ERCAS

European Research Centre for
Anti-Corruption and State-Building
Hertie School of Governance

Working Paper No. 58

Beyond the Hype:
Distributed Ledger Technology in the Field of Public Administration

Niklas Kossow

Berlin, July 2019

www.againstcorruption.eu

ERCAS WORKING PAPERS COLLECTION

Abstract[1]

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.[2]

Keywords: distributed ledger technology; blockchain; data management; public administration; bureaucracy; trust.

[1] An earlier version of this paper was written together with Victoria Dykes to who I am very grateful for her continuous support and ideas in developing this project further.

[2] **Niklas Kossow** is a research associate and PhD candidate at the Hertie School. His research focusses on the use of new technologies in the context of anti-corruption movements and democratization.

Table of Contents

Introduction

Since its peak in 2017, the hype surrounding blockchain technology has somewhat faded. Back then, 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). Yet, the technology still holds promises to be applied in a variety of fields, including public administration. Governments and analysts are still hailing the possibilities that the technology holds for bureaucratic processes. Estonia used a comparable technology early on and 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[3] 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 as many applications are still in their proof-of-concept phase and not fully developed. The aim of this paper is to sift through information on current applications of DLT in the field of public administration. 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.

Research Approach & Literature Review

As solid academic work on used cases is still hard to find, this paper wants to lay ground for 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 abo-

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

ve 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 (Galen et al., 2018).[4]

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.

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. More publications can be found form of reports. Yet, I will start by providing a brief review of the academic literature at hand to argue why there is a need for further research on the topic.

An early text on the uses of blockchain technology that goes beyond bitcoin is Tapscott & Tapscott (2016). Their book "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World" provides a good introduction to the technology as well as a large variety of use cases. They also extensively look at uses of DLT in the context of government, providing insights into potential applications and early experiences. Without too much detail they provide an overview of potential use of blockchain in government service delivery and in the context of democratic elections. In the final part of their book, Tapscott & Tapscott (2016) give a decent overview of limitations and argue that blockchain, for numerous reasons, is not ready yet while remaining 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 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. (2016) 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. De Meijer (2016) analyses the UK government's 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 et al. (2016) argue that blockchain is even more than just a disruptive new technology. They call it an "institutional technology of governance" (Davidson et al., 2016, p. 2) and liken its implications to "the invention of the joint stock company" (Davidson et al., 2016, p. 24).

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-re-

[4] This information is collected via crowdsourcing using a Google spreadsheet: https://goo.gl/eY8DqU

searched 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.

Ølnes *et al.* (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 an 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 et al., 2017, pp. 4-5). Ølnes & 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. This paper was developed further to Ølnes & Jansen (2018) where the authors present an analytical framework contrasting the benefits and challenges of introducing blockchain technology as infrastructure in the context of government work.

Academic papers looking at more specific applications and use cases of distributed ledger technology in public administration are still rare. This is largely due to many projects still being in a testing phase and the technology being still young. One area in which distributed ledger technology is already being piloted is land administration - several projects are looking at the use of DLT to secure land titles. To a lesser degree, the use of smart contracts in handling land contracts is also suggested (Stefanovic et al., 2019; Vos, Lemmen, & Beentjes, 2017). A reoccurring theme is also the use of DLT as anti-corruption applications, something that this paper will also briefly look at (Kim & Kang, 2019). Furthermore, Sicilia & Visvizi (2019) are looking at the use of blockchain in storing meta data and links to library titles to make them more accessible and immutable. Even some of these papers are still in a preliminary state and were made accessible as conference papers.

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.

Defining Blockchain and Different Types of DLT

At its core, the concept of blockchain technology represents a new way to store and secure data. It was first published as part of the bitcoin white paper by Satoshi Nakamoto (2008) as a way to verify who owns the digital currency without relying on a trusted third party[5]. Data is thus not stored on one centralised server, but rather distributed on several servers and thus (ideally) de-

[5] Digital currencies are often also referred to as cryptocurrency as they rely on cryptography.

centralised. This is why the bitcoin blockchain is seen as one type of distributed ledger technology (DLT), which also includes other technology implementations that follow very similar principles.

