Blockchain Technology as Infrastructure in Public Sector – an Analytical Framework

Svein Ølnes
Western Norway Research Institute
Sogndal, Norway
sol@vestforsk.no

Arild Jansen
University of Oslo
Oslo, Norway
arildj@jus.uio.no

ABSTRACT

The blockchain technology has evolved beyond traditional payment solutions in the finance sector and offers a potential for transforming many sectors including the public sector. The novel integration of technology and economy that open public blockchains have brought represents both challenges to and opportunities for enhancing digital public services. So far, the public sector has lagged behind other sectors in both research and exploration of this technology, but pilot cases show that there is a great potential for reforming and even transforming public service delivery.

We argue that the open blockchain technology is best understood as a possible information infrastructure, given its universal, evolving, open and transparent nature. A comparison with Internet is meaningful despite obvious differences between the two. Based on some case studies, we have developed an analytical framework for better understanding the potential benefits as well as the existing challenges when introducing blockchain technology in the public sector.

CCS Concepts

- **Applied computing** → **Computers in other domains** → **Computing in government** → E-government; *Blockchain*

KEYWORDS

e-Government, bitcoin, blockchain technology, information infrastructure

ACM Reference Format:
Svein Ølnes and Arild Jansen: Blockchain Technology as Infrastructure – an Analytical Framework. In *Proceedings of 19th Annual International Conference on Digital Government Research (dg.o'18)*

1 INTRODUCTION

Blockchain technology (BCT) have been met with significant acceptance in recent years, and the technology has developed platforms for various applications in different areas. We find applications in other areas where secure transactions have to be carried out in an otherwise unsecure, unreliable environment like the Internet. Blockchains, including peer-to-peer networking and consensus mechanisms provide secure identification and authentication in various types of distributed computing environments, without the need for a trusted third-party, see e.g. [1], [2] and [3].

Some of the most important features of the open blockchain technology are its global nature and scope, its decentralized and distributed character, its built-in transparency and independence of trusted parties. These features are particularly important in countries vulnerable to corruption and in which there is a general distrust in government on the part of citizens and businesses. However, as our use cases show, most countries can benefit from the global reach and openness that the open blockchain technology offers.

Although BCT has grown remarkably as a foundation for many novel innovations, it is still a somewhat immature technological platform. At present, it seems most suitable for digital ID management and secure record-keeping and document-handling, which are core governmental activities. A blockchain can provide a secure, verifiable record of every single transaction ever made [4], whether it is a financial transaction or a transaction involving a governmental procedure (e.g. recording and timestamping a public document). This gives the technology a potential for beneficially changing secure document management in the public sector.

Many of the [proposed] applications focus on its use in a single organization. We will strongly hold that the real potential of this technology can only be realized when one takes a national, or even international perspective and understands the blockchain technology as an open platform and an emerging information infrastructure (II), understood as "a shared, open and unbounded, heterogeneous and evolving network of technical and non-technical elements" for many different types of application. Thus, building a blockchain based II implies that focus must be on openness and standardization along with an evolving and flexible nature. A comparison with Internet is meaningful despite obvious differences between the two and we discuss both the similarities and the differences in the chapter about BCT and II.

The specific aim of this paper is to discuss how and in what ways the blockchain technology can be used as an infrastructure

dg.o '18, May 30-June 1, 2018, Delft, Netherlands
© 2018 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6526-0/18/05.
https://doi.org/10.1145/3209281.3209293

for specific areas in government. Most governments still have challenges with authentication and validation of documents of different types (e.g. certificates, licenses) and the problem of cross-border handling of such documents is even more challenging. This is also the case for personal IDs for accessing digital services, where the individual countries mostly have solutions in place, but where cross-border interoperability to a large extent is missing. These are only two of a range of governmental support services that can benefit from the use of a blockchain based system.

We explore a few selected use cases from different countries where secure and verifiable document-handling (certificates, licenses, title deeds) and digital identities are involved and where blockchain technology is at the base of the cases. Thus, the research objectives of our paper are:

1) To study how governments may benefit from using blockchain technology as a support infrastructure, and

2) to present a framework for analyzing both driving forces and challenges for its diffusion and use in the public sector

Our paper mainly discusses open, public blockchains given the overarching ideas of information infrastructure. We use Bitcoin as the example of an open blockchain although the content of our paper relates to most open blockchains. Throughout the paper we denote blockchain technology with BCT and blockchain with BC. We try to be consistent in writing the Bitcoin system (including the consensus model etc.) with a capital 'B' and the bitcoin currency with a lower-case 'b'.

1.1 Method Description

Our research approach is exploratory, analyzing the potential for adopting BCT through the lenses of information infrastructure. The empirical base is studies of pilots exploring the use of BCT in the public sector and a survey among Norwegian governmental agencies about blockchain. The survey was carried out by the consultancy companies Sopra Steria, Capgemini, and Accenture as part of preparing a conference report [5].

We have also conducted a workshop on the use of blockchain with around 50 participants from public sector organizations[2] and followed up with interviews of representatives from the Norwegian Tax Administration and the Norwegian Labour and Welfare Administration on their blockchain-related projects. Recent literature overview shows that there is still not much research published regarding the use of BCT in the public sector [6]. The current version 13.5 of the e-Government Reference Library (EGRL) does not include many publications on this topic. Of 9,901 references only six relates to BCT (Ølnes, op. cit.).

