OECD Working Papers on Public Governance No. 28

Blockchains Unchained: Blockchain Technology and its Use in the Public Sector

Jamie Berryhill,
Théo Bourgery,
Angela Hanson

https://dx.doi.org/10.1787/3c32c429-en

OECD

OECD working papers on Public Governance

1. This guide was prepared by the Observatory of Public Sector Innovation (OPSI), in collaboration with the Working Party of Senior Digital Government Officials (E-Leaders). OPSI is part of the OECD's Reform of the Public Sector Division (RPS) of the Directorate for Public Governance (GOV). OPSI collects and analyses examples and shared experiences of public sector innovation to provide practical advice to countries on how to make innovation work.

2. This guide has been drafted by Théo Bourgery, formerly of OPSI, and Jamie Berryhill and Angela Hanson, Innovation Policy Analysts, OPSI. It was drafted under the co-ordination of Marco Daglio, Senior Project Manager, OPSI, and the leadership of Edwin Lau, Head of the Reform of the Public Sector Division. Significant contributions were also made by colleagues from the OECD's Digital Government and Open Data Unit.

3. The guide also greatly benefited from the contributions of Justin Herman, Axelle Lemaire, Emmanuel Noah, Noah Raford, Tess Rinearson, Björn Segendorff, Tomicah Tillemann, Mats Snäll and Stanley Yong, who participated in interviews for OPSI's research. From specialists in Blockchains to entrepreneurs and regulators, their interventions were crucial in the development of this guide.

4. Finally, the guide benefited from revisions and comments provided by Matthieu Crepy, Xavier Lavayssière, Enzo Maria Le Fevre, Barry Lowry, Philip McGrath, and Marchionni Pietro.

Abstract

Blockchain technology has evolved from a niche subject to the hottest tech disruption buzzword, but there is still a lot of confusion about the subject. Without a clear understanding about what Blockchains are, their potential public sector potential impact is sometimes misunderstood or, more often, ignored. Questions related to their technical complexity, risk, security, and appropriateness often serve as obstacles to government officials' ability to truly engage with this emerging technology. In light of this, the Observatory of Public Sector Innovation (OPSI) in collaboration with the Working Party of Senior Digital Government Officials (E-Leaders) has developed a guide on Blockchains and how they may (and may not) apply to government. OPSI is part of the OECD Directorate for Public Governance (GOV).

Table of contents

OECD working papers on Public Governance **2**

Abstract **3**

Foreword **6**

1. Executive Summary **7**

2. What are Blockchains? Concepts and context behind the technology **10**

2.1. What is Blockchain technology? 10
2.2. What problems can Blockchains solve? 13
2.3. What is the different between Blockchain technology and Bitcoin? 15
2.4. How do Blockchains work? 15
2.5. How are governments reacting to Blockchain technology? 20
2.6. What are ways governments can use Blockchain technology? 24

3. Challenges, limitations and other consideration of Blockchain technologies in government **29**

3.1. Immutability 29
3.2. Transparency, Confidentiality and Decentralisation 29
3.3. Data Storage 30
3.4. Data Quality 30
3.5. Coding and Governance Models 30
3.6. Talking About Blockchain 31
3.7. Costs 31
3.8. Challenges related to “Proof of Work” Consensus Model 32
3.9. Conclusion 33

4. Appendix A: Case studies of Blockchain applications and communities in the public sector **35**

4.1. Case study 1 35
4.2. Case study 2 36
4.3. Case study 3 37
4.4. Case study 4 39
4.5. Case study 5 40
4.6. Case study 6 41
4.8. Case study 7 43
4.9. Case Study 8 44

5. Appendix B: Digital signatures and public and private keys **46**

5.1. Encrypting a Transaction 46
5.2. Digital Signature Use and Authentication 46

6. Appendix C: Consensus models **47**

6.1. Proof of Work Consensus (PoW) Model 47

6.2. Proof of Stake Consensus Model 48
6.3. Proof of Authority Consensus Model 48
6.4. Round Robin Consensus Model 48

7. References 49

Tables

Table 1. Examples of hashes 16
Table 2. Top 10 types of projects and industries 22

Figures

Figure 1. Distributed networks compared to centralised and decentralised networks 12
Figure 2. Blockchain – a chain of blocks 16
Figure 3. The interdependence of blocks 16
Figure 4. Blockchain in the public sector, as of March 2018 21
Figure 5. ACT-IAC Blockchain Playbook Key Activities 24

Boxes

Box 1. Key Concepts: Distributed Ledger Technology, Nodes, and Cryptography 11
Box 2. Key Concepts: Distributed and Shared 12
Box 3. Key Concept: Immutable 13
Box 4. Key Concept: Pseudonymous 13
Box 5. Key Concept: Cryptocurrency 15
Box 6. Key Concept: Mining Nodes 17

Foreword

5. The OECD Observatory of Public Sector Innovation (OPSI) aims to make sense of innovation trends across governments. OPSI shines a light on the work of agencies and public servants to create more efficient, effective and responsive public policies and services. OPSI accompanies teams and departments in their exploration and implementation of all forms of innovative efforts, ranging from grappling with emerging and disruptive technologies, leveraging big data analytics and open data, strengthening innovation skills and capacities, promoting citizen-driven policies and services, and fostering innovative procurement and human resource management systems, among others. OPSI's purpose is to understand the dynamics of innovation to create and fuel systemic change in the public sector.

6. OPSI publishes the *Embracing Innovation in Government: Global Trends* series of reports[1] to identify the key trends that will shape the public service of tomorrow.

7. These annual reports uncover the current state of research and practice in the field of innovation and draw on an annual global Call for Innovations crowdsourcing exercise. This exercise has surfaced over 400 compelling innovation initiatives that show the breadth of innovation work from across a range of administrations, agencies and issues. The report selects top initiatives to highlight as case studies in the report. Blockchain has been featured in all *Embracing Innovation* reports so far. For example, the 2018 report discussed the public-private partnership ID2020, which demonstrates the potential for Blockchains to help provide digital identities for the 1.1 billion people in the world who live without an officially recognised identity, including millions of refugees.[2] The 2017 trends report examined how Blockchains could transform the voting process in democracies, as illustrated by a Blockchain-based digital plebiscite[3] on whether the government of Colombia should approve a peace treaty in order to end a long-term conflict.[4]

8. OPSI sees growing curiosity and a need to understand Blockchain technology better in the public sector. In collaboration with the Working Party of Senior Digital Government Officials (E-Leaders), and leveraging our work on uncovering global trends, OPSI has developed this *Blockchains Unchained* guide. The first in what is intended to be a series of straight-forward and easily accessible overviews of topics of interest for the public sector innovation community.

[1] See http://oe.cd/innovation2018 for the February 2018 report, and http://oe.cd/eig for the February 2017 report.

