Government Information Quarterly 34 (2017) 355–364

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Editorial

Blockchain in government: Benefits and implications of distributed ledger technology for information sharing

Svein Ølnes[a], Jolien Ubacht[b], Marijn Janssen[b,*]

[a] Western Norway Research Institute, Vestlandsforsking, Box 163, NO-6851 Sogndal, Norway
[b] Delft University of Technology, Faculty of Technology Policy & Management, Jaffalaan 5, 2628BX Delft, The Netherlands

ARTICLE INFO

Keywords:
Blockchain
Transforming government
Information sharing
Distributed ledger
Smart contracts
Applications
Trust
Intermediation

ABSTRACT

Blockchain refers to a range of general purpose technologies to exchange information and transact digital assets in distributed networks. The core question addressed in this paper is whether blockchain technology will lead to innovation and transformation of governmental processes. To address this question we present a critical assessment of the often exaggerated benefits of blockchain technology found in the literature and discuss their implications for governmental organizations and processes. We plea for a shift from a technology-driven to need-driven approach in which blockchain applications are customized to ensure a fit with requirements of administrative processes and in which the administrative processes are changed to benefit from the technology. Having sound governance models are found to be a condition for realizing benefits. Based on a critical assessment we offer directions for further research into the potential benefits of BC applications in e-government and the role of governance of BC architectures and applications to comply with societal needs and public values.

1. Introduction

The general purpose technology Blockchain (BC) is viewed as one of the most important technology trends that will influence business and society in the years to come (Webb, 2015). BC has emerged as a potentially disruptive, general-purpose technology for companies and governments to support information exchange and transactions that require authentication and trust (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). Blockchain Technology (BCT) stores the same information at different nodes and the information will only be added when the nodes have reached consensus. New transactions can be added, but previous information cannot be removed enabling all nodes to track the history. Storing transaction information in different nodes is called a distributed ledger. This reduces the dependency on a central actor and the risk of manipulation or system failure as all nodes have the full information. BCT can be used for any change of ownership and the storage of important information and documents like certificates, licenses, government decisions and legislation. Typically, information stored in a BC are transactional data like the ownership of land registry, birth and marriage certificates, vehicle registries, (business) licenses, educational certificates, student loans, social benefits and votes.

BCT has the potential to provide benefits to government and society and can present the next step in e-government development, as they enable reduced costs and complexity, shared trusted processes, improved discoverability of audit trials and ensured trusted recordkeeping (Palfreyman, 2015). So far, most literature is focused on the technology level, addressing the technological challenges of using BCT for peer to peer (P2P) processes (Yli-Huumo et al., 2016) or on the opportunities offered to redesign transaction and information exchange processes in the private domain. In contrast, hardly any research is focused on BCT and its ability to address societal needs. Neither is the potential of applications based on the BCT for governments explored in a systematic way (Ølnes, 2016).

Most of the literature about BCT tend to talk about the immense possibilities on one side and technology issues on another, but tend to ignore the issues located between these extremes, such as implementation, trade-offs, limitations, materiality and governance aspects which might limit the possibilities. In this paper we create an overview of potential benefits and identify new roles for government to manage BCT and ensure that their benefits materialize. Our aim is to contribute to a more substantiated discussion about BC in government by drawing the attention to aspects that are underemphasized and need more research.

In Section 2 we present a brief overview of the BC technologies, followed by the characteristics of BCT to governmental processes in Section 3. We then discuss in Section 4 potential benefits that might be achieved by developing, implementing and running BC applications as part of government

* Corresponding author.
E-mail address: M.F.W.H.A.Janssen@tudelft.nl (M. Janssen).

https://doi.org/10.1016/j.giq.2017.09.007

Available online 29 October 2017

processes, followed by possible design options to build different forms of BC technology applications in Section 5. In Section 6, we discuss the implications and the possible roles of government organizations, in line with their social mandates and available design and implementation options, to ensure that the BC applications deliver public value. In our conclusion we contribute to the research agenda on BC-applications in the public domain by presenting future research topics aimed at exploring the added value and to arrive at a better understanding of the consequences of BCT for governments.

2. Blockchain technology basics

On the 31st of October 2008 the white paper "Bitcoin – A Peer-to-Peer Electronic Cash System" by a mysterious Satoshi Nakamoto (2008) was circulated among an email list of cryptographers (Popper, 2015). The described system Bitcoin was launched as a digital service on the 3rd of January 2009. In the time since 2009 the digital currency system has grown in value of more than $60 billion in mid 2017 and is now the most well-known BC application, but more importantly it led to the rise of an ecosystem of innovative ideas and services that stretches far beyond the financial sector (Tapscott & Tapscott, 2016).

Bitcoin was the first system to include the BC data storage structure and has served as the basis for all BC implementations to follow in domains as wide ranging as the energy sector, (Burger, Kuhlmann, Richard, & Weinmann, 2016; Lavrijssen & Carrilo, 2017), supply chains & logistics (Iansiti & Lakhani, 2017; Korpela, Hallikas, & Dahlberg, 2017; Tian, 2016), the music industry (Rethink Music Initiative, 2015), and the healthcare sector (Hoy, 2017). BCT also goes under the name *Distributed Ledger Technology* (DLT). DLT is based on the idea that each participant has access to a shared ledger. The idea of having an open, universally accessible ledger was born with Bitcoin, and the system provided the first solution to the problem of establishing trust in an unsecure environment without relying on a third-party. This is a well-known challenge in distributed computing also known as the *Byzantine generals' problem* (Lamport, Shostak, & Pease, 1982). This problem refers to an army of generals in which each general commands one part of the army and are situated at distributed locations. The generals have different preferences, some nodes might pretend to communicate on behalf of a general, and together the generals must make a common decisions whether to attack, retreat or take any other actions. In Byzantine failure a node (representing a general), can pretend to be a correct one, but presenting different answers to different nodes to manipulate the outcomes. In digital currency research this problem is tackled using the Nakamoto Consensus to avoid double-spending (Van Valkenburgh, 2016).

The basic idea behind the BCT is that it allows actors in a system (called nodes) to transact digital assets using a P2P network that stores these transactions in a distributed way across the network (Back et al., 2014). The owners of the assets, and the transactions involving change of ownership, are registered on the ledger by the use of public key cryptography and digital signatures (Warburg, 2016). Every transaction is validated by the nodes in the network by employing some kind of a '*consensus mechanism*' (a consensus protocol). This works as follows. Whenever a transaction is entered into the P2P network, the nodes first validate the transaction. If the nodes agree on its legitimacy, they confirm the transaction and this decision is laid down in a block. This new block is added to the previous chain of blocks and as such locked. In this way, the latest block maintains a shared, agreed-upon view of the current state of the BC (Buterin, 2014).