In describing the selected cases for Bitcoin and blockchain technology in the public sector, a case study approach [7] has been used. The use cases presented have been chosen both for their high relevance for the public sector and for illustrating different challenges with BCT, especially connected to the potential of the technology to evolve into an information infrastructure. We also wanted to select use cases from different countries and different thematic areas. They have been studied in varying detail. The case study method is especially useful in situations where the researcher has little or no control over the object to be studied, and for its usefulness in answering "how" and "why" questions [7]. This is the case for BCT in e-Government context where to date there are few obvious use cases to study.

1.2 Structure of the Paper

The rest of the paper is organized as follows. Chapter 2 provides a description of the technological foundation, focusing on the Blockchain technology and some current applications. Chapter 3 analyzes this technology in an information infrastructure perspective. In Chapter 4, we discuss selected use cases based on BCT. The cases range from proof of concept (PoC) to full-fledged applications and serve to illustrate the understanding of BCT as a potential information infrastructure. In chapter 5 we outline an analytical framework that aims at supporting the analysis of challenges as well as driving forces for the diffusion and adoption of BCT in the public sector. Our last chapter concludes our findings and addresses further research.

2 BITCOIN AND BLOCKCHAIN TECHNOLOGY

BCT applications. build on well-established research and standards in cryptography including earlier attempts to create virtual currencies (see [8], [9], [10], and [11]). The core principles of Bitcoin are (1) the peer-to-peer architecture, (2) the novel use of blockchain as storage, including hash linking and time stamping, and (3) the consensus mechanisms framing the rules and the security model [12]. The blockchain itself is a distributed database that maintains a continuously growing list of ordered records called *blocks*, containing *transactions.* A transaction can hold different types of data. Each block contains a timestamp and a hash pointer that links to the previous block [13]. In Bitcoin, the individual bitcoins are also linked together through the transactions (ibid.). Contrary to many beliefs it is not the cryptographic linking (by hash pointers) between blocks that makes the Bitcoin blockchain secure; it is the consensus model and the proof of work (PoW) method [13]. Linking blocks with hash pointers makes a blockchain tamper evident, but securing it with proof of work (PoW) makes it tamper resistant (ibid.). The PoW based security model relies on the presumption that the cost of compromising the system must outweigh the profit from doing so.

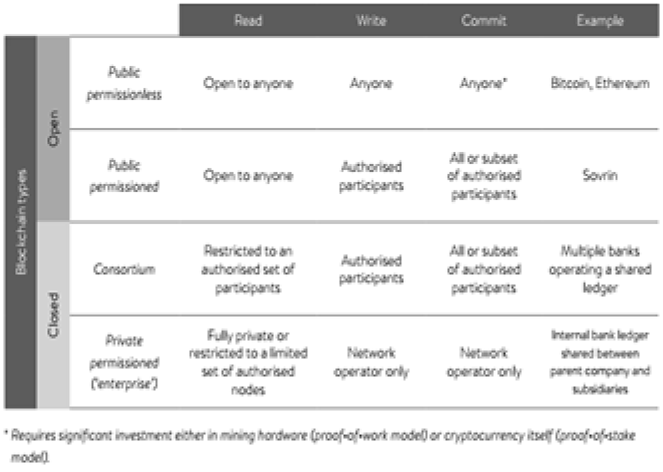
Currently the Bitcoin blockchain is limited to handling a theoretical maximum of seven transactions per second [13] and is therefore not well suited for high volume transactions. However, for efficient storage of more persistent objects and assets (e.g. certificates, licenses etc.) this limitation is of minor concern. These types of objects do not change ownership so frequently that the relatively slow transaction speed of Bitcoin becomes a challenge.

[2] Workshop at the Norwegian Conference on ICT in the public sector (NOKIOS - http://www.nokios.no/kurs_ws_17/)

The only negative effect of the present capacity problems is higher fees. What is stored on the Bitcoin blockchain is a hash (a "fingerprint") of the document (e.g. a license, a certificate, a will, a title deed etc.), not the document itself [14]. Sward et al. (op. cit.) describe the various methods used for this type of storage as well as methods to retrieve the information.

The cost of using an open blockchain like Bitcoin will be transaction costs in the form of fees. A transaction in Bitcoin is usually a transfer of an amount of bitcoin from one user to another. A transaction can also have an additional information payload and only carry a fee and no other value transfer [15]. This would be the case if a public sector agency should use Bitcoin or another permissionless blockchain. The fee is decided by the user and can range from zero to more than 10 USD in Bitcoin depending on the queue of transactions and how fast you need your transaction to be processed.

Although this paper focuses on the blockchain technology per se, it is important to understand how the bitcoin currency and the underlying blockchain technology is tightly interwoven [13]. An open, permissionless blockchain cannot exist without incentives or compensating mechanisms like the currency bitcoin (ibid.). Even if the blockchain can contain information other than the Bitcoin currency transactions, the currency is at present a crucial incentive to secure the transfer of ownership of information and assets.



Blockchain types			Read	Write	Commit	Example
Blockchain types	Open	Public permissionless	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ('enterprise')	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

* Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model).

Figure 1: Main types of blockchains segmented by permission model (from Hile and Rauchs [16])

As the above figure shows, there are more nuances to the open and closed blockchain perspectives. An open, public blockchain can also be permissioned. The permission aspect refers to the different types of permissions that are granted to the participants of a blockchain network [16]. The permissions in the table above are read, write, and commit. 'Read' is the ability to read information from the blockchain, 'Write' is the ability to conduct transactions, and 'Commit' is the ability to append data to the blockchain. For the public sector we believe that open BC systems, comprising both permissionless and permissioned BCs, are the most interesting and relevant given the potential of developing into an information infrastructure, and we will concentrate on this dimension in our paper.