[2] See http://id2020.org.

[3] A plebiscite is a vote to express an opinion on a choice to be made by government.

[4] See http://plebiscitodigital.co.

1. Executive Summary

9. This guide aims to equip public servants with the necessary knowledge to understand what the Blockchain architecture is, the implications it could have on government services, and the opportunities and challenges governments may face as a result. This paper also aims to provide information on what Blockchain technology is not, and areas where its application may not be useful. It is often the case that hype around the impact of emerging and disruptive technologies overstates their practical and pragmatic applications. An understanding of what Blockchain technology is and is not is critical in helping policy makers and civil servants look past the hype and determine whether Blockchain technology is something that may help them advance their missions.

10. Blockchains have become a buzz word, yet ambiguity remains around what they truly are. Their impact on the public sector is at best misunderstood, and most often ignored. The technical complexity of Blockchain technology skews public debate, as the topic can be difficult to discuss and explore for potential application in government. In addition, despite having a wide range of potential uses in many areas of government, Blockchain technology is often incorrectly seen as synonymous with Bitcoin and the "dark web" markets that use Bitcoin as the primary payment method for illicit goods. Blockchain introduces the possibility to manage information and trust in completely new ways that need to be understood in order for the public sector to seize the new opportunities that they present.

11. Current transactional processes predominantly involve institutions such as governments or banks that act as trusted, central third-parties to certify transactions, which potentially position them as single points of failure in the event of a disaster, attack, or other sort of disruption, which raises questions about the continuity of the services they provide and records they keep. Blockchains may help address some of government's existing challenges in this space. Blockchain technology may also help governments reduce fraud, errors, and the cost of paper-intensive processes (ACT-IAC, 2017), and by design can provide perfect transparency over government data and transactions.

12. Section I defines Blockchain technology as a digital distributed ledger system that acts as an open, shared and trusted record of transactions among parties that is not stored by a central authority, which has and continues to be the traditional approach. Instead, all users running Blockchain software—also known as nodes—have a copy. This way, everyone can inspect it (OECD, 2016). Blockchain technology's underpinning assumption is that all transactions will be visible to all nodes in the system at all times. To achieve this, in general, all nodes hold identical 'ledgers' of transactions that are rapidly updated any time a new set of transactions is added. This enables a key feature of the Blockchain architecture: consensus models where nodes in the system confirm the validity of transactions that occur on the platform, and flag inappropriate dealings when necessary.

13. The next stage involves ensuring transaction are tamper-proof. One must imagine a Blockchain as, quite literally, a chain of blocks in which specific transactions are stored. Once transactions are validated by nodes, they are stored in blocks which cryptography and complex mathematical constructions secure. Each individual block is published to the Blockchain in a way that it is linked to the previous block, and will also be connected to the next block once it is added to the chain. Due to its linear, chain-like architecture, blocks are fundamentally dependent on one another, such that changing the information of one ultimately alters the link it has with all other blocks on the chain in a way that can be immediately recognised by the other nodes as have being altered. The chained structure, coupled with consensus rules that require that a majority of nodes agree on the validity of the ledger, ensure that the information contained in the ledger cannot be tampered with. Thus, transactions can be inherently trusted.

14. Interestingly, Blockchain technology suggests that banks and governments could no longer be required as trusted third-parties, at least not in the same capacity as they are today. This is the real disruptive nature and potential value of Blockchains: the development and growth of automated and decentralised decision-making systems that do not require centralised authorities yet still ensure validity and transparency.

15. Section I also discusses the various ways governments have begun to react and adapt to the emergence of Blockchain technology. This includes discussing the landscape of current Blockchain initiatives, as well of the various types of use cases that may the most relevant in the public sector.

16. Section II focuses on the challenges that Blockchain technology poses to public administrations, as well as its limitations which may make render the technology unsuitable for certain uses. These take many shapes and forms, be it matters of data protection, governance, or confidentiality of information. Coding constraints and governance decisions also add to the complexity. In addition, the key aspect of Blockchain technologies—immutability—makes the technology less useful than other proven technologies for many uses. Finally, In addition, the format that some Blockchains take today have inherent limitations, such outrageously high levels of energy required to power the certain Blockchain systems, as well as the slow pace of transactions processes in some systems. However, many limitations are simply used a blockers for further exploration of Blockchain and are not in fact relevant to public sector applications at all. These challenges, limitations, and consideration must be understood by leaders and public servants as Blockchains continue to expand out of the private sphere into the public sector.

17. Finally, a series of appendices provide case studies as well as some more technical discussions of specific aspects of Blockchain technology. Appendix A, in particular, provides the reader with a number of different case studies of Blockchain uses and communities in the public sector – from across the world, and across a variety of departments and agencies. While Blockchain technologies have mostly been used in the financial sector, predominantly for monetary transactions, this powerful technology is also being used for non-monetary matters. Digital identification, proof of land ownership, supply chain management, and even voting, are only a fraction of the disruptive impacts Blockchains could have on the public sector.

18. The purpose of this guide is to help leaders, public servants, practitioners and decision-makers to understand the technology and its associated opportunities and challenges. This will help them make better decisions and more easily assess the use of

Blockchains across different contexts. Although seemingly complex, policy-makers must grasp the technology and its implications, as this trend is already deeply transformative.

2. What are Blockchains? Concepts and context behind the technology

19. Blockchain technology, for many, is considered to be as revolutionary as the rise of the Internet (Rosic, 2016), and has been referred to as a new "trust machine" because of its ability to allow people to interact and conduct transactions even though they may not know each other or have a pre-existing trust-based relationship (Economist, 2015). Although the technology is amassing a body of literature, few sources make sense of the technology in accessible ways,[5] and fewer yet focus on its applicability to the public sector,[6] such as ways it can enable collaboration within and across governments and help reduce fraud, errors, and the cost of paper-intensive processes (ACT-IAC, 2017).

20. Given this state, this guide aims to provide an introduction to the technology and outline some potential areas for consideration for the public sector. The paper:

- Explains what Blockchain technology is and is not;
- Makes the case for public servants to build knowledge of, and capability in, relation to Blockchain technology;
- Make sense of its impacts on the public sector, and anticipate future developments; and
- Explore and discuss existing public sector usage of Blockchains.

21. Importantly, this paper does not contain every definition or concept necessary to fully understand all of the nuances and details of Blockchain technology. It does, however, aim to contain a sufficient level of detail for public sector officials to determine whether Blockchains are something that they may want to pursue further for their own missions.

2.1. What is Blockchain technology?

22. As described by the World Economic Forum, "currently, most people use a trusted middleman such as a bank to make a transaction. But Blockchain networks allow consumers and suppliers to connect directly, removing the need for a third party" (Hutt, 2016).