All transactions are stored in a ledger which all involved nodes hold a copy of. *Blocks* are time stamped batches of valid transactions. For security reasons each block includes the hash of the prior block. The hash is used to identify the information and to ensure the integrity of the data. The linked blocks form a chain, hence the name 'blockchain'. Creating new blocks is known as *mining*. Note that it is not the hash pointers linking the blocks into a chain that gives a BC its security, it merely makes alterations of transactions in the BC easy to discover (Narayanan et al., 2016 pp. 11–13,83).

A ledger contains the shared and agreed-upon state of the BC and the list of transactions that were processed by the nodes. Every node in this decentralized system has a copy of the BC which is continuously synchronized with the other copies. In this way there is no centralized point of vulnerability that computer hackers can exploit. Taking one node down will not lead to a breakdown of the chain of blocks. This typical P2P architecture contributes to the security as well as the immutability of the transactions that are recorded in the BC. In addition, the distributed consensus protocol (which can have several forms such as majority voting, priority voting or having a minimal number of votes) ensures the data integrity of the transactions.

However, this does not mean that the BC is unalterable. The controlling parties that set up the BC (ranging from citizens to public or private organizations) can decide to alter the history of a BC (e.g. the split in the Ethereum BC in 2016 because of diverging points of view of how to handle a major hack (Atzei, Bartoletti, & Cimoli, 2017)). So whereas a BC is tamper evident because of the hash-based linking of blocks, that does not mean that it is unalterable (Narayanan et al., 2016). No BCT can guarantee total immutability, and social agreements between the controlling parties can lead to adaptation in the BC (Gervais et al., 2016). And in the case that a discrepancy in the process of adding blocks occurs which leads to a fork in the chain, then the network solves this by continuing to build on the longest chain, e.g. the chain with the most cumulative resources behind it (Nakamoto, 2008).

To illustrate the way BCT works, we use the example of a so called smart contract. BCT can be used for developing smart contracts in which the agreement on conditions by participants can be stored and once the conditions are met the changes outlined in the contract will be made. Smart contract defines the rules and penalties around an agreement and automatically executes and enforces the obligation in the contract. A smart contract can be defined as "a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated" (Buterin, 2014, para. 2). A smart contract is a program that runs on the BC and has its correct execution enforced by the consensus protocol (Luu, Chu, Olickel, Saxena, & Hobor, 2016). A smart contract contains information about a deal and will only be executed if the conditions are validated by all nodes in the network (Luu, Chu, et al., 2016).

A simple example to illustrate the working of a smart contract is the transfer of ownership of a property, e.g. a house. The buyer of the house enters the sum of money that needs to be paid for the property into a block. Only if the buyer gives his key to the seller within a certain time frame, the payment will be processed and the property registry is updated in the BC. If the key is not transferred, then the money is given back to the buyer. The smart contract contains rules for the transaction that cannot be changed during the process nor interfered with by one of the parties without the other one knowing. The smart contract might outline that others (trusted parties) have to confirm the transfer before the contract is executed to avoid dispute and ensure trust.

Another example in which a smart contract based on BCT can be especially useful is for voting. A smart contract can ensure that a voter in e.g. national elections, can only cast a vote once and can check if the vote is correctly stored by accessing the information. This can reduce potential voter fraud and makes manipulation of voting results more difficult because of the distributed network of nodes and the distributed consensus protocol that ensures the data integrity of the votes that are casted.

Both examples do require having Authentication, Authorization and Accounting (AAA) capabilities in place in order to develop the smart contract on the BCT. In the case of transfer of ownership, the conditions can be stored in the smart contract and once fulfilled, the transaction can be executed resulting in the registration of the new owner in the record. In this way fraud and corruption about assets can be avoided. Using such mechanisms in a smart contract can automate some intermediary roles of a notary in the buying and selling of real-estate, although important notary roles like drafting a contract and compliance checking and enforcing a contract cannot be automated by BCT. Research is needed to fully understand the potential of these smart contracts and to avoid mistakes.

Probably the biggest difference between BCT and conventional digital technologies originates in its distributed, P2P nature. BCs consist of distributed ledgers that are kept in sync via P2P mechanisms and pre-agreed rules about what new data can be added. This deviates from conventional situations in which one party maintains a database with all the data and decides upon the responsibilities to create, read, update, and delete (CRUD) data. Data governance by one organization is relatively straightforward as responsibilities can be centrally coordinated, although in practice data governance is a challenging endeavor. This centralized architecture is in contrast with BCT, in which each node in the network has a full copy of the transactions. Essential in BC is the contribution to higher data integrity in comparison to current implementations in government. *Data integrity* means that the information stored in a system corresponds to what is being represented in reality. Data integrity refers to a broad range of aspects like consistency, security, reliability, timeliness, non-repudiation and non-manipulation that need to be warranted. The distributed nature of BC ensures that manipulating and changing data without having consensus becomes harder, which results in better information integrity, although, complete integrity can never be guaranteed. Indeed this originates from the very nature of distributed computing, and the entering data by the source, whereas many existing applications are based on a single database which are hardly integrated with other sources.

The original BC application Bitcoin focused primarily on transactions of crypto currencies. However, since its origin in 2009, BC use cases have expanded into a wide range of sectors beyond the financial domain (Tapscott & Tapscott, 2016). BC applications can range from simple to complex transactions and information exchange and smart contracts can be used to regulate these transactions. Also the public sector has several services and transactions that could benefit from the use of BCT, or at least should investigate its potentials. Therefore, understanding the potential benefits is key to determining in which areas the BC technology can be effectively used within the public domain. In the next section we explore BCT for the public sector.

3. Blockchain in government

BC technology can be used for any transaction or information exchange that takes place in which the government is involved. The fundamental characteristics of this technology enables implementation in a wide range of processes for asset registry, inventory, and information exchange, both hard assets like physical property, and intangible assets like votes, patents, ideas, reputation, intention, health data, information etc. (Swan, 2015). The essence of a BC is that organizations can keep track of a ‘ledger’ and that organizations jointly create, evolve and keep track of one immutable history of transactions and determine successive events.

Governments from all over the world are conducting pilots using BCT. Government BC applications are diverse in nature and include digital identity, the storing of judicial decisions, financing of school buildings and tracing money, marital status, e-voting, business licenses, passports, criminal records and even tax records (see for examples Blockchain Projects, 2017). We recommend further research to compare the variety of initiatives and to analyze the source of benefits.