Data on the blockchain is stored on a decentralised computing system that consists of nodes[6] communicating with each other. On these nodes, the data is stored in blocks. Originally designed to record transaction data, blocks can in theory store any kind of data, which is why the applications of blockchain technology can be so varied (Sward, Vecna, & Stonedahl, 2018; Walport, 2016). Using a cryptographic hashing mechanism[7] blocks are linked to each other. New data written on the blockchain thus always contains a cryptographic image of the previous data and thus secures the integrity of the data, as changes in the data would invalidate the integrity of the chain. Data can thus not be changed later, and the blockchain provides an audit trail as to which data was entered to the blockchain at what point. In this process the distributed ledger is stored simultaneously on all nodes that are part of the system - this can be as little as three servers, but in the case of bigger, public blockchains these are thousands of nodes. DLT thus avoids one central point of failure.

Different types of DLT differ not only in size of blocks and frequency that they can be written, but also in the way they are programmed, who gets access to the system, and which mechanism is used to link blocks together. The last two points are particularly crucial, as we will show when highlighting the different types of DLT. The bitcoin blockchain was implemented as a public system: technically, anyone can read and write data onto the bitcoin blockchain, which is not the case on other DLT applications. Furthermore, to add a new block to its ledger, the bitcoin blockchain uses a so-called "proof-of work" algorithm[5]. This algorithm is crucial to the system as it is mechanism by which different nodes establish consensus about what data is written onto the distributed ledger or not. It is thus referred to as a consensus algorithm. As we will highlight below, there are a variety of consensus algorithms used in different DLT applications, with proof-of-work still being the most common.

Different types of Distributed Ledgers

As already highlighted above, the bitcoin blockchain is a DLT described as a *public blockchain*. This 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 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, 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[8] are distributed ledgers with a fixed or limited number of nodes who

[6] These can be any type of device with an IP address able to run a program that validates transactions on the blockchain (Drake, 2017).

[7] The bitcoin blockchain is using a SHA-256 hash algorithm the process of linking two blocks created a hash of the transactions: 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. In the bitcoin blockchain, the block also contains a nonce, a cryptographic puzzle that needs a certain amount of computing power to be solved but can easily be verified - it thus regulates who can add the next block to the blockchain and how many blocks can be added. This mechanism is thus referred to as "proof-of-work" since a nonce has to invest computing power in order to add a block to the blockchain. Since a reward in form of a cryptocurrency is paid out to the successful node, the entire process is described as mining.

[8] 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 data and transactions on the blockchain.

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).

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 less vulnerable to outside attack, such as distributed denial of service (DDoS) attacks[9] (Rodrigues et al., 2017). 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 consen-

[9] 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.

sus 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.[10] 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 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.

[10] 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/

Table 1: Key Attributes of Distributed Ledger Technology

Disintermediation	Security	□ No single central point of failure o More resistant to attacks □ Higher transaction rates □ Lower transaction costs o 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.
	Efficiency	
Immutability	Accountability	□ 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
Transparency	Inclusiveness	□ Enable broad participation □ Allow access to the public o Limited in private blockchains

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 & 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 & Dykes, 2018a). 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.