23. Blockchain technology is a form of distributed ledger technology that acts as an open and trusted record (i.e., a list) of transactions from one party to another (or multiple parties) that is not stored by a central authority. Instead, a copy is stored by each user running Blockchain software and connected to a Blockchain network—also known as a *node* (see Box 1 for descriptions of some of these key concepts). Instead of a central authority maintaining a database, all nodes have a copy of the ledger and updates to a Blockchain ledger are propagated throughout the network in minutes or seconds (ACT-

[5] See for example Rinearson, 2017a and 2017b, and Mamoria, 2017.

[6] See for example Cheng et al, 2017 and Ølnes, 2015.

IAC, 2017). In these networks, a majority of nodes must review and validate a transaction before it can be verified and recorded. This way, nobody can tamper with the ledger, everyone can inspect it, and it can be trusted (OECD, 2016). For individual transactions, Blockchains use cryptography to keep transactions secure (see Box 1). It is important to note that, although this report often refers to nodes taking actions (e.g., validating transactions, sharing blocks, etc.), the vast majority of these steps are done automatically by Blockchain software and require no manual intervention.

Box 1. Key Concepts: Distributed Ledger Technology, Nodes, and Cryptography

Distributed Ledger Technology

A technology upon which records of transactions are "spread across multiples sites, countries or institutions, and is typically public. [Transaction] records are stored one after the other in a continuous ledger, but they can only be added when participants [confirm the feasibility and validity of the transaction]".

Source: Walport, 2016; Rinearson, 2017

Nodes

A node is simply a user or computer on a Blockchain platform that is running Blockchain software. The general job of "full nodes" is to store a full copy of a Blockchain ledger, receive data from other nodes, validate the data, and pass it to other nodes on the network so long as it is valid. "Mining nodes" perform these tasks, but also publish new blocks to a Blockchain through the mining process, as discusses later in this document. Finally, "lightweight nodes"—generally found on devices with limit processing power such as smartphones and Internet of Things (IoT) devices—are nodes that are do not maintain full copies of a Blockchain ledger and tend to send their data to full nodes for processing and validation.

Source: Yaga et al, 2018

Cryptography

Cryptography is the act of creating codes that allow data to be kept secret. Cryptography converts this data into a format that can only be read/decoded by authorised users. Thus, the data can be transmitted without fear of it being decrypted and compromised by unauthorised actors. Authorised actors may decrypt the data using a "key", which is essentially a corresponding private code that only an authorised user should know (see Appendix B for details on keys).

Source: www.techopedia.com/definition/1770/cryptography

24. One of the key inherent characteristic of Blockchain is its *distributed* and *shared* nature (see Box 2). Because of this, "Blockchain–based systems have the potential to reduce or eliminate the friction and costs of current intermediaries", and thus allow for "improved data integrity, decentralisation and disintermediation of trust, and reduced transaction costs" (Krawiec et al, 2016). Traditional databases and information systems are different in that data is stored on a centralised server that is generally owned and

maintained by a central authority (Ray, 2017). See Figure 1 for a comparison of distributed networks compared to alternatives.

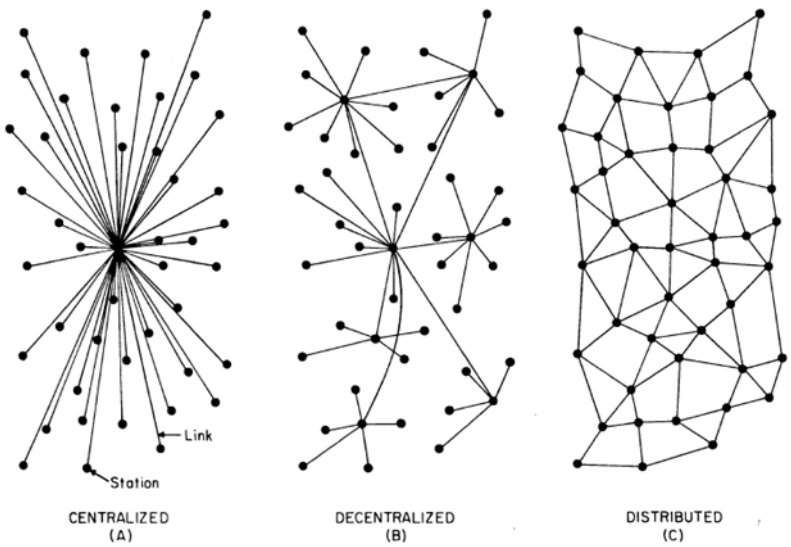
Box 2. Key Concepts: Distributed and Shared

Distributed: All copies of one document are constantly and automatically synchronised hence identical at all times. Furthermore, "there is no canonical copy; all copies are created equal"

Shared: There is perfect information across all actors in the system. All platform members have access to all members' information.

Source: Rinearson, 2017

Figure 1. Distributed networks compared to centralised and decentralised networks



Source: Baran, 1964

25. Another key inherent characteristic of Blockchain technology is the immutability of Blockchain transactions (see Box 3). In general, once a transaction is added to a Blockchain ledger, it cannot be undone. This immutability is one of the principle aspects that contribute to the trustworthiness of Blockchain transactions. With a traditional, centralised database when a user adds or modifies data, they connect with the server to make their changes, and the data remains on the server. Because all of the data is held in one place, if the security of the server or the authority that runs the server is compromised, data can be modified or deleted (Ray, 2017). Sometimes, this may occur without anyone realising that this has occurred.

Box 3. Key Concept: Immutable

Immutable means that something is unchanging over time or unable to be changed.

In the context of Blockchains, it means once data has been written to a Blockchain, no one, not even a system administrator, can change it. Immutability allows senders, receivers, and any interested party to be able to verify that data have not been altered.

Source: https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains

26. As a result of these key concepts, Blockchains by nature ensure perfect transparency over all users and all validated transactions that have occurred. Consequentially, all users in the system have information about all parties' willingness and ability to carry out transactions (e.g., make a payment), and a record of what has already occurred.

27. Because of these benefits, Blockchains have the potential to impact a large variety of topics and "create genuine opportunities for the government and other local and regional authorities" in reducing operation costs, increasing transparency and trust between governments and citizens, facilitating financial inclusion and boosting operational and financial capacities of small and medium-sized enterprises (Krawiec et al, 2016).

28. Contrary to popular belief, in general, Blockchain technology allows its users to be pseudonymous, but does not allow for total anonymity (see Box 4). However, this can differ on "permissioned" ledgers where access to view and add to Blockchains can be restricted with more customised rules and user permissions, such as rules that require users to have their identities validated (see following section on "Different types of Blockchain ledgers: Permissioned and Permissionless").

Box 4. Key Concept: Pseudonymous

On many Blockchain platforms, user identities can be anonymous but their accounts are not, as all of their transactions are visible to all other users. On these platforms, user accounts can be created without any identification or authorisation process. This allows users to use a pseudonym – a fictitious name. However, some permissioned Blockchains may require and a user's identity be verified before they are able to access or interact on the Blockchain.