An important part of blockchain development is its governance. In e.g. Bitcoin, no single group of stakeholders (e.g. miners, full node clients, core developers) is in full control, and consensus between the different groups has to be reached. Changes to the protocol are proposed through BIPs (Bitcoin Improvement Proposals) and are then voted on by miners. Full node clients "vote" by downloading upgraded versions of the reference client, or choosing not to download [17]. However, the recent forks resulting from a very intense scaling debate concerning whether to raise the size of blocks in order to increase the capacity of the blockchain has raised concerns and caused many people to describe the debate as a governance crisis [17]. Bitcoin, however, does not have any way of managing conflicts, that can lead to paralyzing deadlocks or contested forks, both of which can be harmful to the overall ecosystem (ibid.). Thus, the governance model of blockchain technologies is important if the technology also is to be used as a platform and infrastructure for public digital services.

The figure above shows the layered architecture of the Bitcoin blockchain network. The first three layers constitute the base. Over them, there may be additional layers for various purposes, e.g. payment channels for faster off-chain transactions, sidechains and drivechains for new use of the Bitcoin blockchain without disturbing the main blockchain and at the same time enjoy the high security of Bitcoin, and layers enabling smart contracts on the Bitcoin blockchain.

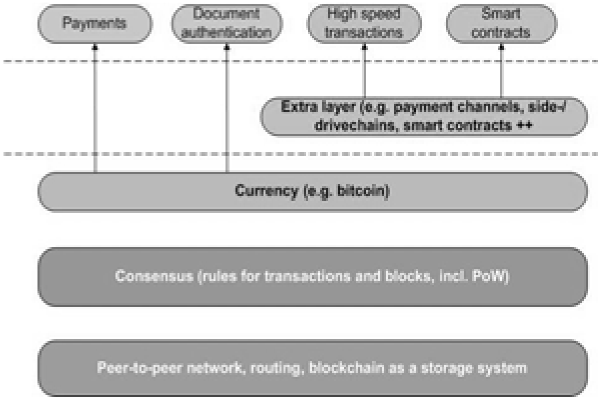

Payments
Document authentication
High speed transactions
Smart contracts
Extra layer (e.g. payment channels, side-/drivechains, smart contracts ++
Currency (e.g. bitcoin)
Consensus (rules for transactions and blocks, incl. PoW)
Peer-to-peer network, routing, blockchain as a storage system

Figure 2: Layered architecture of open blockchains, exemplified by Bitcoin.

Bitcoin originally focused on transactions of the digital currency. However, its use has since expanded into a wide range of sectors beyond the financial domain [18]. BCT applications can range from simple to complex transactions and information exchange and smart contracts can be used to regulate these transactions. Therefore, the key to understanding its potential, not least in the public sector, is to investigate in which areas the BC technology can effectively be used within its legal framework. In a study on how to use BCT in the Swedish land register administration, four potential benefits are pointed out: 1) less need for trusted third parties, 2) the number of steps and time elapsed to carry these out may be shorted down significantly and 3) the need for paper copies may be dramatically reduced, and 4) digital signatures result in a simpler authentication process [19]. We discuss this use case in more detail in chapter 4.

3 BLOCKCHAIN IN AN INFRASTRUCTURE PERSPECTIVE

An ICT infrastructure is usually regarded as the collection of hardware and software components, including networks that are required to enable communication and interoperations between ICT systems. Ølnes and Jansen [20] have shown that the generic BCT (including the consensus and security mechanisms) are becoming platforms for many applications, such as securing document handling and other types of digital assets, gradually building a heterogeneous and growing user base. However, one challenge is how to maintain backward compatibility as well as horizontal equivalence across different combinations of capabilities.

ICT infrastructures are primarily understood as technical facilities. However, the growth of the Internet, including WWW created a need for a holistic, socio-technical and evolutionary approach when studying such networks of distributed, but interlinked information systems, usually denoted as information infrastructure. Following Hanseth and Lyytinen [21] and Star and Ruhleder [22], we understand Information Infrastructure (II) as "a *shared, open* and *unbounded, heterogeneous and* evolving *socio-technical system consisting of a set of IT capabilities and their user, operations, and design communities.*" An infrastructure is being built over time in a step-wise manner where "different actors shape, maintain, and extend it "in modular increments, not all at once or globally" [22]. Because this dispersed and distributed ownership, the lack of centralized control is a fundamental attribute of an II. Consequently, different actors shape, maintain, and extend an II "in modular increments, not all at once or globally" [23].

3.1 Blockchain technology as information infrastructure

From the outset, BCT was designed to support cryptocurrencies and similar applications and was not intended to comprise a general-purpose platform. First of all, an open, permissionless BCT and its related applications are [in principle] available to everybody, which demonstrates its *openness.* Furthermore, as we have described above, many new applications have been built on blockchain platforms (see e.g. Figure 1), clearly indicating the potential of this technology to be *shared* across multiple communities in various ways. These developments also demonstrate its *evolving* nature, including a growing number of new platform, as we have illustrated in Chapter 2.