The BC technology requires situations in which multiple parties are involved in a transaction. A notable example is granting permits to the organizers of mass events, like concerts and demonstrations, which requires the municipality, police, fire brigade and health organizations to agree and to ensure they are prepared for dealing with the mass. Another example is the transfer of car ownership. To find a car owner, the car's transaction history has to be analyzed assuming that it contains an unambiguous property identifier. The owner of the car can be identified by searching a ledger as everybody has the same view on the BC. The rule states that only the owner can sell the car. When the car is sold a transaction needs to be created in which the previous owner confirms selling the car, the new owner confirms buying the car and the bank (or another party) confirms the payment for the transfer of the ownership. Another example is keeping an overview of the authorities provided in a public organization and the ability to change the authority only if there is agreement among nodes which are classified as being higher ranked in the hierarchy. As such, BC is a technology that replaces single databases by a distributed ledger of shared information, which should result in higher security and accessibility. This difference is schematically depicted in Fig. 1. Each node in the network contains a full copy of the BC, the transactions are recorded in the ledger and each node has access to the full history of transactions. Access to the ledger can be restricted, and the number of nodes as well as the type of consensus mechanism need to be determined. These choices influence the stewardship role of government, which we address in more detail in Subsection 6.5.

A final example is the use of BCT for land title projects. This BC applications is particularly useful when ownership records are not preserved in a systematic way or the operating organization is not trusted. In some countries the ownership of a land title is hard to detect. By using a BC application every transaction of land property should be registered. BCT prevents manipulation and loss of data. The transfer of land property requires that the lawful owner has to sign, for which there should be proof of ownership, no left mortgage should rest on the land property, and a payment (money transfer) from the buying to the selling party has to be made. BC can be used to protect the rights of the owner of the land, to resolve disputes, to make sure that ownership is correctly transferred and to prevent any unauthorized and fraudulent changes. However, BCT does not help to address the accuracy of the land titles, but rather seeks to clarify the authenticity of the title. In the case that input is manipulated and still complies with the conditions it will nevertheless be accepted by the network and added to the BC. Hence BC can be used as one of the instruments to fight corruption with land registries, but should be part of a wider institutional setting including other instruments for a legally correct and compliant land registry administration.

These examples show that BC applications can have significant effects on the way organizational processes are designed. E.g. in the case of using a BC applications for land registry organizations involved in land registry processes can directly interact with each other. This reduces the mediating role of the land register organizations who only need to focus on developing, maintaining and governing the BC application. Yet, if and how such organizations should be transformed to serve as owners and guardians of the BC application is still an open question. To the best of our knowledge, there are no deep analyses of these changing administrative processes and organizations in their institutional context yet and research in this area is required.

Some authors even go one step further by arguing that BC is “an institutional technology of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments” (Davidson, De Filippi, & Potts, 2016, p.1). Atzori (2015) even stated that BC can be viewed as technology that competes with the role of government in society. Technology competing with an institution might be

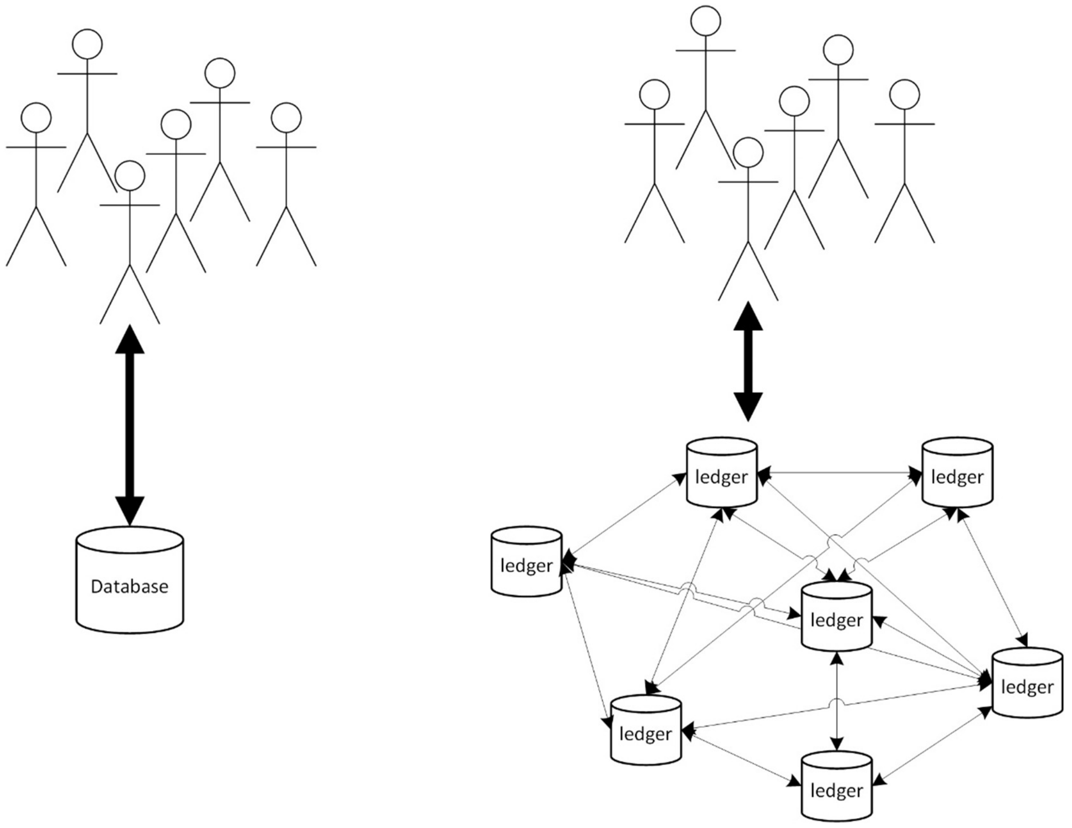

Fig. 1. Shift from central databases to distributed ledgers for information sharing.

considered as a technology-push, far-fetched and naïve, but nevertheless such propositions should not be ignored and research is needed to position this in a more realistic view which takes into account both technical and institutional elements. What the BCT has to offer is that instead of transactions being handled directly by government organizations, they can be handled by distributed ledger technology running on P2P platforms that are enabled and facilitated by (or on behalf of) government organizations. This raises questions about who will set-up, execute and maintain these architectures which will likely still be the role of government, but the actual transactions might be performed without the government.

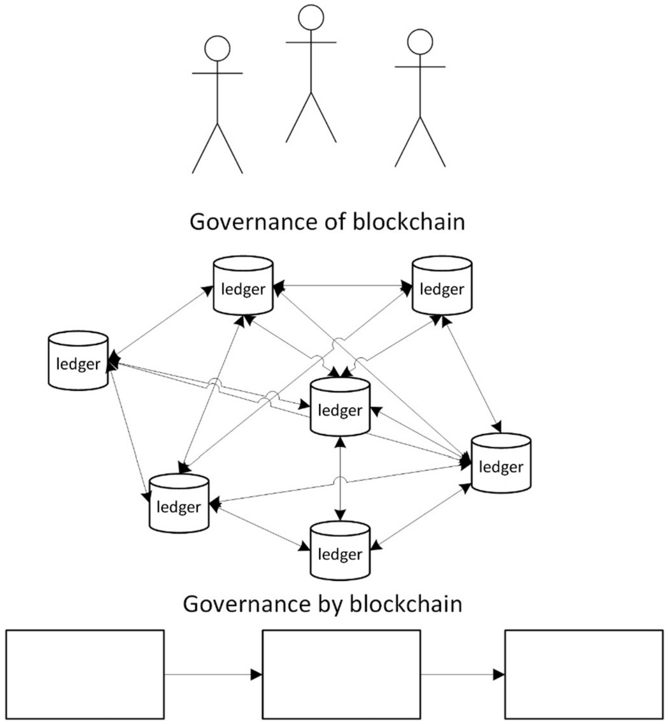

Fig. 2. Dual forms of governance.