Source: (Yaga et al, 2018)

2.2. What problems can Blockchains solve?

29. To understand the potential benefits of Blockchains, current issues in data management and transaction security must first be understood. This section outlines these two existing issues. To aid explanation, it relies on two analogies:

- The integrity of shared documents and information (the e-mail analogy);
- The limitations of the 'trusted third-party' logic (the bank analogy).

2.2.1. The e-mail analogy

30. The status quo: It is a common process to share documents among peers and colleagues through the use of e-mails. This results in the duplication of the document. There are automatically two copies: the sender's, which is saved on one's personal device or drive, and the e-mail recipient's. This process can be reiterated an infinite number of times – thus the duplication of one document is theoretically never-ending.

31. The issue: Such a process cannot exclude the possibility that one of these copies, and one of these copies only, be amended and tampered with independently of all others. As amended copies duplicate exponentially, the history of changes becomes ambiguous: which document becomes the correct one? Which one can be relied upon to 'state the truth'?

2.2.2. The bank analogy

32. The status quo: Digital financial transactions and transfers have become a common and fully accepted aspect of peoples' economic lives. In such contexts, we expect a bank to act as a trusted third-party to verify and confirm that:

- The identity of the sender is valid and it is indeed them, and not someone else, who has requested the transfer;
- The sender has the necessary funds to make the transfer;
- The recipient is indeed the one aimed for, and not someone else.

33. In other words, we expect the bank to confirm the validity of the transaction; and that only banks can conduct such confirmations. In this content, the bank acts as the only trusted third party.

34. The issue: This single ledger held by the bank and the bank can ultimately create a single point of failure, whereby hackers may gear cyberattacks to this specific entity – which, if not protected enough, can enable access to sensitive information (Webb, 2016). The outcome is a rather grave one: the trust placed upon the third party no longer holds and transactions are no longer believed to be secured. In addition, digitally enabled economies require ledgers that can be quickly accessed by multiple people from multiple places. Digital information [today] can be erased, updated or altered without leaving any discernible trace of such activity" (Hanson, 2017).

35. Thus, Blockchain ledgers would need to meet two key conditions in order to address these issues and eliminate dependency upon a centralised authority, if desired:

- Immutable: data management and history must become completely unchanging, and;
- Distributed: Trust must be instilled between two parties without the necessity to go through a centralised authority – thus eliminating the risk of a single point of failure.

36. In other words, one must create an eco-system in which the history of transactions and information will be immutable, and thus complete. It follows that transactions must be entirely secure at all times and places on the platform. Finally the architecture must enable complete trust between users with whom no prior transacting relationship, such as by making transactions transparent to all users.

2.3. What is the different between Blockchain technology and Bitcoin?

37. Blockchains are technologies with specific and unique attributes. Such technologies are then applied to specific platforms. Hundreds of these platforms have been introduced since the creation of Blockchains.

38. The first and most well-known of these platforms is Bitcoin, with a cryptocurrency of the same name (see Box 5). Bitcoin has attained record-breaking values, reaching a peak value of nearly USD 20 000 per bitcoin and a total value over USD 326 billion in December 2017, (Rosenfeld and Cheng, 2017) and fluctuating dramatically thereafter. On any single day for the past two years, an average of over 259,000 transactions has taken place on the Bitcoin platform.[7]

Box 5. Key Concept: Cryptocurrency

A cryptocurrency is a virtual coinage system that functions much like a standard currency, enabling users to provide virtual payments for goods and services free of a central trusted authority. Cryptocurrencies rely on the transmission of digital information, utilising cryptographic methods to ensure legitimate, unique transactions"

Source: Farell, 2015

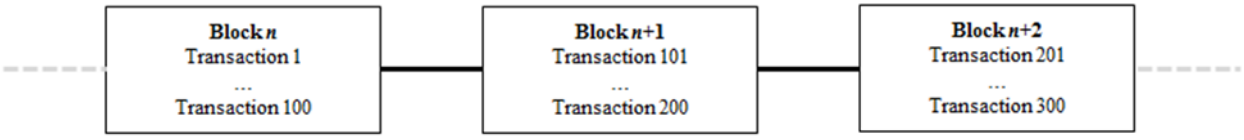
39. A discussed more later in this guide, a significant challenge to understanding and implementation of Blockchain technology in the public sector is that it is too often linked to the turbulence of the Bitcoin platform, and the "dark web" markets that use Bitcoin as the primary payment system for illicit goods (Economist, 2015). Blockchain technology, however, is much more than cryptocurrencies its usefulness as a political and administrative tool needs to be better understood.

2.4. How do Blockchains work?

40. Blockchain technology, as the name suggests, is merely a chain of "blocks", each containing a unique set of transactions that each contain a cryptographic fingerprint called a "hash" (see Table 1). Each block is a set of validated transactions that are grouped together in such a way that the information remains accessible but cannot be tampered with. Blocks are not independent of one another. Rather, all blocks are intrinsically related insofar as they are linked in linear, sequential order by their own unique hashes that act as fingerprints—hence the concept of a chain.

[7] For an up to date read, see BlockchainInfo's live track: https://blockchain.info/charts/n-transactions (last accessed 19 February 2018).

Figure 2. Blockchain – a chain of blocks



2.4.1. Hashing

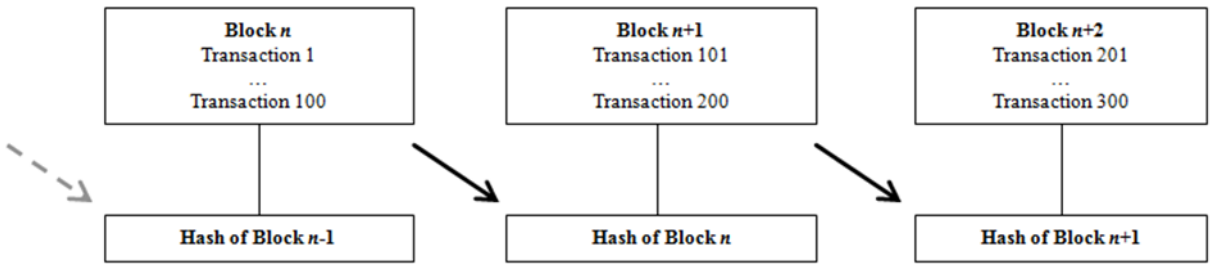
41. Hashing is a cryptographic function that generates a unique fixed-length hash code for any given input, such as text, an image, a video. The specific input, if unchanged, will always produce the same exact hash code. If, however, absolutely any part of the input (e.g., one letter was changed from lower-case to a capital letter), the hash code would change to an entirely different and unique hash code.[8]

Table 1. Examples of hashes

Input	Hash
OPSI	6057121102B54E7210E021645C5305F4DD3F154ECAF8CE6DA69AED5FE4317428
OPSi	E23F99DF38E5A29119853DBACB40ED647CF7F9D6FA3850A76EF170AC11E46732
Organisation for Economic Co-operation and Development	335662EA7181CA392C518A7225ABD31BB36B9DF7D075EC465D3BA8BF8B17F96C

42. For blocks, the transactions in a block are hashed to create a unique hash code for the block. These hash codes are used to interconnect blocks together. Blocks are added one after the other in linear, chronological order, with each containing its own hash code *and the code of the previous block*. This links the blocks together to form a chain (see Figure 3).