The *control* of an II is, as illustrated above, distributed and dynamically negotiated [23]. Blockchains, as represented by e.g. Bitcoin, Ethereum etc, is clearly a distributed technology as the main purpose of its design has been to avoid central control, e.g. by trusted third-parties. It was from the outset developed as a peer-to-peer network technology [1]. The recent debate over the block size [24] shows that no party is in control of the changes to be made and that these changes must be negotiated dynamically: miners have their say, full node clients have their say as well as core developers, but none of the groups can dictate the terms. This has been, and is currently, a subject of heated debate, and the community has not yet reached a conclusion on the scaling issues [25].

There is, however, also some fundamental differences between Internet and blockchains. The design of Internet (understood as the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide), was based on strictly layered and modular architecture. This implies that each layer has a limited set of capabilities and offers a well-defined (functional) interface. Although blockchain technology can me (conceptually) described in a similar manner, cf. figure 2 above, it does not follow such principles, in that applications on a higher level (layer in the protocol stack) do not build on identical lower level functionality, which may imply that horizontal interoperability on each layer is not possible, e.g. between different blockchain implementations.

Furthermore, Internet is based on the end-to-end principle, implying that application-specific features reside in the communicating endpoints, rather than in intermediary nodes. This result in that that each node is as simple as possible has minimum functionality. One consequence is that security functions (other than that those necessary to guaranty secure delivery of IP packages) were not part of the original Internet (but is now taken care of on top of the TCP protocol [26]. Similarly, security functions aimed at data quality assurance are not part of the core BC technology, but have to be implemented in each application. There is no common standard for such functionality across different BC application, e.g. cryptocurrencies. Thus, if BCT is going to comprise the basis for a support infrastructure (in government or outside), standardization is necessary. The Internet is a global network that comprises many voluntarily interconnected autonomous networks, without a central governing body. Standardization of the core protocols (IPv4 and IPv6) is an activity of the IETF, a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise. Similarly, interoperability is maintained by ICANN, administering the principal name spaces of the Internet [27].

BCT is governed in a somewhat different way and the governance model differs between various blockchain systems. For Bitcoin there is so far no formal governing bodies. The main constituencies comprising the Bitcoin community, e.g. the (full node) users, the miners, the developers, the service providers, and the merchants must agree on changes to have them deployed [15]. De Filippi and Loveluck [28] distinguish between two distinct coordination mechanisms: governance by the infrastructure (achieved via the Bitcoin protocol) and governance of the infrastructure. It is the latter that needs consensus between the primary interests (constituencies). They conclude that lessons from

Table 1: The characteristics of an infrastructures and different types of BCT based platforms

Property	**Information infrastructure, e. g. Internet**	**Permissionless Blockchain/Bitcoin**	**(Public) permissioned Blockchain**
Open	Yes, allowing unlimited connections to user communities and new capabilities	Partly yes. it is open to any users and offers a platform for payment system and secure document/asset handling	Public BC may be open to most citizens and other relevant actors
Shared	Universally by all stakeholders and across multiple IT capabilities	Potentially shared among those who are involved in building and maintaining this platform	Possibly restricted by those implementing the private BCs
Installed base	The current Internet applications are integrated with its users and use practices, still growing exponentially	The present installed base is limited, which may stimulate innovations but lack the networks effects	Limited, depending on the type of application it is aimed at.
Evolving	Yes, unlimited by time or user community. Both linear and nonlinear growth	Yes, although it may be too early to say how. Although it is a new technology, Bitcoin has demonstrated innovative potential.	In general, yes, but we have limited experience. Will have a problem of keeping up developing pace compared to permissionless BCs
Control	Distributed and dynamically negotiated. Standardization is regulated by formal procedures	Distributed control based on open source software. Changes are dynamically negotiated in user community. Procedures for standards are missing.	Centralized, but to a limited set of stakeholders

the past regarding both the successes and failures of Internet governance should be taken into account when developing the Bitcoin governance (op. cit.).

3.2 The installed base and blockchain technology

Of particular importance in an (information) infrastructure is its *installed base,* including both technical and non-technical elements. The evolution of IIs are path-dependent due to the "living legacy" of existing technical solutions along with organizational, economic and legal elements, interconnected practices and regulations that are often institutionalized in the organization [21].An adequate understanding of the installed bases is particularly important in building IIs in governments (eGovIIs), as an increasing number of information systems are shared in order to provide online government services, and the dynamics related to these systems often require both forward flexibility and backward compatibility. Hanseth and Lyytinen (op. cit.) emphasize that the understanding of the installed base of an information infrastructure is essential for its governance, not least in order to handle the existing collection of legacy systems which may be barriers for innovations.

The installed base of the blockchain technology is currently limited, as its applications have a short history. However, we see an increasing social and technical diversity where new applications and various platforms are emerging, e.g. new altcoins, smart contracts [29], sidechains [30]. In comparison, it took more than 20 years for the Internet to gain acceptance on a broader scale.

This limited installed base may both stimulate and inhibit innovations. On the one hand, it may enable the development and diffusion of new applications as there are few "technical bindings" such as legacy systems. New users can therefor start to use innovative solutions if they are sufficiently attractive or meet specific needs. The growth of cryptocurrency and various electronic cash systems clearly illustrates this. On the other hand, the lack of bonds to an existing installed base– for example, users of existing applications in relevant areas (such as payment systems, secure document handling and asset management etc.) – may imply that there are few incentives for adoption of new applications based on blockchain technology unless they are made more attractive. The growth of the Internet represents a good illustration; from the outset, it had no "legacy" applications to tackle. On the other hand, Internet benefitted from using the existing (technical) infrastructure of telecommunications. For BCT, the challenge is to stimulate the development and use of BC applications that can gain momentum and through network effects build a sufficient installed base, and at the same time benefit from existing infrastructure elements in government, see also the discussion of bootstrapping below.