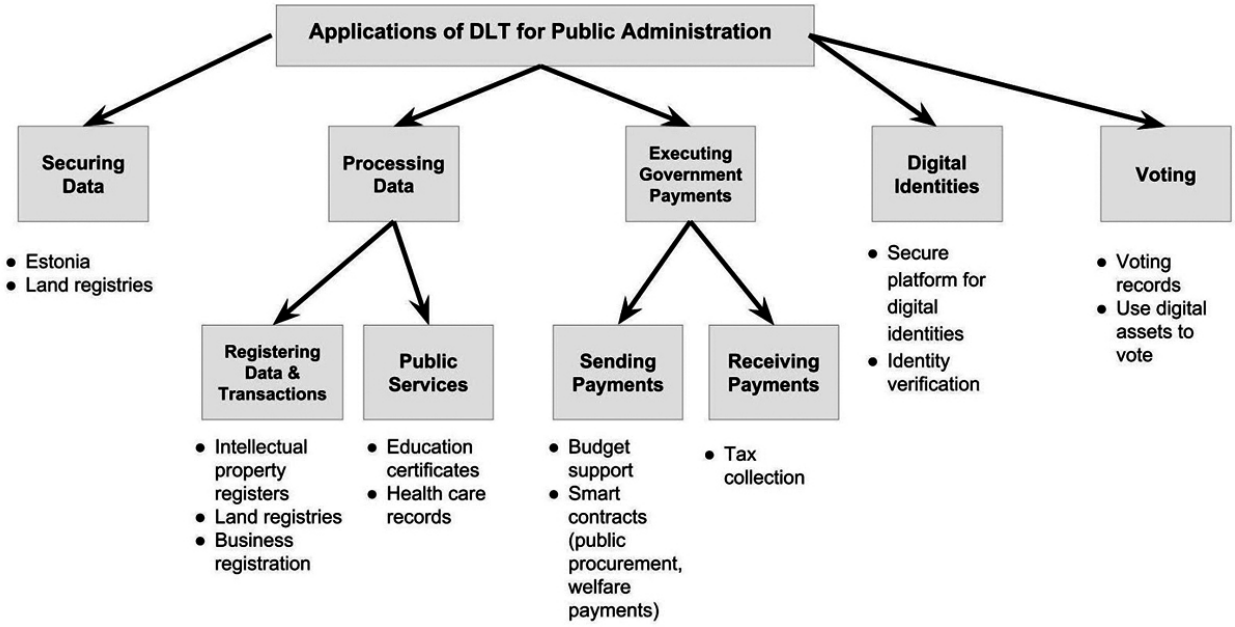
To this date, many of these attributes are not shown in proven use cases. However, there are already a number of cases which have gone through a proof-of-concept process and which are likely to launch for prototyping in 2018 or beyond. For the purpose of this paper, we collected a number of these cases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

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[11]. To date, the majority of DLT based applications uses digital currencies, often in forms of tokens, for their purposes. 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, 2264 publicly traded digital currencies exist[12]. 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 1: Applications of DLT for Public Administration



Source: Author's Illustration

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. Yet, so far DLT is mostly an inefficient way to store larger quantities of data - this means data larger than a few kilobytes (Sward et al., 2018). Still, small data, such as data on transactions can easily be stored and secured. This opens opportunities for securing data by securely storing and

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

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

time-stamping a cryptographic hash of the original data. If the hash is stored on an immutable ledger, it can be used as a verification mechanism: any other version of the original data would, if the hash-function is reapplied, result in a different hash value. It can thus be used to continuously verify data. The stored hash on the blockchain proves that at a certain point, data existed in a specific form. Since DLT makes this hash immutable and traceable, it adds a layer of security to the system. 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, & Sluganovic, 2017).

A case that is often cited in this context is Estonia. While not using an actual DLT system, its "X-Road" system also uses hash-functions and time-stamping to add security to its data exchange system. This makes it possible to detect fraudulent data. While attempts to delete or change data cannot be prevented, the system can detect any wrongdoing (Kivimäki, 2018).

Case study: land registries

The context of land registries offers some of the most advanced used cases of DLT use in order to secure data. Amongst others, projects have been piloted in the context of land registries. Countries such as Bermuda, Costa Rica, Dubai, Georgia, Honduras, Sweden & Ukraine have all launched project to secure their land registries using blockchain technology (Reese, 2017). In Georgia, the company *Exonum*[13] offers a DLT implementation that aims to facilitate land sales. For the moment, the company introduced a system that secures Georgia's land registry. Essentially, it uses an existing system by the Georgian National Agency of the Public Registry (NAPR). Here, user can digitally register their land titles with the NAPR. Together with Bitfury, a company that already previously operated bitcoin mining servers in Georgia, a hybrid blockchain was added to the system: land titles are timestamped, hashed and registered on the blockchain. By doing so, they are immutably fixed on the blockchain and protected against fraud (Shang & Price, 2018). The hash can be reapplied to the land titles to check if they were tempered with. Without changing the system for users, the system thus adds greater security and thus aims to prevent corruption and increase trust. In a second phase, the project aimed to realise land titles to be also processed through the system, but at the time of writing this phase was not yet completed[14].

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 et al., 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[15] and education certificates on the blockchain.