Figure 3. The interdependence of blocks



Source: David, forthcoming.

43. If anyone tried to alter the contents of one of the blocks in any way, it would change the hash code for the contents and for the block. This would easily discoverable to the entire network because it would be obvious that the digital fingerprints have been

[8] Sample hashes can be made easily online, such as at https://passwordsgenerator.net/sha256-hash-generator.

changed and any associated transactions would be rejected by the nodes, which are responsible for validating transactions and blocks.

44. These three principles, when combined, are the key factors that allow Blockchain transactions to be immutable:

1. Blocks are chained together using these unique hash codes.
2. The slightest change to an input would result in a change to the transaction's hash code, which would cascade into changes to the block's hash code and the hash codes of subsequent blocks.
3. Through the consensus process of the nodes, the nodes would quickly realise that block was tampered with and would reject it.

2.4.2. Reaching consensus to publish new blocks to a Blockchain (e.g., mining)

45. Blocks are not added to the chain automatically. New blocks are published to a Blockchain through a process called "mining", which is carried out by "mining nodes" (see Box 6).[9] After one node initiates a transaction, it is reviewed and validated by other nodes. Afterwards, the transaction waits in a queue with other pending transactions until a mining node validates a group of pending transactions and adds them to a block. The mining node then publishes the validated block to the Blockchain (Yaga et al, 2018). Upon publishing the block, the mining node begins to broadcasts the block to the rest of the network. Mining nodes do not accept any invalid transactions, and thus do not add them to a block or subsequently publish them to the Blockchain or broadcast them to the network. Although it sounds complex, the process is generally automated by Blockchain software. The frequency of the mining process and different parameters associated with it (e.g., how many transactions are in a block and how long they wait in a queue) vary depending on how the relevant Blockchain platform is designed.

Box 6. Key Concept: Mining Nodes

Mining nodes are a subset of all nodes—generally nodes or pools of nodes with powerful computers—that are responsible for publishing new blocks to a Blockchain. Mining nodes validate that the transactions were appropriately cryptographically signed (through the use of a private key) by the sender and adding validated transactions to the Blockchain by publishing them in blocks. In some Blockchain platforms like Bitcoin, these mining nodes are compensated financially for doing extra work needed in order to validate and publish new blocks (see Proof of Work section in Appendix C).

Source: (Yaga et al, 2018)

46. A critical step before this is that a mining node must gain permission to publish a block to the Blockchain. The "consensus model"[10] that a Blockchain platform is programmed to use sets forth the rules by which a mining node obtains this permission.

[9] The term "mining" is most accurately used for Blockchain implementations that use the Proof of Work consensus model (see Appendix C). The name of the process for publishing new blocks varies depending on the consensus model. For the purpose of simplicity, this guide refers to the process of publishing new blocks as "mining", regardless of the consensus model used.

[10] See Appendix C for more information on consensus models.

For several platforms, such as the Bitcoin platform, which uses the Proof of Work consensus model, this is a competitive process where nodes compete to earn the right to publish a new block to the Blockchain. For other consensus models, such as the "Proof of Authority" model, the process is not competitive. Rather, user permissions are used to determine who may publish new blocks to a Blockchain. In this regard, Proof of Authority is not all that different from typical government databases and information systems today, where known users are given special permissions to access and add new information to a ledger based on their role and access rights. Consensus models can be quite complicated, and some models are more applicable to the public sector than others. More information on consensus models can be found in Appendix C.

47. When a mining node publishes a new block to a Blockchain, the block is shared throughout the network; the individual copy of the Blockchain that is held by all nodes is updated. The other nodes on the network are responsible for also validating the new block, including ensuring that is contains the hash code of the previous block and that all of its transactions are valid, among other things (Yaga et al, 2018). If the block is valid, the node passes block on to other nodes, which locks in the transaction so long as the majority of nodes confirm that it is valid.

48. The only way in which an invalid transaction or block could be propagated throughout the network would be if a majority of nodes actively collaborated to do so—known as the "51% attack". Due to the highly distributed model on which Blockchains are built, and the pseudoanonymity of users across the globe for most platforms, it becomes particularly difficult for a contradictory consensus to be reached. For Blockchain applications likely to be used in the public sector, such as those based on the Proof of Authority consensus model, access restrictions based on user permissions settings also help to prevent this.

49. Since the information is identical on all ledgers, it must follow that the decision, in general, is approved through the consensus of the majority of the nodes. This is what is understood by a distributed decision-making process – whereby consensus rules over the feasibility of the transaction, as opposed to banks and other central authorities. The trust effectively shifts from the centralised authority to the users of the system. Levels of checks and balances, along with functions to protect both transactions and the confidentiality of nodes, are so advanced that they are inherently trustworthy.

2.4.3. Different types of Blockchain ledgers: Permissioned and Permissionless

50. Blockchain ledgers can be public or private. In a public network (such as Bitcoin), anyone can have access and propose transactions, whereas in a private network only specific authorised users can participate. This draws an important distinction between *permissionless* (or "public") and *permissioned* (or "private") ledgers.

51. Permissionless ledgers, such as Bitcoin, "allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies" (UK Government, 2015). Permissionless ledgers most often use either the Proof of Work or Proof of Stake consensus model (see Appendix C), which is what enables mutually distrusting users (i.e., users who do not know each other or otherwise do not have an existing trust-based relationship) to conduct transactions among themselves.

52. Permissioned ledgers, on the other hand, limit contributions to a restricted set of users who have been given rights. Access to view transactions on permissioned ledgers may also be restricted, or could be public, depending on the ledger's settings.

Permissioned ledgers may be the most applicable types of ledgers for the public sector, and would be better suited to use consensus models such as Proof of Authority or Round Robin models (see Appendix C), depending on the purpose of the ledger and its users. Permissioned ledgers can greatly enhance accountability, as transactions can be transparent to everyone, while only authorised users are able to actually record new transactions. The rules for how permissioned ledgers function can be decided on and programmed up front. In the public sector, that can, for example, take into account government rules and laws (Marchionni, 2018), and can also set various levers of user permissions for individuals and nodes using the ledger.

