considering the growing field of hopeful DLT applications.

Having highlighted the expected potential and applications of blockchain in public administration, we went on to look at the challenges faced in this context. We considered legal and bureaucratic obstacles to the introduction of the technology, security concerns and the overall question of the appropriateness and usefulness of the technology in a variety of public administration applications. In this paper, we found the number of challenges significant. Especially legal challenges will be hard to overcome. The specific problems faced when introducing DLT to public administration also come on top of general problems faced by the technology, namely questions of scalability.

While a large community of observers are expecting the advent of the blockchain revolution, the authors of this paper are more reserved. Blockchains offer interesting database solutions with high potential to affect many sectors, and in particular many actors in public administration. Yet, its implementation has yet to take several years. Rather than leading to a revolution, DLT will lead us to solid reforms. In many countries, public administration wont find it easy to embrace these, but still it is safe to say that the blockchain is here to stay.

References

Aitken, Roger (2018). *Blockchain To The Rescue Creating A 'New Future' For Digital Identities*. URL: https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/ (visited on 03/15/2018).

Alkan, C.V. (2017). *Decentralized Objective Consensus without Proof-of-Work*. URL: https://hackernoon.com/decentralized-objective-consensus-without-proof-of-work-a983a0489f0a (visited on 03/15/2018).

Atzori, Marcella (2015). "Blockchain technology and decentralized governance: Is the state still necessary?" In:

Berke, Allison (2017). *How Safe Are Blockchains? It Depends*. URL: https://hbr.org/2017/03/how-safe-are-blockchains-it-depends (visited on 03/15/2018).

Brown, Alan, Jerry Fishenden, and Mark Thompson (2014). *Digitizing Government*. Palgrave Macmillan Publishing.

Buterin, Vitalik (2015). *On Public and Private Blockchains*. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (visited on 03/15/2018).

Cheng, Steve et al. (2017). *Using blockchain to improve data management in the public sector*. URL: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector (visited on 03/15/2018).

Crosby, Michael et al. (2016). "Blockchain technology: Beyond bitcoin". In: *Applied Innovation* 2, pp. 6–10.

Davidson, Sinclair, Primavera De Filippi, and Jason Potts (2016). "Disrupting governance: The new institutional economics of distributed ledger technology". In:

Doles, Silva (2017). "Cryptocurrencies and International Regulation". In: *Modernizing International Trade Law to Support Innovation and Sustainable Development (Congress)* 4.

Drake, Nate (2017). *How to run a full Bitcoin node*. URL: https://www.techradar.com/how-to/how-to-run-a-full-bitcoin-node (visited on 03/15/2018).

Dunleavy, Patrick et al. (2006). *Digital Era Governance: IT Corporations, the State, and E-Government*. OUP Oxford.

Etherum (2018). *Proof of Stake FAQ*. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ (visited on 03/15/2018).

European Commission (2018). *European Commission launches the EU Blockchain Observatory and Forum*. URL: https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-eu-blockchain-observatory-and-forum (visited on 03/15/2018).

Finck, Michéle (2017). *Blockchains and Data Protection in the European Union*. Research Paper No. 18-01.

Glaser, Florian (2017). "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis". In: *Proceedings of the 50th Hawaii International Conference on System Sciences*, pp. 1543–1552.

Greenspan, Gideon (2017). *Do you really need a blockchain for that?* URL: https://coincenter.org/entry/do-you-really-need-a-blockchain-for-that?mc_cid=a7bfc69a19 (visited on 03/15/2018).

Guo, Ye and Chen Liang (2016). "Blockchain application and outlook in the banking industry". In: *Financial Innovation*.

Higgins, Stan (2018). *Lithuania's Central Bank Unveils Blockchain Startup Sandbox.* URL: https://www.coindesk.com/lithuanias-central-bank-unveils-blockchain-startup-sandbox/ (visited on 03/15/2018).

Kasireddy, Preethi (2017). *Blockchains dont scale. Not today, at least. But theres hope.* URL: https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a/ (visited on 03/15/2018).

Kazeem, Yomi (2018). *The worlds first blockchain-supported elections just happened in Sierra Leone.* URL: https://qz.com/1227050/sierra-leone-elections-powered-by-blockchain/ (visited on 03/15/2018).

Kossow, Niklas and Victoria Dykes (2018). *Bitcoin, blockchain and corruption: an overview.* URL: https://knowledgehub.transparency.org/helpdesk/bitcoin-blockchain-and-corruption-an-overview (visited on 03/15/2018).

Kreditanstalt für Wiederaufbau (2017). *KfW entwickelt Software mit Blockchain-Technologie.* URL: https://www.kfw-entwicklungsbank.de/Internationale-Finanzierung/KfW-Entwicklungsbank/News/News-Details_431872.html (visited on 03/15/2018).