The most applicable way of processing data on the blockchain comes, however, through the use of so-called *smart contracts*. As explained briefly above, these are self-executing contracts written in computer code. The code defines the terms, consequences and rules of the contract; writing it on a DLT system enables a smart contract to self-execute if, for instance, a certain condition is met[16]. In the context of public administration, smart contracts would enable a range of

[13] See, for instance: https://exonum.com/blog/04-03-17-georgia-agreement/

[14] Interviews with two individuals involved in implementing the system.

[15] See, for instance: https://medicalchain.com/en/

[16] A simplified example here would be a bet on weather developments. Party A pay party B a specified amount of money if the sun shines on a specific day. A smart contract could be programmed to automatically check weather data and be tied in to a bank account so that the payment is automatically executed if the sun shines on the day specified in the contract.

data to be processed through a DLT system, from land sales (Shin, 2017) to intellectual property registers (TaylorWessing, 2017) or the act of registering a business (Cheng et al., 2017). In many of these cases, experiences for users might not chance a lot, but a DLT backend would make data handling more efficient and secure.

Case study: land sales

In the context of data processing, land registries again prove to be one of the most advances use cases. The Swedish land registry ("Lantmäteriet"), together with several partners developed a pilot to handle sales in Sweden on a blockchain infrastructure. This would revamp the process of land sales, by creating an app for this purpose. Through a DLT infrastructure, the app would tie together the buyer and the seller, as well as the Swedish land registry and the banks involved in the sale. Rather than relying on a series of individual steps that involves different parties not communicating directly with each other (the project partners list 33 necessary step), land sales would be completed in a few simple steps using one, integrated application. This is made possible by involving not only the land registry itself in the development, but a range of actors, including specialised blockchain companies, a private bank, as well as the Swedish central bank. The smart contract used to regulate and execute the land sale would be tied in via DLT to all actors involved (Kairos Future, 2017). The project finalised its third phase in 2018, running a complete transaction using the platform[17].

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, & Chew, 2017). Given the nature of DLT applications and the origin as the backbone of cryptocurrency applications it seems a natural conclusion to also use cryptocurrencies for government transactions. While being an interesting concept, this idea was rarely proposed. However, in several instances DLT was used to track payments and increase efficiency in the execution of payments. Example for that are aid payments in Jordan refugee camps supporting 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 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. 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).

Case study: building blocks

As mentioned above, the World Food Programme (WFP) in Jordan uses a private-blockchain implementation as a backend to organise cash-based transfers in Jordan refugee camps. The programme titled *Building Blocks* was first piloted in India, before applied to first 10,000 and then

[17] A demo version of the app can be found at: https://chromaway.com/landregistry/

100,000 refugees living in refugee camps in Jordan. It applies a blockchain backend to an already existing framework: refugees can spend money allocated to their accounts in shops and supermarkets in the camp using their iris scan as identification. Previously, local banks would handle these transactions and charge significant fees. Building blocks is using a distributed ledger to note all transactions refugees conduct, to withdraw money from their account. Rather than executing one bank transaction per payment, the DLT based system enables the WFP to securely and efficiently collect information on payments and execute payments in bulk. This results in large savings since the WFP pays less transaction fees. According to a respondent who was involved with the project, the savings came up to $40,000 per month even before the programme was extended to over 100,000 refugees. As pointed out above, building blocks was implemented as a private blockchain solution: this means that the WFP ran all nodes that were part of the blockchain system. This makes it easier to implement and addresses potential privacy concerns in the context of this system. However, it also makes the blockchain backend more similar to a traditional database since added security benefits do not apply. Since late 2018, the WFP addressed this concern by extending building blocks to include UN Women, which uses the system as part of its "cash for work" programme. Women that take part in the programme can earn funds that they'll be able to spend in supermarkets run by the WFP.

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. The idea is to use DLT infrastructure to fill a gap in the development of digital identities and 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 the future (Aitken, 2018). Blockchain has in particular been part of the concept of self-sovereign identities. Here, a digital identity is kept on a mobile device, for instance, a smart phone. All personal data is kept on the phone and not shared with an external server. However, DLT is used to verify claims. An example for such a claim is the ability to drive – a user or claim holder makes the claim that they are holding a valid driver's license. A claim issuer, in this case a state authority, verifies this claim. The verification of the claim is stored on a hybrid blockchain. If a user now wants to proof they own a driver's license, they do not have to share the details of the license or unnecessary personal data, but rather can share the claim that is verified by the DLT device. Using a blockchain thus enables a user to share necessary identity information using a digital ID, but without having to give up their personal data.