However, as we illustrate below, the blockchain technology is evolving beyond its primary application area and comprise platforms that already support a range of applications, including secure document and asset management in other areas, see [20]. The discussions are summarized in Table 1 above.

Hanseth and Lyytinen [31] distinguish between two types of horizontal IIs: *application and support infrastructure*. We may conceptualize the blockchain technology platform as an emerging support infrastructure, while bitcoin and other digital currencies are part of the application layer. By so doing, we do not impose any restriction on how these technologies may evolve, as we do not yet know how new applications, such as secure document handling, smart contracts, digital ID management etc. will be realized on a growing support infrastructure.

The structure and development trajectory of the blockchain technology has been compared to that of the Internet, see e.g. Valkenburgh [12] and Ølnes and Jansen [20]. Although such comparisons may result in misleading associations, we believe there are some lessons to be learned from the history of building the Internet. The kernel of Internet architecture is essentially the TCP/IP protocol suite, built in a layered and modular way. Furthermore, the Internet is transparent and neutral to any type of information being sent across the network (as unfiltered data). Equally important is its basic characteristic: being open, global and borderless with no censorship. Thus, based on the end-to-end-principle (see e.g. [32]), the Internet may be considered an "unintelligent" network, meaning that there is minimum functionality inside the network, making it efficient, flexible and dynamic. Similarly, the blockchain platform, including Bitcoin, is a transaction-processing network because it pushes most of its "intelligence" to the edges, thus being able to support various smart devices. It does not offer a range of financial services and products, and it does not have automation and various features built in, thus making the interfaces much simpler, and thereby simpler to support innovations, analogous to Internet [33]

3.3 Infrastructure growth through bootstrapping

Hanseth and Lyytinen [21] have outlined a strategy for a set of design principles and rules to guide the design so that a set of system features is selected to meet chosen design goals. They exemplify the bootstrapping problem, i.e. to come up with solutions early on that persuade users to adopt while the user community is non-existent or small: How can ICT solutions in an information infrastructure get a value? We clearly understand that an II's capabilities must meet early users' needs directly in order to fulfill their mission. The strategy includes these elements: i) design initially for usefulness, ii) draw upon existing installed base, iii) expand installed base by persuasive tactics. IIs are often bootstrapped by experimenting and thereby enrolling new user communities [21])

One very illustrating example is when Tim Berners-Lee designed the first WWW services. They were initially intended to meet information-sharing needs among high energy physicists, however expanded quickly to a growing, worldwide community [22]. Thus, we believe that a similar bootstrapping approach is useful to foster the growth of BCT-based applications. Although this technology is not yet mature, it has demonstrated significant developments from being used by a handful of persons to today's millions of users and links [34], We see a significant investment rate, indicating lots of start-ups, and expansion in terms of diversity of components and services added to the technology [25], as e.g. different wallets, and platforms as e.g. Ethereum and lots of other altcoins [35], [36]. In particular, we believe that successful applications in the public sector can stimulate such developments, as many governments have high trust and a large user base, see below in next chapter.

4 EXAMPLES OF BLOCKCHAIN IN GOVERNMENT

The BCT may be used for many types of transactions where the government is involved. Its security mechanisms enable implementation in a wide range of processes for asset registry, inventory, and information exchange, for both hard assets like physical property and intangible assets like votes, patents, ideas, reputation, intention, health data and other information [37]. This has led to the belief that BCT is going to replace the current database technology. This would be a big mistake, Greenspan and others warns [38].The essence of a BC is that organizations can keep track of a common 'ledger' and that organizations jointly create, evolve and keep track of one immutable history of transactions and determine successive events. However, these features also come with some technical challenges, with regard to both privacy and capacity.

The Norwegian Tax Administration carried out a small blockchain project in 2016 to better understand the technology and to investigate its potential. The project can be characterized as a proof of concept (PoC), and a private blockchain was used for the purpose.

The goal of the project was to use blockchain technology to secure documents and make them immutable. Up to now the Tax Administration does not have a system that can guarantee (to some extent) the originality of documents and prove their immutability.

The system worked as expected. However, one of their conclusions was that the immutability of the documents could be a problem with regard to privacy and the right to be forgotten. Transactions on a blockchain, at least an open, public blockchain, cannot be deleted and this could pose a problem for the enhanced privacy proposed in the forthcoming General Data Protection Regulation (GDPR) [34]. The Tax Administration has not concluded on a blockchain strategy, but continues to explore the technology both on its own and together with other public agencies.

Also the Norwegian Labour and Welfare Administration (NAV) has conducted trials with blockchain technology. Like the Tax Administration's, their trial was also a PoC to become better acquainted with the technology. They tried the technology (private blockchain technology) on a case regarding social security recipients' reporting a move to a new address. The blockchain technology was used to control transactions in the current system's processes.

Their conclusion was that blockchain technology is suitable for the need of a replicated, fault tolerant, verified and immutable transaction log involving parties with limited trust to each other. However, they also concluded, at least for the time being, that if your need is to share an immutable stream of events where you control the access, there are simpler systems that can meet the demand. They acknowledge BC's potential for the future, but they think that it is too early to proceed with the technology now.