Lee, Timothy B. (2017). *Bitcoin fees are skyrocketing.* URL: https://arstechnica.com/tech-policy/2017/12/bitcoin-fees-are-skyrocketing/ (visited on 03/15/2018).

Martinovic, Ivan, Lucas Kello, and Ivo Sluganovic (2017). *Blockchains for Governmental Services: Design Principles, Applications, and Case Studies.* Working Paper No. 7. Centre for Technology & Global Affairs (Oxford).

Maupin, Julie (2017). *The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All.* URL: http://www.g20-insights.org/policy_briefs/g20-countries-engage-blockchain-technologies-build-inclusive-transparent-accountable-digital-economy/ (visited on 03/15/2018).

McKinlay, John et al. (2018). *Blockchain: background, challenges and legal issues.* DLA Piper.

Meijer, Carlo RW de (2016). "The UK and Blockchain technology: A balanced approach". In: *Journal of Payments Strategy & Systems* 9.4, pp. 220–229.

Nakamoto, Satoshi (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* URL: https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/bitcoin.pdf (visited on 03/15/2018).

Nofer, Michael et al. (2017). "Blockchain". In: *Business & Information Systems Engineering* 59.3, pp. 183–187.

Norton Rose Fulbright (2016). *Can smart contracts be legally binding contracts?* URL: http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf (visited on 03/15/2018).

O'Dwyer, Karl J. and David Malone (2014). "Bitcoin Mining and its Energy Footprint". In: *ISSC 2014 / CIICT 2014*.

OECD (2009). "Innovation and Systemic Innovation in Public Services". In: *Working Out Change: Systemic Innovation in Vocational Education and Training*, pp. 29–58.

Ølnes, Svein (2016). "Beyond bitcoin enabling smart government using blockchain technology". In: *International Conference on Electronic Government and the Information Systems Perspective*, pp. 253–264.

Ølnes, Svein and Arild Jansen (2017). "Blockchain Technology as s Support Infrastructure in e-Government". In: *International Conference on Electronic Government*, pp. 215–227.

Ølnes, Svein, Jolien Ubacht, and Marijn Janssen (2017). "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing". In: *Government Information Quarterly* 34.3, pp. 355–364.

O'Shields, Reggie (2017). "Smart Contracts: Legal Agreements for the Blockchain". In: *North Carolina Banking Institute* 21 (1).

Pal, Alasdair (2018). *Blockchain name-grabbing has echoes of dotcom bubble.* URL: https://www.reuters.com/article/us-blockchain-companies/blockchain-name-grabbing-has-echoes-of-dotcom-bubble-idUSKBN1FS1F3 (visited on 03/15/2018).

Popov, Serguei (2017). *The Tangle.* URL: https://iota.org/IOTA_Whitepaper.pdf (visited on 03/15/2018).

Reese, Frederick (2017). *Land Registry: A Big Blockchain Use Case Explored.* URL: https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem/ (visited on 03/15/2018).

Rodrigues, Bruno et al. (2017). "A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts". In: *IFIP International Conference on Autonomous Infrastructure, Management and Security*, pp. 16–29.

Santiso, Carlos (2018). *Will Blockchain Disrupt Government Corruption?* URL: https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption (visited on 03/15/2018).

Shin, Laura (2017). *The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project.* URL: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/ (visited on 03/15/2018).

Tapscott, Don and Alex Tapscott (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Penguin.

TaylorWessing (2017). *Blockchain technology and IP.* URL: https://www.taylorwessing.com/download/article-blockchain-technology-and-ip.html (visited on 03/15/2018).

Walport, Mark (2016). *Distributed ledger technology: Beyond blockchain.* URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (visited on 03/15/2018).

White, Mark, Jason Killmeyer, and Bruce Chew (2017). *Will blockchain transform the public sector?* URL: https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html (visited on 03/15/2018).

Wood, Lamont (2010). *The clock is ticking on encryption.* URL: https://www.computerworld.com/article/2511969/security0/the-clock-is-ticking-on-encryption.html (visited on 03/15/2018).

Woodward, Alan (2016). *Anonymity vs Pseudonymity In Cryptocurrencies.* URL: https://www.profwoodward.org/2016/01/blog-post_30.html (visited on 03/15/2018).

World Food Programme (2017). *Blockchain Against Hunger: Harnessing Technology In Support Of Syrian Refugees.* URL: https://www.wfp.org/news/news-release/blockchain-against-hunger-harnessing-technology-support-syrian-refugees (visited on 03/15/2018).

Yli-Huumo, Jesse et al. (2016). "Where Is Current Research on Blockchain Technology? A Systematic Review". In: *PLOS ONE* 11.10, pp. 1543–1552.