Case study: eID+

On of the pilots of digital identities is run in the Swiss canton Schaffhausen. The company *Procivis* developed an application called *eID+* together with the canton authority. It works via an app that users need to install on their smart phone. In the app they provide their personal information including name, gender, date and place of birth, place of residence and nationality. As explained in the concept above, this personal information remains on the user's device and is not shared externally. The entered data is treated as claims that are verified by the local administration. The eID+ can then be used to access digital government services and portals provided by the canton government. Schaffhausen sees the project as a pilot that will be extended in the next years with more service being available for eID+ holders. Data on smart phones is encrypted and password protected in case the device is lost. An underlying hybrid blockchain system makes the verification of claims possible

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 and several pilots have already tried to apply the technology. This can take shape in two ways:

First, there are pilots that use blockchain technology to cast votes in themselves. Here, voters are proving their identify (through an e-ID, biometrics or passports) which then gets associated with a cryptographic key set - a public and a private key. They then get assigned voting tokens that they can send to candidates. Transactions and thus votes would be encrypted and anonymised so that the secrecy of the vote is guaranteed. Using their key pair voters could also change their vote until the last moment. While used in some company settings, this type of system has yet to be used in an official state election[18].

Second, DLT can be used in the context of voting not to record the vote itself, but to increase the security of the voting process. Here, the blockchain is used as a bulletin board that publishes procedures of the vote. This contains information on how many votes are in the (digital) ballot box and how many votes were cast. As such, it is vital to the integrity of an electronic voting system, it makes it possible to audit and verify the election. According to Kiayias et al. (2018) this makes the bulletin board not only a crucial part of an electronic voting system, but also a single-point of failure. Putting the bulletin board on a public blockchain could thus alleviate this security concern (Cucurull & Puiggalí, 2016). The case study below will explain this concept in more detail.

Case study: immutable logs

As one of the most experienced companies providing electronic voting system, Scytl has been advancing the idea of using a blockchain to stores voting logs for several years (Cucurull & Puiggalí, 2016). It follows from their concept of an immutable log that makes an election auditable and thus secures the integrity of the election. Scytl argues that the information logged during an election should be stored in a location where the logger does not have writing or modification permission: otherwise the logger becomes a point of failure and information could be altered. Scytl thus used several means to publish these logs, amongst others publication on a GitHub[19] page. As Cucurull & Puiggalí (2016) describe, this publication could also take place on a blockchain. Scytl has piloted this using private blockchains, showing the concept to work. However, in an interview they pointed out that a public blockchain would make more sense for heightened security and greater transparency. However, transaction costs on a public blockchain a currently too high to develop a workable solution.

As shown above, many pilots and use cases exists that show the potential for the use of DLT in a variety of public administration contexts[20]. However, the widescale implementation of any of such projects should also be greeted with a healthy amount of scepticism. Several challenges and considerations have to be taken into account.

---

[18] In 2018 there were reports that the Swiss company Agora successfully applied blockchain technology in a part of Sierra Leone at the country's 2018 presidential election. However, it turned out the company had only used blockchain technology to count votes as an international observer - no actual voters had cast their vote using a blockchain (Biggs, 2018; Duffin, 2018; Kazeem, 2018)

[19] GitHub is a public repository for computer code, enabling collaborative editing.

[20] 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.

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.

Why the public sector won't use public blockchains

Many of these challenges come with the idea of a *public* blockchain, as described above. While this implementation holds the promise of increased transparency and inclusiveness, it also provides challenges that are difficult to overcome for public administration:

Legal Challenges

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 node's 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) (Finck, 2017; McKinlay et al., 2018). Furthermore, public blockchains cannot easily be turned off when their usefulness has ended since a respective government would not control all the nodes in operation. 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. Without prior experience, this is largely unexplored territory (McKinlay et al., 2018).