53. The exact same logic that differentiates permissionless and permissioned ledgers applies to differentiate the Internet from any company or agency's Intranet. The Internet is accessible to all, and all can participate in their own ways to its construction – building space and/or content. The intranet however, is much more constrained in its access and the uses that can be made of it. In other words, users are granted access to the intranet, while access to the Internet follows a by-default rule. The intranet is an excellent representation of a permissioned ledger – a place where access is controlled in light of required attributes; users within that space are trusted by essence; and the space's integrity is ensured only by approved users.

2.4.4. Smart Contracts

54. Some Blockchain platforms allows for Smart Contracts, which are small computer programs that use a Blockchain for execution. Smart contracts can take transactions protocols to a new level by enabling the creation of self-executing contracts (or workflows) with the terms of the agreement between the parties being directly written into lines of software code (ACT-IAC, 2017). Smart contracts are automated "if/then" software programs that self-execute when a specific trigger occurs (Marchionni, 2018). Like other Blockchain transactions, smart contracts are maintained and run across all nodes in a Blockchain (ACT-IAC, 2017).

55. Smart contracts intend to provide a digital workflow process, whereby a series of necessary and binding steps must be taken before the outcome is reached, or the contract ends. They are "executed exactly as programmed without any possibility of downtime, censorship, fraud or third party interference" (Marchionni, 2018). The most developed platform today for smart contracts is Ethereum – one on which smart contracts for inter-bank payments and e-identification mechanisms are currently being tested.

56. In the context of the public sector, we can imagine smart contracts providing the ability to provide certainty and transparency in transactional processes. An example of a small process could be reimbursements for employee travel. A potential example of a more significant process could be to determine and govern times at which social aid would be granted, and conditions under which it must continue or stop. The logical steps that today apply to our relationship with government could be automated. In some instances, the potential exists for intervention in service provisioning to be eliminated completely or significantly reduced. For a given service, each government entity—potentially in collaboration with other involved entities—can develop smart contracts that are programmed with workflows and necessary requirements to handle the various types of inputs (Marchionni, 2008).

2.5. How are governments reacting to Blockchain technology?

57. Although Blockchain technology developments have been most extensive in the financial services industry,[11] the discussion and application of Blockchains is also rapidly emerging in the public sector. Governments are taking action to learn more about Blockchain technology and to introduce Blockchain concepts—and the associated opportunities and challenges—with policy-makers and civil servants. Indications that governments are realising the transformative and potentially disruptive nature of this emerging technology include the organisation of a roundtable on Blockchains and cryptocurrencies at the EU parliament for Members of the European Parliament (MEPs) in April 2016 (Patrick, 2016); the ongoing exploration of Blockchains by the Senate and National Assembly of France; and the recognition of distributed ledger technology as a means for legal financial bonds transfers by the French Ministry of the Economy for specific private equity transactions (Ordonnance n. 2016-520, 2016).

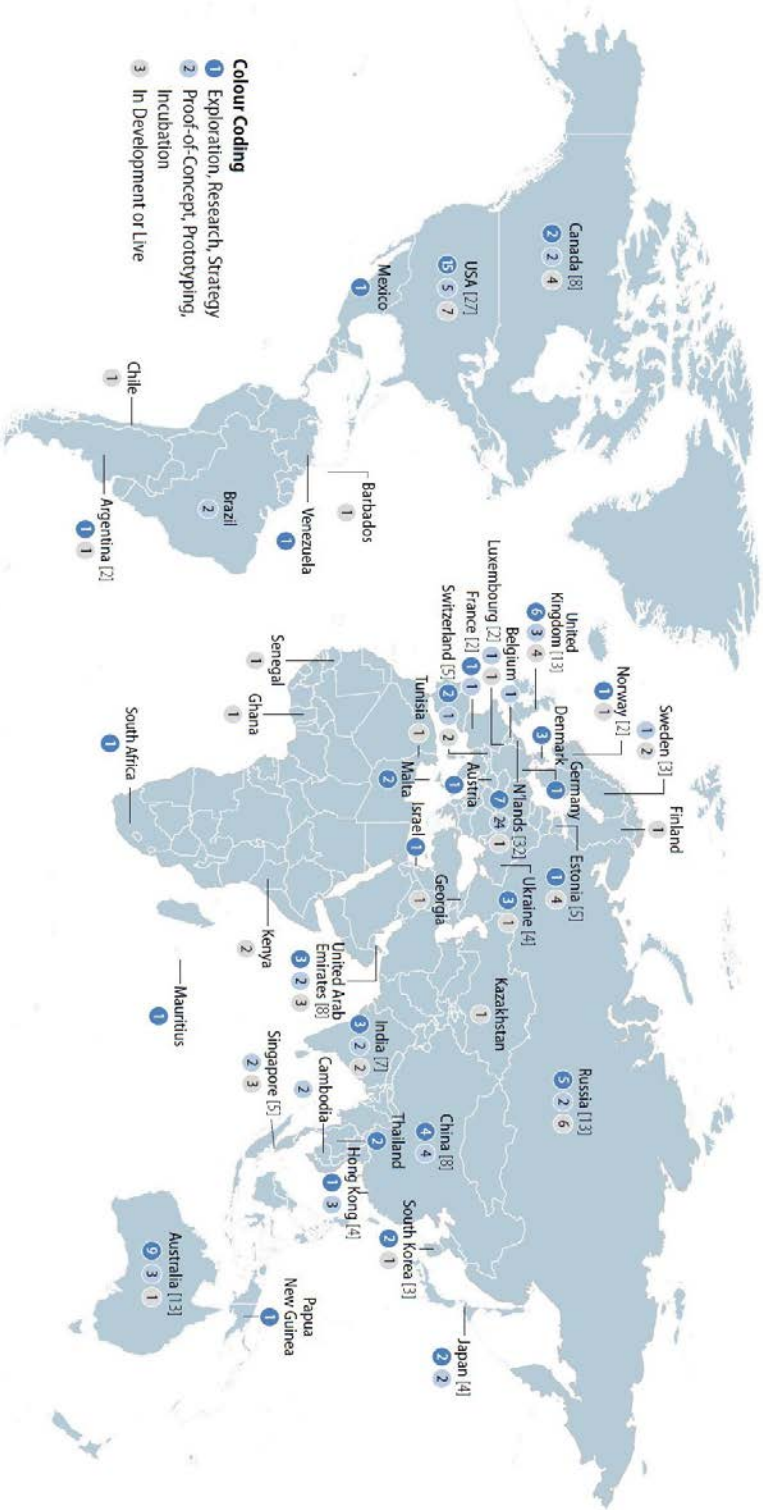
Governments are involved in at least 200 Blockchain Initiatives

58. As illustrated in Figure 4, at least 46 countries around the world have launched or are in the planning stages to launch over 200 Blockchain-related initiatives. Case studies on several of these initiatives are presented in Appendix A.