Table 1
Potential benefits and promises of BCT.

Category	Benefits and promises	Literature	Explanation
Strategic	Transparency	Atzori (2015); Underwood (2016)	Democratizing access to data. History of transactions remains visible and every nodes has complete overview of transactions.
	Avoiding fraud and manipulation	Cai and Zhu (2016); Swan (2005)	Hacks or unauthorized changes are difficult to made without being unnoticed, as information is stored in multiple ledgers that are distributed.
	Reducing corruption	Kshetri (2017)	Storage in distributed ledgers allows for preventing corruption. For example by storing landownership in a BT and having clear rules for changing ownership which cannot be manipulated.
Organizational	Increased trust	Palfreyman (2015); Zyskind and Nathan (2015); Mainelli and Smith (2015); Swan (2005)	Trust in in process by increased control due to immutable recordkeeping and by verification of the data by multiple nodes.
	Transparency and auditability	Palfreyman (2015); Tapscott and Tapscott (2016); Atzori (2015)	Being able to track transaction history and create an audit trail. Also by having multiple ledger which can be accessed for consistency.
	Increase predictive capability	Tapscott and Tapscott (2016)	As history information can be traced back, this availability of the historic information increased the predictive capability.
	Increased control	Zyskind and Nathan (2015); Kraft (2016); Mainelli and Smith (2015)	Increased control by needing consensus to add transactions.
	Clear ownerships	Yermack (2017)	Governance need clearly defined and how information can be changed.
Economical	Reduced costs	Palfreyman (2015)Tapscott and Tapscott (2016); Ølnes (2016)	The costs of conducting and validating a transaction can be reduced as no human involved is needed.
	Increased resilience to spam and DDOS attacks	Gervais et al. (2016)	Higher levels of resilience and security reduces the costs of measure to prevent attacks
Informational	Data integrity and higher data quality	Tapscott and Tapscott (2016)	Information stored in a system corresponds to what is being represented in reality due to need for consensus voting when transacting and distributed nature. This result in higher data quality.
	Reducing human errors	Cai and Zhu (2016); Tapscott and Tapscott (2016)	Automatic transactions and controls reduces the making of errors by humans.
	Access to information	Palfreyman (2015); Swan (2015)	Information is stored at multiple place which can enhance the easy the access and speed of access.
	Privacy	Tapscott and Tapscott (2016); Zyskind and Nathan (2015)	User can be anonymous by providing encryption keys or access can be ensured to avoid others to view the information.
	Reliability	Tapscott and Tapscott (2016); Swan (2005)	Data is stored at multiple places. Consensus mechanisms ensures that only information is changed when all relevant parties agrees.
Technological	Resilience	Tapscott and Tapscott (2016); Swan (2005)	Resilient to malicious behavior.
	Security	Gervais et al. (2016); Tapscott and Tapscott (2016); Underwood (2016); Ølnes (2016); Mainelli and Smith (2015)	As data is stored in multiple databases using encryption manipulation is more difficult. Hacking them all at the same time is less likely.
	Persistency and irreversibility (immutable)	Atzori (2015); Underwood (2016); Swan (2005)	Once data has been written to a BC it is hard to change or delete it without noticing. Furthermore the same data is stored in multiple ledgers.
	Reduced energy consumption	Tapscott and Tapscott (2016)	Energy consumption of the network is reduced by increased efficiency and transaction mechanisms.

Governance plays a role in BC in two different ways as schematically shown in Fig. 2. On the one hand, *governance by BC* means that the BC implementation of a governmental process organizes information exchange and transactions between users. This is shown at the bottom of Fig. 2. Transactions can be fully automated and executed using BCT. This resembles how Bitcoin implementation sets conditions for digital money exchange. *Governance by BC* entails that governments develop a BC system which requires knowledge of the design options to develop the fitting type of BC architecture.

On the other hand, the development, execution, maintenance and adaptation of BC architectures and applications need to be guided. We term this *governance of the BC technology*, or BC governance for short, which determines how the technology operates and how the users can engage with it. All too often there might be a few experts who dictate the rules in which the application governs the users, whereas policy-makers should play a prominent role to ensure that public values and societal needs are fulfilled and taken into account in the design and governance of BC architectures and applications. Close cooperation between experts and policy-makers is needed to develop governance by BC on the one hand, and to ensure compliance with public values and societal needs for BC applications developed by other parties on the other hand. Understanding the design variables and implications of these variables on the realization of the benefits is an important research area to advance the understanding of BC architecture and applications. In the next section we critically assess the potential benefits and promises of BC technology.

4. Potential benefits and promises of BCT

In Section 2 we presented the characteristics of BCT such as its distributed, P2P nature and each node in the network having a full copy of transactions. How do these characteristics relate to potential benefits in the public domain? Many authors published a variety of benefits that might be accomplished by using BCT, as listed in Table 1. This long list of benefits are too good to be true and certainly not all will likely be accomplished at the same time. There was no review of benefits yet and many of the benefits are not supported by argumentation or empirical evidence. The benefits are stacked, are dependent on each other and whether they will be accomplished depends on the design decisions within the BC architecture and application development process. Basic benefits are related to improved data integrity and transactions that are irrefutable which in turn can result in being able to trace changes (transparency) which in turn support initiatives to reduce corruption and fraud. On the downside, one must take into account that distributed solutions like BC are much more inefficient than traditional centralized database solutions, are more difficult to scale up to higher capacity, and cannot be changed easily resulting in less flexibility (Ølnes, 2016). This is especially the case for open, public BCs like Bitcoin or Ethereum where future development needs to be supported by a majority of users (De Filippi & Loveluck, 2016).

The reliability of information is expected to be improved by using consensus mechanisms which ensures that only information is changed when all relevant parties agree. The security is created by having distributed ledgers which are harder to manipulate. Design choices determine whether users are anonymous or have an identity. For many government applications identity management will be a key aspect. Hence, BC should be connected with identity management systems which might be at the expense of other benefits like privacy. Identity controls will be one of the challenges when having a huge amount of users. How do you ensure that the user who has the key is the one who should have the key?