This conclusion is also the dominant view of the respondents in a survey conducted recently among public sector bodies in Norway [5]. The main goal of the survey was to find out how key persons in public sector agencies viewed four emerging technologies: Robotics, Blockchains, Artificial Intelligence, and Virtual and Augmented Reality. The respondents viewed BCT as immature and not ready for use in the public sector.

A very relevant example is the use of BCT for land title (deed of conveyance) projects. This BC application is particularly useful when ownership records are not preserved systematically 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 would be registered. BCT can prevent manipulation and loss of data. The transfer of land property requires that the lawful owner must sign, for which there should be proof of ownership, no remaining mortgage be registered on the land property, and a payment (money transfer) from the buying to the selling party must be made. BCT 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.

Estonia is considered one of the leading countries of the world when it comes to digitization in public sector, thanks not least to its innovative fundament of the X-Road system [39]. On top of the X-Road system the Estonian government has built transparent services that lets the citizens not only easily access their own data, but also see who else has accessed their data and when. This technology was built by the company GuardTime and was based on core hash functions also key elements in blockchain technology [40].

Estonia wants to go further and embrace the blockchain technology in full. One of the first application areas will be in their e-Residency program (op. cit.). The e-Residency program is a way for Estonia both to increase their limited population of 1,3 mill. inhabitants without open up for mass immigration, but also a way of exporting their core e-Government technology. Kaspar Korjus, the managing director of the e-Residency program, says that governments can help unleash the full potential of blockchain technology by providing a smart policy framework and by providing verified online identities, and that is what Estonia plans to do (op. cit.).

Finally, we describe two use cases dealing with secure storage of academic certificates. Both the University of Nicosia (UNIC) and MIT have developed solutions for this. Here we will describe MIT's solution *BlockCert* [41]. The MIT Media Lab's primary motivation was to empower students to be the curators of their own credentials. The system is based on the Open Badge standard for representing credentials from higher education and works this way: 1) The university publishes the student's credentials on the Bitcoin blockchain signed with their own digital certificate, 2) Those responsible for validating the student's credentials, e.g. a potential employer, downloads the BlockCert Wallet, 3) The app computes a SHA256 digest of the certificate, 4) The hash stored on the Bitcoin blockchain is fetched, 5) The two hashes are compared, 6) The university's signature is checked, 7) The app checks that the certificate has not been revoked by the issuer [42]. Although both universities are private the topic is just as relevant for public universities and the solutions are offered to both types. The cases are also interesting for other types of credentials and licenses and can thus be seen as general cases for secure document handling.

Table 2: Summary of use case results with regard to information infrastructure properties

	Tax	Welfare	Land titl.	Certific.
Open	No	No	Read	Read, Write, Commit
Shared	No	No	Partly	Yes
Installed base	-	-	Handled by Gateways	No particular
Evolving	N/A	N/A	N/A	N/A
Control	Central	Central	Partly open (distr.)	Open and partly std. (Open Badge)

5 ANALYSIS AND DISCUSSION

Below, we will discuss different types of challenges that are related to potential benefits when adopting BCT applications. From the descriptions, it becomes clear that some benefits are attributed to other technologies (like encryption, identity management) and some benefits require significant social changes and transformations. Trust is not created by technology, it is the user that must believe it is safe. However, so far, at least the Bitcoin blockchain has proven to be secure as it has resisted all attacks.

Whether the benefits will be achieved depends on both the applications themselves and the encompassing social system and its governance. Realizing the benefits of BC requires understanding the government processes along with the legal framework and political setting etc. imposed on government. Current institutional structures might need to be altered to enable distributed transaction management with a governance structure to guide it, as e.g. illustrated in the Swedish land title case [19].

In addition, the adapted structure needs to take the societal requirements into account to ensure that public values like equal access, transparency, accountability and privacy are being upheld. Most of the benefits might also be accomplished using other technology means. This raises the question of 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 is thus subject to change.

We have developed an analytical framework presented in Table 3. It draws from a literature review by Ølnes et al. [43] that have summarized possible benefits and promises of BCT. Below, we have included these categories in column 1, categorized as governance and control, economy and information quality and operational aspects.

The challenges and driving forces are listed in Column 2-4. The specific assessments of the different factors are derived from analyzing the use cases presented above. However, our estimates aim mainly at serving as illustrations of how the framework can be used. They do not present a complete evaluation or judgement.

The second column addresses the potential legal barriers as well as the possible legal support for using BCT application. At the (political) governance level, the use of BCT can contribute to secure fundamental values such as openness, democracy and privacy, and through better transparency hamper corruption. However, regarding the more detailed (operational) security requirements, it must be verified that the level of security that BCT offers complies with specific national and international legislation. for example, the EU General Data Protection Regulation (GDPR), to be implemented this year, implies new requirements, for example to be able to update information and "the right to be forgotten", which seems to be in conflict with the immutability principle of BCs. However, we believe that such functionality can be implemented on a higher technical level, e.g. through making such information inaccessible. The Bitcoin blockchain does offer a platform for secure and transparent payment and other financial operations in hostile environments that do not have adequate technical or institutional infrastructure. However, in most countries, such applications will require changes in laws and regulation. Furthermore, the security measures must comply with requirements in existing legislation.