59. From the initiatives represented in Figure 4, some trends can be seen in which types of projects and industries are industries are emerging as initial front-runners in the use of Blockchain in the public sector (see Table 2). Therese initiatives represent both practical applications of Blockchain technology, as well as communities of practice and partnerships to share ideas and different types of partnerships to explore and implement Blockchain projects.

[11] See Dalal et al, 2017 and the 'Project Ubin' case study in Appendix A.

Figure 4. Blockchain in the public sector, as of March 2018



Source: OECD analysis of data collected by The Illinois Blockchain Initiative, https://illinoisblockchain.tech and http://bit.ly/blockchain-govt-tracker.

Table 2. Top 10 types of projects and industries

Rank	Types of projects (count)	Industries
1	Strategy/Research (42)	Government Services (173)
2	Identity (Credentials/Licenses/Attestations) (25)	Financial Services (73)
3	Personal Records (Health, Financial, etc.) (25)	Technology & Internet of Things (26)
4	Economic Development (24)	Healthcare (23)
5	Financial Services/Market Infrastructure (20)	Real Estate (22)
6	Land Title Registry (19)	Supply Chain (19)
7	Digital Currency (Central Bank Issued) (18)	Energy (13)
8	Benefits/Entitlements (13)	Transportation (13)
9	Compliance/Reporting (12)	Education (8)
10	Research/Standards (12)	Telecom (4)

Note: Projects may have more than one project type.

Source: OECD analysis of data collected by The Illinois Blockchain Initiative, https://illinoisblockchain.tech and http://bit.ly/blockchain-govt-tracker.

Governments are Initiating Communities of Practices and Public-Private Partnerships

60. Governments are forming communities of practice within and across sectors (e.g., public sector, civil society, and industry) and public-private partnerships (PPPs) to work together on exploring the use and implications of Blockchains in the public sector. These types of arrangements are emerging across administrations and share an effort to bring public agencies and private firms together in developing Blockchain systems. They include large consortia such as Hyperledger,[12] but also the Crypto Valley Association in Switzerland,[13] the Blockchain Trust Accelerator in the United States (US),[14] or the Blockchain and Virtual Currency Association of India. They aim to bring all actors into one same community with similar goals and aims with regards to Blockchain technology.

61. In an interview with OPSI, Justin Herman, who heads one such community of practice—The United States Emerging Citizen Technology Office (ECTO), within the U.S. government's General Services Administration's (GSA)—explains that "public-private partnerships are not only desired; they are encouraged".[15] Since the creation of the Dubai Future Foundation's Global Blockchain Council in early 2016,[16] at least 15 Blockchain-related projects have been launched to date, a large majority of which are PPPs (Raford, 2017). More specifically, a trend is emerging in private firms assist government agencies with the technological aspect of the work. One example of PPPs in this sector is the ID2020 initiative,[17] a PPP between United Nations agencies, private sector companies such as Microsoft and Accenture, and foundations such as the Rockefeller Foundation. ID2020 has the potential to make a profound impact on the public sector as well as the 1.1 billion people in the world who live without an officially

[12] See https://www.hyperledger.org.

[13] See https://cryptovalley.swiss.

[14] See Appendix A for a case study on the Blockchain Trust Accelerator.

[15] See Appendix A for a case study on ECTO.

[16] See Appendix A for a case study on the Global Blockchain Council.

[17] See http://id2020.org.

recognised identity, including many refugees, by providing these individuals with an identity through a platform based on Blockchain technology and built on open standards and an interoperable application programme interface (API).

62. This rapid development in PPPs, and stronger links between private and public spheres, is in part due to the lack of subject-matter knowledge and Blockchain-related technical expertise within governments. The proliferation of PPPs makes sense, given that coding proficiency within government remains limited at this point. Axelle Lemaire (2017), former Minister for Digital Affairs for France, said of the French administration, "we would have to hire data scientists with salaries that compete with that of private companies. This is simply impossible". Smart Dubai's office, acknowledging the issue, has provided 14,000 civil servants with data literacy courses. Regardless, even when the public sector outsources coding tasks to the private sector, it is still critical to maintain a baseline level of in-house knowledge to ensure resources are handled efficiently and securely and that the underlying assumptions and decisions that are coded into the Blockchain technologies are understood and achieve the desired effect. It is government's responsibility to ensure that private data is safeguarded and that appropriate decisions have been made in the design of Blockchain protocols and applications.

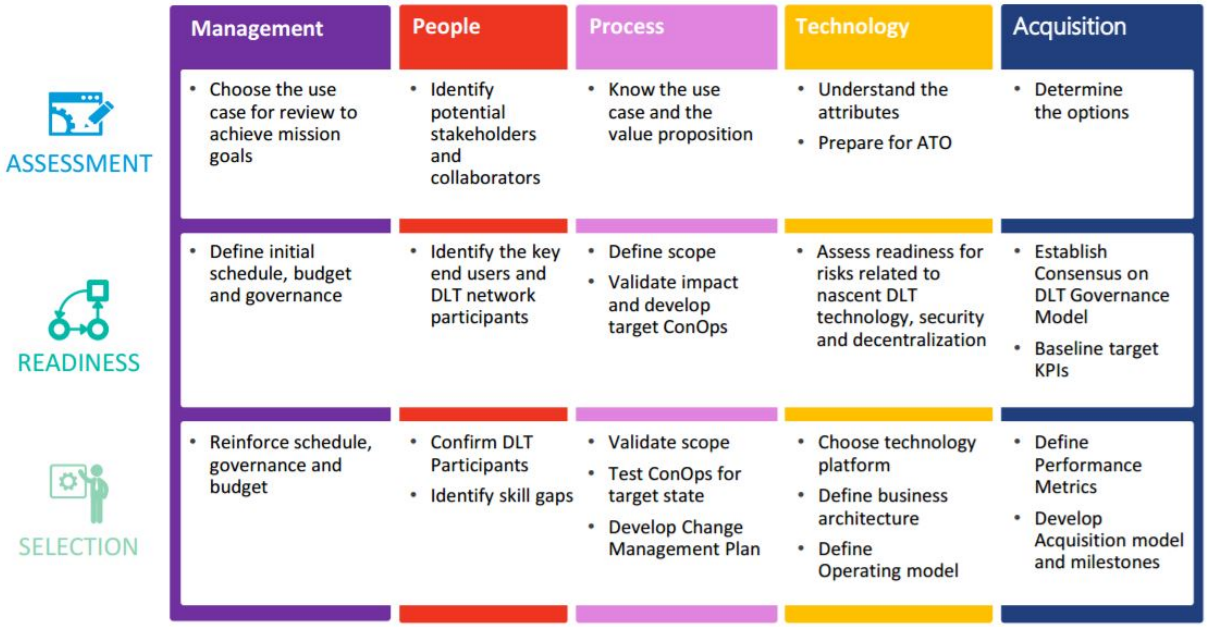
63. Given the knowledge and experience held by industry, governments should consider developing strategies for collaborating and partnering with the private sector to pursue Blockchain goals. Such collaborations have become simpler of recent months, as a number of corporations have launched Blockchain-as-a-service offerings, which allow governments to spin up Blockchain networks more efficiently and easily than has been possible before (ACT-IAC, 2017). Universities also may prove to be invaluable partners, as they can serve as evaluators of new technologies, sources of skilled individuals, and homes for experimentation, knowledge exchange, and proofs of concept (UK House of Lords, 2017).