The table shows a diversity of benefits that are attributed to BCT, from which many of them might not be BC specific and require considerable organizational and institutional practices to let the BC system function in such a way that the benefits outweigh potential risks. From the description it becomes clear that some benefits are attributed to other technologies (like encryption, identity management) and are not BC specific. Some other benefits are not BC specific at all, like reducing fraud and corruption. BCT cannot prevent fraud in the provision of social services; the system of delivering social services needs to be changed to reduce fraud or corruption. Sometimes the benefits even become mythical. Swan views BC as a way to counter repressive political regimes (Swan, 2005, p. VIII). Also trust is not created by a technology. BCT can facilitate better control and audit which ultimately might result in more trust. However, a condition is having the necessary institutional arrangements in place that can be trusted. The reduction of energy is questionable as the use of more computing nodes might result in the opposite. The implementation and adoption determine if possible benefits can be realized. Hence, the benefits seems to be exaggerated and whether the benefits can materialize depends on the BC applications, their governance and the social and -institutional context for their use.

Realizing the benefits of BC requires understanding of government processes and the conditions and requirements posed on government. Current structures might need to be altered to enable distributed transaction management with a governance structure to guide it. In addition the adapted structure needs to take the societal requirements into account in order to ensure the functioning of a proper public administration that meets public values like equal access, transparency, accountability and privacy. Most of the benefits might also be accomplished using other technology means. This raises the question which benefits are BC specific and for which situations BC is the desired solution, while taking into account that the BCT is still evolving and thus subject to change.

Part of this evolution is addressing the BCT limitations like its current limits to scalability, flexibility and response time (Vukolić, 2015). Promising innovations like sidechains (Back et al., 2014) and drivechains, off-chain payment channels [e.g. Lightning Network] (Luu, Narayanan, et al., 2016), smart contracts (Bartoletti & Pompianu, 2017), colored coins (Rosenfeld, 2012), IOTA utilizing a blockless 'tangle' (IOTA, 2017) and more are aimed at overcoming such barriers.

Also some benefits might be exaggerated like the immutable nature and security. BCs powered by the consensus protocol Proof of Work (PoW) have been susceptible to 51% attacks, e.g. the miners that control more than half of the PoW resources can control the inclusion of new blocks and also possibly rewrite the BC history (Atzei et al., 2017). Money laundering, ransom ware, and hacking of exchanges and users have plagued Bitcoin and other permissionless BCs (Xu, 2016). However, recent research shows that the ratio of shady transactions in the Bitcoin network has been substantially decreasing over the past years (Tasca, Liu, & Hayes, 2016).

To summarize, realizing the benefits might be more cumbersome than initially thought. Furthermore, realizing these benefits might need modification of the current set of technologies, and implementations need to be guided by governance. Research into these emerging BC-related developments and their opportunities for government requires interdisciplinary research into possible BC architectures and applications that combines the evolutionary character of the technology with its institutional and social embedding. In the next section we present and discuss the design choices in BC architectures that influence the potential benefits of BC applications.

5. Blockchain technology design space

There is no such thing as "the blockchain" as BCT comes in many different forms, with different properties. The main variants are either private or public closed BCs (termed as a private/public permissioned BC) versus private or public open BCs (termed as a permissionless BC) (Mainelli & Smith, 2015; Walport, 2015). Table 2 shows the main variations, based on the level of openness and the allocation of permissions. Whether a ledger is public or private determines who has access to copies of the ledger, whereas the attribute of permissioned versus permissionless determines who maintains the ledger. Permissioned BCs are controlled by the owners and only they have the possibility to provide access and assign new nodes to the BC architecture. Generally, when a private BC is set up, a permissioned network is created in which participants need permission to join the network. Yet governmental organizations can also choose to develop a public BC, which can be viewed and mutated by the public under conditions set out by the governmental organization.

The roles of users in BC applications vary dependent on their read and write rights. Some users might only be able to read data, whereas others will create data by conducting transactions. In permissioned BCs only the appointed users can add new blocks and transactions to the BC. This entails that these operators of nodes in the BC are appointed by the owner of the BC architecture. In this way only trusted organizations can operate a node, and be involved in the consensus-making process for adding new information to the blocks. The operators might be limited to public organizations, but this reflects a design choice.

Governments need to discuss what type of BCT works best since there are benefits and trade-offs for every type. Understanding the most important design decisions is a key element. Control, data ownership, privacy and access are among the key design decisions. The more control is exercised, the less the BC system will resemble the original idea behind the BC vision.

A BC application can be open for all or restricted in some elements like voting and access to (parts of) data. Table 3 shows the main characteristics of open versus closed BCs. In an open BC all information can be viewed by others which might cause serious privacy problems, e.g. if health, personal or other

Table 2
Main variations in BC applications.

	Permissioned	Permissionless
Public	No restricted data access or transactions. Only a restricted set of nodes can participate in the consensus mechanism.	No restriction on access, transaction (data writing) or validation.
private	Restricted access, data writing and validation. Only the owner determines who can participate.	Restrictions on access and who can transact. No restriction on participation in the consensus mechanism.

Table 3
Comparing open and closed BC applications.

	Open blockchains	Closed blockchains
Who can update	Everybody	Appointed entities
Who can produce data	All users	Customers and/or partners
Incentive to follow rules	Economic	Reputation
Storage	Distributed	Centralized
Trust central actors	No	Yes
Transaction costs	Varies from low to high	Low
Capacity/throughput	Low/slow	High/fast
Immutability	Strong	Unclear
Currency/token	Yes	No
Examples	Bitcoin, Ethereum	HyperLedger, Corda

sensitive information is stored in the BC then access should only be granted when the conditions set by the data protection act are met. This requires encryption and access control to the distributed ledger. To this end, BCs can be extended with other technologies like encryption and business rules (Engelenburg, Janssen, & Klievink, 2017). For example, the European General Data Protection Regulation (GDPR) requires that users should be able to view their data, have the right to change or even to remove data (right to be forgotten) (European Parliament, 2016). In these cases, the BC application should be able to meet these requirements. This is an example for the role of government in *governance of BC* as introduced in Section 3 to make sure that the BC system complies with laws and regulations (Fig. 2).

Closed BCs do not need economic incentives and thus do not need a currency or token because the security is controlled by the consortium governing the BC, which is called a consortium consensus model (Van Valkenburgh, 2016). The developer of the BC applications can decide to have a limited number of nodes to be involved in the consensus mechanism. For example, if a citizen wants to update their data, only the citizen and the involved public organization (often the municipality) need to agree to make the change. Therefore defining which nodes have the permission to vote is another key design variable.