Column three discusses the extent to which institutional structures (e.g. responsibilities, authority etc.) and organizational patterns (e.g. division of labor, work procedures etc.) represent barriers or challenges. It is most likely that the decentralized and even distributed control structure will challenge the prevailing hierarchical governance structure in government, as we see in the Swedish case. On the other hand, BC's network oriented structure may help and even stimulate forces aiming at breaking down the current government data silos.

The fourth column addresses technical factors, among other information infrastructure characteristics. We see that public blockchains offering access for anyone fulfill the requirement of being an open platform and even potentially an II. Furthermore, public permissionless BC's allowing (in principle) anyone to write and even to contribute in further development correspond to the share characteristics of an II, as shown in Figure 1. Furthermore, Figure II depicting the layered structure of BCT also illustrates the dynamic and evolving capacity of BCT.

Table 3: Framework for estimating potential benefits and challenges when implementing BCT in government

	Challenges/driving forces		
Potential Benefits	**Legal factors**	**Institutional and Organizational factors**	**Technical factors**
Governance and control - Transparency - Reduce corruption - Democracy & participation	Use of BCT is not explicitly regulated by law in most countries. However, openness, transparency and privacy are supported by legislation.	The use of public permissionless BCT must be supported by overall policy. The *distributed control* structure of BCT may challenge the existing regime of authority and control in many governments.	The *open and shared* characteristics corresponds to the *public permissioned* and *permissionless* BCs (cfc h. 2 and Figure 1)
Economic -Reduced cost -increased resilience to spam and DOS attacks	Except the use of BCT as currency, there are few barriers.	Organizational and even institutional changes are necessary to realize benefits, and the full potential can only be realized across organizations.	The *installed base* may act both as a barrier and a facilitator (bootstrapping mechanisms)

Information quality and operational aspects - Data integrity and security - Privacy -Reliability, Resilience -Persistent/immutable	Such characteristics comply with requirement related to privacy regulations, which then will act as a driver. There are challenges regarding updating information and "right to be forgotten".	Data integrity and reliability is dependent on/requires well designed quality assurance procedures, etc., which implies changes on various levels	*Privacy by design* can easily be supported by BCT. The current lack of standards is a driver for innovation; however, it is also a barrier to adoption in the public sector and in society at large.

Addressing economic aspects, our case studies provides evident indications of the potential for cost saving. Outside the use of BCT as a currency/financial instrument, there may be fewer legal barriers. However, such usage will imply substantial changes in organizational procedures and responsibility, even institutional barriers related to authority and governance may be challenges. Again, the distributed control of BCT implies a management problem, at least in a sector-oriented, fragmentary government structure, as cost and benefits are not closely connected. However, similar to the building of the Internet, much of the infrastructure costs must be covered centrally, while the benefits are realized elsewhere in the government organizations and in society at large.

As an illustration of blockchain potential, the UK's Government Office for Science [44] has proposed several use cases for blockchain technology that point to using the technology to (1) protect critical infrastructure, (2) establish novel payment systems for work and pensions, (3) strengthen international aid systems, (4) document authentication and smart contracts, and (5) handle European VAT. Of these suggested application areas, we think authentication of documents (CVs and other certificates, licenses, intellectual properties and patents, wills etc.) is the most interesting in terms of short–term realization.

For many countries, corruption is often a threat to ordinary ways of doing business, not least in Government. Thus, tamper-evident and tamper-resistant ICT systems can provide significant benefits. For example, the Government of Honduras recently started collaborating with the blockchain company Factom aiming to use this technology for storing land title deeds and thereby rendering corruption more difficult [45].

The above examples also show that the blockchain technology is becoming easier to use. The open and global nature of public blockchains means that the technology is available and accessible to all people, and the only requirement is an Internet or mobile network connection. However, usability has not been given high priority thus far, and the crucial management of keys shares many of the same challenges as similar management from other domains [46].

6 CONCLUSIONS

Our case studies have illustrated the important aspect of a shared, open and evolving socio-technical platforms that characterize information infrastructures like the one we believe that BCT has the potential to become. In its ten-year history, BCT, still a novel technology, has demonstrated its dynamic and innovative character. Even though closed BCs can successfully be applied within organizations, BCT's full potential can be realized only in a borderless context, similar to that of the Internet. Accordingly, in order to realize the greatest benefit from the BCT, it is necessary to build inter-organizational applications and possibly expand those globally.

We therefore argue that ICT systems based on the blockchain technology, implying decentralized and distributed management and control, offer robust and flexible solutions that cannot be corrupted. However, lessons learned from earlier efforts to introduce new technology underscore the importance of following a systematic step-by-step approach in order to gain more experience before implementing large scale systems. As a first step, we have provided examples of application areas where the solutions are technically rather uncomplicated, and where there are few organizational or institutional barriers. However, given the promising benefits that blockchain technology holds, it is also important that researchers in the field of e-Government begin discussing important questions: Are governmental agencies ready to investigate the potential of blockchain technology, and what are the main barriers? What are the important factors determining whether to adopt Bitcoin technology in the public sector? And should BCT in the public sector be based on permissionless or permissioned open, public blockchains?

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, vol. 1, no. 2012, p. 8, 2008.

[2] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," *J. Econ. Perspect.*, vol. 29, no. 2, pp. 213–238, 2015.

[3] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[4] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, 2016.

[5] NOKIOS, "Teknologiradar 2017," Trondheim, Conference report, Nov. 2017.

[6] S. Ølnes, "Beyond Bitcoin Enabling Smart Government Using Blockchain Technology," in *International Conference on Electronic Government and the Information Systems Perspective*, 2016, pp. 253–264.