Scalability and inefficiencies

One of the most considerable challenges associated with public blockchains 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. Adding information to the blockchain thus 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 this paper), but generally, scalability remains a concern with public blockchains (Buterin, 2015).

Security unknowns

The conventional image of a blockchain is a public one where the information stored upon it is publicly readable but often encrypted. Encryption also supports the overall integrity and security of the blockchain: it ensures that the data stored on the blockchain is immutable. But, as one interview partner with extensive experience in implementing software systems for government noted, there are constantly advances in decryption technologies. Having potentially sensitive information stored on a public, encrypted blockchain thus presents a different set of risks than storing

information on a centralized, secured, and non-publicly accessible server. Anyone who downloads a public blockchain could potentially compromise the information held within it should they possess the necessary decryption capability. The likelihood of this happening is currently low, but it can't be discounted, especially as computing processes advance and new risks present themselves (Wood, 2010).

Given these concerns listed here, we find public blockchains largely unfit for the use in public administration. This view is shared by Walport (2016) who also only considers private or hybrid chains in his assessment of distributed ledger technology in the context of public administration. These implementations, however, also carry less of the promises of DLT as outlined above they are less disruptive tools, but rather offer incremental change to the nature of public administration. Additionally, as this paper will outline below, their application also faces further challenges that need to be considered.

Remaining challenges to DLT implementation

While many challenges to the implementation of blockchain technology are associated with public blockchains, several remain that might stand in the way of using DLT in the context of public administration.

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.

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). Given how poorly understood and difficult to explain it tends to be even for individuals who are otherwise experienced in matters of IT, blockchain technology might be even harder to sell than other digital tools.

A larger concern for meaningfully implementing blockchain technology in government, however, 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 (Dunleavy et al., 2006). The novelty of blockchain technology makes it difficult to even attempt to recruit individuals with actual experience implementing blockchain-based solutions - there simply aren't 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. 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 and reflect poorly on the government's competence as well as on the viability and desirability of pursuing blockchain-based solutions[21].

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 disa-

[21] Interview with an Estonian expert on e-government.

dvantage: they are not able to operate as intelligent customers who can decisively articulate what services they do and do not need and instead are at the mercy of the vendors (alleged) expertise[22].

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.

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).

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 et al., 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[23] (Brown, Fishenden, & Thompson, 2014). Government digitalisation experts who were interviewed 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, it's highly unlikely a blockchain-based solution for public administration would see enough use and positive feedback from citizens to justify the resources put into its development.

A major promise of DLT use is the increased trust in the accuracy of the information held by DLT applications. In the context of public administration, there are two issues with this claim: for one, DLT can only guarantee that once entered, data on a blockchain cannot be altered - it does not prevent fraudulent data to be entered in the first place (Kossow & Dykes, 2018b). Furthermore, the context of developed, western countries, the areas where blockchain technology could be used are not typically ones where rampant concerns with fraud are regularly encountered. One example is the possible application of DLT in the process of 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 person's 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 "there's not enough fraud in the system to be worth checking."[24]

Countries with higher corruption levels might evaluate this situation differently. However, 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 potential users.

Legal challenges

Potential legal implications relate to data protection ordinances and the storing of personal

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

[23] This is the idea that 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).

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

data on blockchains, as is currently playing out in Europe with the General Data Protection Regulation that came into effect in May 2018. It includes 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 can't 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). A solution to this might be changes to the blockchain protocol that makes it possible to delete information. Alternatively, information published to a blockchain could 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 often under one control (Finck, 2017)[25].

As it was pointed out above, another possible application of blockchain technology 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 country's 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 can't 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.

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 it 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. These were derived 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, I went on to offer a classification of blockchain use cases in the context of public administration. Hereby, I 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, the challenges faced in this context were considered. This included legal and bureaucratic obstacles to the introduction of the technology, as well security concerns and the overall question of the appropriateness and usefulness of the technology in a variety of public administration applications. This paper finds public blockchains to be largely inappropriate for these purposes. With other DLT implementations challenges seem manageable, but there is a serious question in what context DLT can make a difference. Greater trust and accountability as key features of DLT is largely

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

needed in societies where corruption in public administration remains the norm.

While a large community of observers are expecting the advent of the blockchain revolution, this paper remains 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 won't find it easy to embrace these, but still it is safe to say that the blockchain is here to stay.