6. Implications for government

The potential benefits make BCT attractive for use by governments and other organizations. Yet its distributed nature and the need for making design choices requires transformations by government to reap these benefits. Whereas traditional systems have a relatively straightforward control, the distributed nature of BCT requires changes in responsibilities and new governance approaches. Implementing BC without extensive changes might not result in all derived benefits. Currently, most of the projects are technology-driven to explore the potential and find the limitations, but BCT is likely to mature which will result in putting the societal challenges central instead of the technology. In the following paragraphs we explore issues raised by BC implementation for e-government that need to be addressed.

6.1. Blockchain as a transformation driver

Creating information integrity and smart contracts can have a significant impact on how we organize the ICT-architectures, but also on how we govern the transactions. By the distributed registration of documents and assets the traditional roles of public administrations are challenged and new governance roles appear. Fig. 3 shows the gradual shift initiated by BCT by showing the changes in the information infrastructure level (bottom) and the governance level (top). This results into three stages of 1) traditional 2) BC information infrastructure and 3) transformation.

The left side in this figure shows the traditional situation in which one organization is usually responsible for certain data and owns, operates and maintains systems for ensuring this. One organization is responsible and the systems belong to that organization, e.g. for the provision of passports.

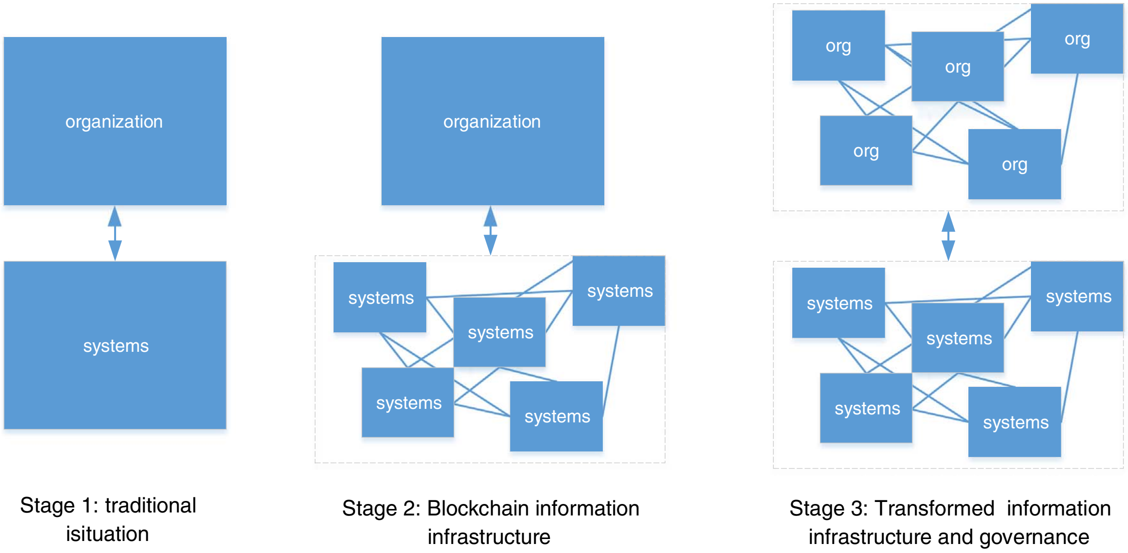
organization
systems
Stage 1: traditional isituation
organization
systems
systems
systems
systems
systems
Stage 2: Blockchain information infrastructure
org
org
org
org
org
systems
systems
systems
systems
systems
Stage 3: Transformed information infrastructure and governance

Fig. 3. Transformation from organization to network governance stages.

The data of the passport owner and the passport number are stored in a single database.

In the following stage BC is introduced as shown in the middle of the figure. In this figure the use of BC as an immutable distributed ledger for recording passport provisioning is shown. There are many nodes operated by different parties to ensure the distributed nature of BC. The information infrastructure resembles a network structure. The organization responsible for passport provisioning sets the rules for the governance of the BC: which parties are allowed to propose a transaction (in some countries municipalities), how the voting procedure for accepting transactions is arranged (multiple nodes should agree) and who is allowed to run a node. The organization is likely to develop and maintain the software for the distributed ledger.

Finally, the government is transformed and the governance by a single entity has changed into networked governance in which multiple parties are responsible for governing and transacting. BC is expected to facilitate direct interaction between citizens, providing administration without a governmental administrator and tailoring services provided by governments (Keyser, 2017). This requires new ways for how we govern our society. There are rules (smart contracts) which determine how new parties can be added to the governance layer and how decisions are made concerning the change of the BC applications. Which government organization is responsible for the software maintenance is defined and decision-making procedures and authorities are defined for how governance can change. In such a situation the ownership transfer of a car is done without any intervention of the land registry organizations. Once the car seller (e.g. a car dealer), buyer and bank provide the necessary information and agree the transaction is effected and the information updated.

6.2. Need-driven approach: There is no uniform solution

BC implementations can take various forms resulting in different benefits. BC implementations are largely technology driven and often various combinations of technologies are needed to make the BC architecture fit for e-government applications (Engelenburg et al., 2017). For example, transactions might be stored in a BC, but underlying data about the documents might be stored in another system to which the transactions refer. In other domains, experiments with permissionless BCs are already on the rise and a growing range of BC vendors already offer dedicated permissioned BC technologies.

For applications in the domain of e-government, institutional aspects play an important role and should be taken into account when using BCT. Like in cloud computing there will likely be a discussion about the geographical location of the servers and nodes. Some governments require that servers will be geographically located in their jurisdiction, as else different laws might apply.

Many of the current pilots and solutions might be driven by the technology, instead of by the societal problems that need to be tackled. BC advocates present this technology as a silver bullet for solving almost any type of information-related problem, but how to use this in practice is more cumbersome. The technology-driven nature can be explained by the immaturity of the technology and limited knowledge about its potential. In the maturity process a change from a technology-driven to a need-driven approach needs to be taken. In this approach the societal problems and public values need to be incorporated and the BC architecture and applications for e-government need to be developed in accordance with new governance models. In this realm BC might only be one of the elements.

6.3. Experimentation and the need for standardization and flexibility

Implementing BC is no linear, rational or deterministic process. There are many uncertainties and experimenting is needed to learn to know the technology in order to understand the possibilities and also its limitations. Furthermore, new technology applications often result in a change of human behavior which in turn influences technology applications (DeSanctis & Poole, 1994). Experimenting requires also that the applications can be changed and can be adapted to changing circumstances. The ability to adapt is often viewed as a critical success factor for ICT systems. Yet it is not clear how BC implementation will fit with this requirement of adaptability to address updates in implementation and governance. Small scale experiments are needed to explore this interaction between the technological characteristics of BC systems and the specific requirements from e-government processes.

In addition, when going beyond small scale experiments, any large scale implementation needs some level of standardization to ensure interoperability. A strategy of experimenting might be conflicting with the strategy of standardization. Trying to standardize an immature technology could also hamper the development of it and a non-suitable standard might be chosen.