[7] R. K. Yin, *Case Study Research: Design and Methods*. SAGE Publications, 2013.

[8] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, 1983, pp. 199–203.

[9] A. Back, *Hashcash - A Senial of Service Counter-Measure*. 2002.

[10] W. Dai, "B-money," *Consulted*, vol. 1, 1998.

[11] N. Szabo, *Bit gold*. Website/Blog, 2008.

[12] P. van Valkenburgh, "Open Matters - Why Permissionless Blockchains are Essential to the Future of the Internet," Coin Center, Dec. 2016.

[13] A. M. Antonopoulos, *Mastering Bitcoin - Unlocking Digital Cryptocurrencies*, 1st ed. San Francisco, 2014.

[14] A. Sward, V. OP_0, and F. Stonedahl, "Data Insertion in Bitcoin's Blockchain," *Ledger*, vol. 3, no. 1, 2018.

[15] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc., 2017.

[16] G. Hileman and M. Rauchs, "2017 Global Blockchain Benchmarking Study," 2017.

[17] P. De Filippi, “Blockchain-based Crowdfunding: what impact on artistic production and art consumption?,” *Obs. Itaú Cult.*, no. 19, 2015.

[18] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Penguin, 2016.

[19] Lantmäteriet, “‘Framtidens husköp i blockkedjan’ (‘Future real estate trade through the blockchain’),” Lantmäteriet, Jun. 2016.

[20] S. Ølnes and A. Jansen, “Blockchain Technology as a Support Infrastructure in e-Government,” presented at the eGov/ePart 2017, St. Petersburg, 2017, vol. Electronic Government, pp. 215–227.

[21] O. Hanseth and K. Lyytinen, “Design theory for dynamic complexity in information infrastructures: the case of building internet,” *J. Inf. Technol.*, vol. 25, no. 1, pp. 1–19, 2010.

[22] S. L. Star and K. Ruhleder, “Steps toward an ecology of infrastructure: Design and access for large information spaces,” *Inf. Syst. Res.*, vol. 7, no. 1, pp. 111–134, 1996.

[23] P. Weil and M. Broadbent, “Leveraging the new Infrastructure,” *Harv. Bus. Sch. Press Boston*, 1998.

[24] K. Croman *et al.*, “On Scaling Decentralized Blockchains,” in *Proc. 3rd Workshop on Bitcoin and Blockchain Research*, 2016.

[25] M. Pilkington, “Blockchain Technology: Principles and Applications,” *Res. Handb. Digit. Transform. Ed. F Xavier Olleros Majlinda Zhegu Edw. Elgar*, 2016.

[26] Wikipedia, “Internet security,” *Wikipedia, the free encyclopedia.* 29-Mar-2018.

[27] L. A. Bygrave and J. Bing, *Internet governance: Infrastructure and institutions.* Oxford University Press on Demand, 2009.

[28] P. De Filippi and B. Loveluck, “The invisible politics of bitcoin: governance crisis of a decentralized infrastructure,” 2016.

[29] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, vol. 2, no. 9, 1997.

[30] A. Back *et al.*, “Enabling blockchain innovations with pegged sidechains,” *URL Httpwww Opensciencereview Compapers123enablingblockchain-Innov.--Pegged-Sidechains*, 2014.

[31] O. Hanseth and K. Lyytinen, “Theorizing about the design of Information Infrastructures: design kernel theories and principles,” *Sprouts Work. Pap. Inf. Environ. Syst. Organ.*, vol. 4, no. 4, pp. 207–241, 2004.

[32] J. H. Saltzer, D. P. Reed, and D. D. Clark, “End-to-end arguments in system design,” *ACM Trans. Comput. Syst. TOCS*, vol. 2, no. 4, pp. 277–288, 1984.

[33] A. Antonopoulos, *The Internet of Money*. Merkle Bloom LLC, 2016.

[34] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, “Do the rich get richer? An empirical analysis of the Bitcoin transaction network,” *PloS One*, vol. 9, no. 2, p. e86197, 2014.

[35] D. G. WOOD, *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. Ethereum, 2014.

[36] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” Technical Report (draft). https://lightning. network, 2015.

[37] M. Swan, *Blockchain: Blueprint for a new economy*. O’Reilly Media, Inc., 2015.

[38] G. Greenspan, “Do you really need at blockchain for that?,” *Coin Center*, 26-Jul-2017. .

[39] “Governments may be big backers of the blockchain,” *The Economist*, 06-Jan-2017.

[40] K. Korjus, “Welcome to the blockchain nation,” *E-Residency Blog*, 07.072017. .

[41] M. L. MIT Media Lab, “Blockcerts-An Open Infrastructure for Academic Credentials on the Blockchain,” *Medium*, 24-Oct-2016. .

[42] MIT Media Lab, “What we learned from designing an academic certificates system on the blockchain,” *Medium*, 02-Jun-2016. .

[43] S. Ølnes, J. Ubacht, and M. Janssen, *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*. Elsevier, 2017.

[44] UK Government Office for Science, “Distributed Ledger Technology: beyond block chain,” Government Office for Science, London, Jan. 2016.

[45] V. L. Lemieux and V. L. Lemieux, “Trusting records: is Blockchain technology the answer?,” *Rec. Manag. J.*, vol. 26, no. 2, pp. 110–139, 2016.

[46] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, “A first look at the usability of bitcoin key management,” 2015.