Bibliography

Aitken, R. (2018). *Blockchain To The Rescue Creating A "New Future" For Digital Identities*. Retrieved from https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/

Atzori, M. (2015). *Blockchain technology and decentralized governance: Is the state still necessary?*

Berke, A. (2017). *How Safe Are Blockchains? It Depends*. Retrieved from https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

Biggs, J. (2018). Sierra Leone government denies the role of blockchain in its recent election. Retrieved July 5, 2019, from TechCrunch website: https://techcrunch.com/2018/03/19/sierra-leone-government-denies-the-role-of-blockchain-in-its-recent-election/

Brown, A., Fishenden, J., & Thompson, M. (2014). *Digitizing Government*. Palgrave Macmillan Publishing.

Buterin, V. (2015). *On Public and Private Blockchains*. Retrieved from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017). *Using blockchain to improve data management in the public sector*. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6-10.

Cucurull, J., & Puiggalí, J. (2016). Distributed Immutabilization of Secure Logs. *International Workshop on Security and Trust Management*, 122–137.

Davidson, S., De Filippi, P., & Potts, J. (2016). *Disrupting governance: The new institutional economics of distributed ledger technology*.

de Meijer, C. R. W. (2016). The UK and Blockchain technology: A balanced approach. *Journal of Payments Strategy & Systems*, *9*(4), 220–229.

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

Drake, N. (2017). *How to run a full Bitcoin node*. Retrieved from https://www.techradar.com/how-to/how-to-run-a-full-bitcoin-node

Duffin, A. (2018). Blockchain Election in Sierra Leone? Not Quite. Retrieved July 5, 2019, from Cryptoslate website: https://cryptoslate.com/sierra-leone-blockchain-election/

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital Era Governance: IT Corporations, the State, and E-Government*. OUP Oxford.

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

Finck, M. (2017). *Blockchains and Data Protection in the European Union*.

Galen, D., Boucherle, L., Davis, R., Do, N., El-Baz, B., Wharton, K., & Lee, J. (2018). *Blockchain for Social*

Impact: Moving Beyond the Hype. Retrieved from https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf

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

Greenspan, G. (2017). *Do you really need a blockchain for that?* Retrieved from https://coincenter.org/entry/do-you-really-need-a-blockchain-for-that?mc_cid=a7bfc69a19

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*.

Higgins, S. (2018). *Lithuania's Central Bank Unveils Blockchain Startup Sandbox*. Retrieved from https://www.coindesk.com/lithuanias-central-bank-unveils-blockchain-startup-sandbox/

Kairos Future. (2017). *The Land Registry in the blockchain - testbed*. Retrieved from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Kasireddy, P. (2017). *Blockchains don't scale. Not today, at least. But there's hope*. Retrieved from https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a/

Kazeem, Y. (2018). *The world's first blockchain-supported elections just happened in Sierra Leone*. Retrieved from https://qz.com/1227050/sierra-leone-elections-powered-by-blockchain/

Kiayias, A., Kuldmaa, A., Lipmaa, H., Siim, J., & Zacharias, T. (2018). On the Security Properties of e-Voting Bulletin Boards. *International Conference on Security and Cryptography for Networks*, *5*, 505-523. https://doi.org/10.1007/978-3-319-98113-0

Kim, K., & Kang, T. (2019). Will Blockchain Bring an End to Corruption? *International Journal of Information Systems and Social Change*, *10*(2), 35-44. https://doi.org/10.4018/ijissc.2019040103

Kivimäki, P. (2018). There is no blockchain technology in the X-Road. Retrieved June 26, 2019, from Nordic Institute for Interoperability Solutions website: https://medium.com/e-residency-blog/welcome-to-our-digital-nation-payoneer-5fc1976f02de

Kossow, N., & Dykes, V. (2018a). *Bitcoin, blockchain and corruption: an overview*. Retrieved from https://knowledgehub.transparency.org/helpdesk/bitcoin-blockchain-and-corruption-an-overview

Kossow, N., & Dykes, V. (2018b). *Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption*. Retrieved from https://www.giz.de/de/downloads/giz2018-eng_ICT-to-strengthen-Anti-Corruption.pdf

Kreditanstalt für Wiederaufbau. (2017). *KfW entwickelt Software mit Blockchain-Technologie*. Retrieved from https://www.kfw-entwicklungsbank.de/Internationale-Finanzierung/KfW-Entwicklungsbank/News/News-Details_431872.html

Lee, T. B. (2017). *Bitcoin fees are skyrocketing*. Retrieved from https://arstechnica.com/tech-policy/2017/12/bitcoin-fees-are-skyrocketing/

Martinovic, I., Kello, L., & Sluganovic, I. (2017). *Blockchains for Governmental Services: Design Principles, Applications, and Case Studies*.