6.4. Shared BC infrastructure provider

There are many experiments with BCT within the government (see for example: https://www.blockchainpilots.nl/). In these experiments often different technology and software are used, which might result in a fragmentation when they are also used in operation. Whereas this diverging strategy is needed to find useful applications and to mature the technology, this might result in a fragmentation and large duplication of efforts in the longer term. Therefore experimentation needs to be guided by standardization to ensure convergence to a common standard. Ølnes and Jansen (2017) plea for a BCT-based platform for running various applications in e-Government. Such a shared infrastructure avoids the development of a new infrastructure by each project and enables the reuse of existing efforts. Furthermore, it might not be clear who controls the technology and if the requirements from the legislative environment are met. Atzori (2015) argues that “In a world increasingly reliant on technology and ruled by networks, whoever owns and controls these platforms always have a significant power over civil society” (p. 29). For government this underlines the necessity to being able to manage and control the technology for the purpose of services that relate to public values.

On a general level Bitcoin/permissionless BC has properties that point toward an information infrastructure and thus can be very important as future infrastructures for open innovations (Ølnes, 2016). Many governments have established their own cloud infrastructure to foster innovation (which might be partly operated by private parties). In a similar vein the government might become a shared BC provider using an infrastructure that enables local governments, ministries and public agencies to create BC application and ensure safe, secure and reliable execution compliance with legislations. In this way the BC expertise can also be concentrated and joint standards can be created. Technology and also data standardization is needed for interoperability.

6.5. Data stewardship and accountability

BCT is expected to facilitate direct interaction between citizens, providing administration without a governmental administrator and tailoring services provided by governments (Keyser, 2017). Often it is stated that BC technology replaces the middleman. Using BCT it is possible to have no central authority or third party required to authorize, verify, and approve a transaction. For example, in Bitcoin there is no central bank to manage the currency. In many situations the government is steward for registering and updating all kind of registries. BCT might *disintermediate* the role of government by storing official records and offering the data. Still somebody has to design, operate and maintain the system. Equipment running BCT always owned and maintained by somebody, although they do not own or control the software running on it. BC might change the power balance among parties and in particular the *information stewardship* role can be affected. The emphasis will be on creating the infrastructure and governing its use and its adaptions to ensure the right data quality. Government can play the role of a trusted administrator who initiates and operates a registry, determines the transaction rules and audits applications to ensure proper functioning. In their role as data steward, governments will likely remain responsible for operating the applications and they can be held accountable in case of failure or when having data quality problems. As such BCT will require a reintermediation of the roles of government. It is likely that the roles of the government will be changing and more research is needed in this direction to explore the roles within the changing actor arena.

BC applications are designed by experts with only limited accountability for their design decisions to the public. Although BCT discusses democratizing data access it might be the other way around. Experts who design a system are a minority and dictate the rules in which the application governs the users. Miners provide the computing power and might only be interested in earning money and in improving their profits. Only a happy few can change the code and how the system is governed. A design will likely represent the interests of the actors. Although BCT might be used for supporting different values, its implementations are value-laden and reflect the design choices. A careful policy-making process should be in place in which societal needs are leading. In this process decisions should be accounted for, like for any other government decision. This role should ensure that the motivations behind decisions made by each agency and the performance and outcomes of the complete cross agency process can be accounted for.

6.6. Auditing blockchain applications

An audit is a systematic examination of the working by an independent party. Whereas in traditional auditing the focus is on auditing the transactions, the immutable (or at least difficult to change without noticing) nature shifts the emphasis of auditing to the system level. In BC both the software and algorithms need to be audited to ensure its proper functioning and the compliance with legislations should be analyzed. This changed nature of the auditing procedures needs to be explored for its consequences in the institutionalized environment of auditing services and related actors.

The algorithms embedded in the software determines if rules are met and transactions are correct. These "algorithms become increasingly autonomous and invisible, they become harder for the public to detect and scrutinize their impartiality status" (Janssen & Kuk, 2016, p. 371). Therefore there is a need to store and audit the algorithms of the BC. In open source the source software code is always open to the public. Although proponents argue that making source code available enable the public to review the code and improve the quality, others have questioned this. Both sides can be right dependent on the circumstances (Ven, Verelst, & Mannaert, 2008). In a similar vein, understanding the underlying algorithms of BC is not easy, as the materiality is difficult and specialized expertise is necessary. Nevertheless, the public should be able to relay on the proper functioning of software and algorithms. The open source literature can provide practices and guidance for realizing this and we suggest further research in this direction.

7. Conclusions

BC is an innovative, general purpose technology, offering new ways of organization in many domains for recording transactions, events, certificates and ownership. BC is a form of distributed computing in which transactions are democratized by introducing consensus mechanisms allowing a transaction to happen. Whereas evidence from cases of BC applications in the private domain are abundant, BCT also offers potential benefits in the domain of e-government. However, these are not easily realized and the implications for government need to be explored by means of interdisciplinary research that goes beyond the now common technology-driven approach toward BC applications. The potential benefits in terms of strategic, organizational, economical, informational and technological aspects identified in this paper. However, we also argue that reaching these benefits might be more cumbersome than thought.

We have discerned two perspectives for governments in relation to the rise of BC architectures and applications. On the one hand the perspective of *governance by BC*, in which public organizations adopt BCT for their own processes, like service provisioning, and in which BCT is used to govern transactions. The other perspective is termed *governance of BC*, or BC Governance, which determines how BC should look like, how to adapt to changes and should ensure that public values and societal needs are fulfilled. Both require in-depth knowledge of the BC technology and the situation at hand.

An extra challenge lies in the immaturity of the BCT itself, which is still evolving. Small scale experiments in e-government are required to explore possible applications in order to materialize the potential and to avoid costly failures. Design decisions determine how BC can be used, which benefits are gained and what limitations the implementation has. For large scale implementation, it is important to design for flexibility, one of the most important design criteria for e-government systems. This requires strong governance as the very characteristics of BCT has built-in mechanisms (consensus protocol and immutability of the records) that are at odds with flexibility.

A critical assessment of the potential benefits of BC for e-government requires research into the changes in the data stewardship and accountability role of governments. More research into creating trust, dis- and re-intermediations, organizational transformation, governance models, design variables, auditing and the effects on the benefits and limitations are needed. This calls for a co-evolving process between a technology that is still under development and finding the matching governance response to stimulate the positive effects of the use of BC applications while mitigating possible unwanted consequences for society at large. A process of experimentation by governments themselves for BC applications in their own services seems paramount in order to gain a deeper understanding of the working of the BC as a complex socio-technical system and to find and possibly redefine their own role and functions within a changing institutional environment.

Acknowledgement

The authors would like to thank Tomasz Janowski for his detailed reviews and suggestions.

References

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts (SoK). In M. Maffei, & M. Ryan (Vol. Eds.), *Principles of security and trust. POST2017. Lecture notes in computer science*. *vol. 10204*. *Principles of security and trust. POST2017. Lecture notes in computer science* (pp. 164–186). Berlin, Heidelberg: Springer. http://dx.doi.org/10.1007/

978-3-662-54455-6_8.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. *Open science review* (https://www.blockstream.ca/sidechains.pdf).

Bartoletti, M., & Pompianu, L. (2017). *An empirical analysis of smart contracts: platforms, applications and design patterns.* (arXiv:1703.06322, March 18th 2017).

Blockchain Project Dutch Government (2017). via: https://www.blockchainpilots.nl/resultaten.

Burger, C., Kuhlmann, A., Richard, P., & Weinmann, J. (2016). *Blockchain in the energy transition: A survey among decision-makers in the German energy industry.* Berlin: Deutsche Energie-Agentur GmbH & ESMT European School of Management and Technology (November 2016).

Buterin, V. (2014). Ethereum White Paper: A next-generation smart contract and decentralized application platform. *Ethereum white paper* (Retrieved from https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf).

Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation, 2*(1), 20.

Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting governance: The new institutional economics of distributed ledger technology (July 19th, 2016). Available at https://ssrn.com/abstract=2811995.

De Filippi, P., & Loveluck, B. (2016). The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691.

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science, 5*(2), 121–147.

Engelenburg, S.v., Janssen, M., & Klievink, B. (2017). Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, events and blockchain technology. *Journal of Intelligent Information Systems*. (forthcoming) https://doi.org/10.1007/s10844-017-0478-z.

European Parliament (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union* L199/1, 4.5.2016.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 3–16). ACM (Retrieved from http://dl.acm.org/citation.cfm?id=2978341).

Hoy, M. B. (2017). An introduction to the blockchain and its implications for libraries and medicine. *Medical Reference Services Quarterly, 36*(3), 273–279. http://dx.doi.org/10.1080/02763869.2017.1332261.

Iansiti, M., & Lakhani, K. R. (2017). *The truth about blockchain. Harvard Business Review* (January/February 2017).

IOTA. https://iota.org/https://blog.iota.org/iota-luxoft-and-st-petersburg-polytechnic-university-supercompute-the-tangle-33092417ec0c accessed on September 21st 2017.

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly, 33*(3), 371–377. https://doi.org/10.1016/j.giq.2016.08.011.

Keyser, R. (2017). Blockchain: A Primer for Governments. February 6th 2017. Retrieved from http://www.viewpointcloud.com/blog/government-technology/blockchain-governments-primer/.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. *Conference: Hawaii international conference on system sciences (HICSS), At Big Island, Hawaii, January 2017. Volume 50*http://dx.doi.org/10.24251/HICSS.2017.506.

Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications, 9*(2), 397–413.

Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly,* 1–23.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS), 4*(3), 382–401.

Lavrijssen, S., & Carrilo, A. (June 2, 2017). Radical innovation in the energy sector and the impact on regulation. *TILEC Discussion Paper No. DP 2017–017* (Available at SSRN: https://ssrn.com/abstract=2979206).

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 254–269). ACM (Retrieved from http://dl.acm.org/citation.cfm?id=2978309).

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharing protocol for open blockchains. *Proceedings of the 2016 ECM SIGSAC conference on computer and communications security (CCS 2016), Vienna, Austria, October 24–29 2016* (pp. 17–30). . http://dx.doi.org/10.1145/2976749.2978389.

Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives, 3*(3), 38–69.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted, 1*(2012), 8.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press (Retrieved from https://www.google.com/books?hl=en&lr=&id=LchFDAAAQBAJ&oi=fnd&pg=PP1&dq=narayanan+bitcoin+and+cryptocurrency&ots=ArkGbX3KhC&sig=NZmYEUYu_GuLf2vJQuxlpu9nxwA).

Ølnes, S. (2016). Beyond Bitcoin enabling smart government using blockchain technology. In H. J. Scholl, (Vol. Ed.), *Proceedings of the International Conference on Electronic Government, EGOV2016. Vol. 9820. Proceedings of the International Conference on Electronic Government, EGOV2016* (pp. 253–264). Springer LNCS.

Ølnes, S., Jansen, A., Janssen, et al. (2017). Blockchain technology as s support infrastructure in e-government. *Proceedings of the international conference on electronic government, EGOV2017. vol. 10428. Proceedings of the international conference on electronic government, EGOV2017* (pp. 215–227). Springer LNCS.

Palfreyman, J. (2015). Blockchain for government? Retrieved from https://www.ibm.com/blogs/insights-on-business/government/blockchain-for-government/.

Popper, N. (2015). *Digital gold - Bitcoin and the inside story of the misfits and the millionaires trying to reinvent money* (1st ed.). New York, NY, USA: HarperCollins.

Rethink Music Initiative (2015). *Fair music: Transparency and payment flows in the music industry.* Boston: Berklee Institute of Creative Entrepreneurship (July 14th 2015).

Rosenfeld, M. (2012). Overview of colored coins. December 4th 2012. Retrieved from https://bitcoil.co.il/BitcoinX.pdf.

Swan, M. (2015). *Blockchain: Blueprint for a new economy.* O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). *The impact of blockchain goes beyond financial services. Harvard Business Review* (Retrieved from https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services).

Tasca, P., Liu, S., & Hayes, A. (2016). The evolution of the Bitcoin economy: Extracting and analyzing the network of payment relationships. Available at SSRN. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762.

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. *13th international conference on service systems and service management (ICSSSM), 24–26 June 2016, Kunming, China*http://dx.doi.org/10.1109/ICSSSM.2016.7538424.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15–17.

Van Valkenburgh, P. (2016). *Open matters — Why permissionless blockchains are essential to the future of the internet.* Coin Center62 (Retrieved from https://coincenter.org/files/2016-12/openmattersv1-1.pdf).

Ven, K., Verelst, J., & Mannaert, H. (2008). Should you adopt open source software? *IEEE Software, 25*(3), 54–59.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *International workshop on open problems in network security* (pp. 112–125). Cham: Springer.

Walport, M. (2015). *Distributed ledger technology: Beyond blockchain.* UK Government Office for Science (Retrieved from https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain).

Warburg, B. (2016). How the blockchain will radically transform the economy. *TEDSummit*TED Talk (June 2016. Retrieved from https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy?language=en).

Webb, A. (2015). 8 tech trends to watch in 2016. *Harvard business review, December 8th 2015* (Retrieved from https://hbr.org/2015/12/8-tech-trends-to-watch-in-2016).

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation, 2*(1), 1–16. http://dx.doi.org/10.1186/s40854-017-0062-0.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7–31.

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), e0163477. http://dx.doi.org/10.1371/journal.pone.0163477.

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE security and privacy workshops (SPW2015)* (pp. 180–184). .