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

McKinlay, J., Pithouse, D., McGonagle, J., & Sanders, J. (2018). *Blockchain: background, challenges and legal issues*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/bitcoin.pdf

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.

Norton Rose Fulbright. (2016). *Can smart contracts be legally binding contracts?* Retrieved from

http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf

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

Ølnes, S. (2016). Beyond bitcoin enabling smart government using blockchain technology. *International Conference on Electronic Government and the Information Systems Perspective*, 253-264.

Ølnes, S., & Jansen, A. (2017). Blockchain Technology as s Support Infrastructure in e-Government. *International Conference on Electronic Government*, 215-227.

Ølnes, S., & Jansen, A. (2018). Blockchain Technology as Infrastructure - an Analytical Framework. *Proceedings of 19th Annual International Conference on Digital Government Research*. https://doi.org/https://doi.org/10.1145/3209281.3209293

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355-364.

Pal, A. (2018). *Blockchain name-grabbing has echoes of dotcom bubble*. Retrieved from https://www.reuters.com/article/us-blockchain-companies/blockchain-name-grabbing-has-echoes-of-dotcom-bubble-idUSKBN1FS1F3

Popov, S. (2017). *The Tangle*. Retrieved from https://iota.org/IOTA_Whitepaper.pdf

Reese, F. (2017). *Land Registry: A Big Blockchain Use Case Explored*. Retrieved from https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem/

Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., & Stiller, B. (2017). A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. *IFIP International Conference on Autonomous Infrastructure, Management and Security*, 16-29.

Santiso, C. (2018). *Will Blockchain Disrupt Government Corruption?* Retrieved from https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption

Shang, Q., & Price, A. (2018). A Blockchain-based Land Titling Project for the Republic of Georgia. *Innovations*, *12*(3/4), 72-78.

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

Sicilia, M. A., & Visvizi, A. (2019). Blockchain and OECD data repositories: opportunities and policymaking implications. *Library Hi Tech*, *37*(1), 30-42. https://doi.org/10.1108/LHT-12-2017-0276

Stefanovic, M., Ristic, S., Stefanovic, D., Bojkic, M., & Przulj, D. (2019). Possible Applications of Smart Contracts in Land Administration. *2018 26th Telecommunications Forum, TELFOR 2018 - Proceedings*. https://doi.org/10.1109/TELFOR.2018.8611872

Sward, A., Vecna, I., & Stonedahl, F. (2018). Data Insertion in Bitcoin's Blockchain. *Ledger*, *3*, 1-23. https://doi.org/10.5195/ledger.2018.101

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

TaylorWessing. (2017). *Blockchain technology and IP*. Retrieved from https://www.taylorwessing.com/download/article-blockchain-technology-and-ip.html

Vos, J., Lemmen, C., & Beentjes, B. (2017). Blockchain-Based Land Administration: Feasible, Illusory or a Panacea. *2017 World Bank Conference on Land and Poverty*, 1-31. Washington, D.C.

Walport, M. (2016). *Distributed ledger technology: Beyond blockchain.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

White, M., Killmeyer, J., & Chew, B. (2017). *Will blockchain transform the public sector?* Retrieved from https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html

Wood, L. (2010). *The clock is ticking on encryption*. Retrieved from https://www.computerworld.com/article/2511969/security0/the-clock-is-ticking-on-encryption.html

Woodward, A. (2016). *Anonymity vs Pseudonymity In Cryptocurrencies*. Retrieved from https://www.profwoodward.org/2016/01/blog-post_30.html

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

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? A Systematic Review. *PLOS ONE*, *11*(10), 1543-1552.