64. A PPP based in the United States, the American Council for Technology and Industry Advisory Council (ACT-IAC), has developed a Blockchain Primer[18] and a Blockchain Playbook[19] to support government organisations in understanding and applying Blockchain. The playbook walks public servants through the phases and key activities that ACT-IAC has identified as important for leveraging Blockchain technologies in government (see Figure 5).

[18] See https://www.actiac.org/act-iac-white-paper-enabling-blockchain-innovation-us-federal-government.

[19] See https://blockchain-working-group.github.io/blockchain-playbook.

Figure 5. ACT-IAC Blockchain Playbook Key Activities



Source: https://blockchain-working-group.github.io/blockchain-playbook/, https://www.actiac.org/system/files/Blockchain%20Playbook%20Flyer.pdf

2.6. What are ways governments can use Blockchain technology?

65. As discussed, governments around the world are rapidly expanding their exploration and use of Blockchains for a variety of uses. Just about every area of the public sector could benefit from Blockchains in some way (ACT-IAC, 2017). In the future, centralised authorities could become less relevant in the context of Blockchain technologies, or their role could shift to providing a platform and governance for decentralised services rather than being at the centre of every transaction.

66. In reviewing global trends and research, a number of Blockchain technology use cases have emerged that governments are most actively exploring, and in some cases, actively implementing.

67. In many instances, it may be possible that a number of the use cases below could interact with each other in order to achieve desired outcomes. For example, a Blockchain that manages the disbursement of financial aid to social security recipients may cross-reference a Blockchain that manages identity information and another Blockchain that contains information that could confirm eligibility for benefits, thus mitigating fraud risk and automating processes that may have previously involved significant overhead from multiple authorities. This is similar to how data sharing across databases enabled by Application Programming Interfaces (API) occurs today, but leveraging Blockchain technology can be more advantageous and less complicated for some uses (Marchionni, 2018).

68. In considering these uses, it is important to remember that both permissioned and permissionless Blockchain ledgers exist. With permissioned Blockchains, the government entity or entities that create and manage a Blockchain will have the ability to prescribe

relevant permissions for accessing and adding new information. (See previous section on "Different types of Blockchain ledgers: Permissioned and Permissionless").

69. Appendix A provides a series of case studies on Blockchain communities and the real-world applicability of Blockchain technologies in the public sector, including cases that illustrate some of the uses discussed in this section.

2.6.1. Identity (credentials, licenses, etc.).

70. Blockchains could be used to establish digital identities[20] for citizens, residents, businesses, and other government affiliates. In addition to using Blockchain technology to manage identity, multiple aspects of the identity could be managed using Blockchain technology. For example, birth certificates, marriage licenses, passport and visa information, and death records could be managed via Blockchains (ACT-IAC, 2017). In fact, as seen in Figure 4, identity management is the second most pursued Blockchain project type, second only to strategy and research. In addition to making services more seamless and less burdensome for individuals, Blockchain-based identities could also help protect against identity theft, which is Europe's most significant enabler of crime (UK House of Lords, 2017), especially if associated with some type of multi-factor authentication or biometric, though the latter may be controversial in some countries.

2.6.2. Personal records (health, insurance, financial, etc.)

71. Beyond those mentioned under identity, other personal records may be managed with Blockchains. Health records, for example, could be made accessible and interoperable to all hospitals in a network or in a country. Governments will need to strongly consider patient privacy rights in such an application, such as ensuring patient authorisation is given in advance, and that ultimately, they own and control their own data. Within government, payroll systems could be built using Blockchain technologies, where employees could input their time and be paid automatically through smart contracts (ACT-IAC, 2017). Personal records is tied with identity for the second most common type of Blockchain project pursued by governments around the world, with 25 projects (see Figure 4).

2.6.3. Financial services and banking

72. Blockchain technology can be used by governments to ease the overhead and burden associated with transferring funds among parties (e.g., facilitating inter-bank and international payments).[21] In addition, some countries' central banks are experimenting with their own digital currencies build upon Blockchain platforms. For example, Canada has experimented with a digital currency called CAD-COIN as a way to better understand the technology first-hand.[22]

---

[20] An example of a Blockchain-enabled identity program is the ID2020 initiative (https://id2020.org), as discussed in OPSI's *Embracing Innovation in Government: Global Trends 2018* report. See http://oe.cd/innovation2018 (page 22).

[21] An example of Blockchain technology being used for financial services can be found in the Project Ubin case study in Appendix A.

[22] See https://www.forbes.com/sites/laurashin/2016/06/16/canada-has-been-experimenting-with-a-digital-fiat-currency-called-cad-coin.

2.6.4. Land title registry

73. Land title registry[23] is a natural fit for Blockchain technology. Land titles and other records related to ownership could be chronologically recorded on a Blockchain ledger, along with any details relevant to a sale of property. As Blockchain transactions are immutable, a full historical record of a property or other asset could be reviewed through previous records in a Blockchain. This could minimise the need for expensive and time-consuming third-party involvement for transactions (ACT-IAC, 2017). As scene in Figure 4, land title registry is the sixth most pursued Blockchain project type.

2.6.5. Supply chain management, asset tracking, and inventorying

74. Similar in principle to land title registry, having a comprehensive historical record of an asset is the essential purpose of supply chain management and asset tracking.[24] Blockchain transactions can be used as a means of documenting every transfer of an asset from its origin. Governments could track an asset from its creation, through potentially multiple stages of transportation, and eventually through purchase and even managing asset inventory. This gives anyone with permission the ability to view the chain of custody (e.g., government officials, the public) and thus enables trust in the asset (Yaga, 2017). Potential examples include tracking food, medicines, natural resources such as diamonds, and many others from origin to distribution.

2.6.6. Benefits, entitlements, and aid

75. The benefits, entitlements, aid processes of today often involve a significant amount of overhead and checks for compliance. Government programs such as social security and pension payments, medical care benefits, and domestic and international aid could benefit tremendously from Blockchains. For example, smart contracts could be used to automate processes for eligibility verification and disbursement of funds, such as distribution of funds for those affected by a major natural disaster. In addition, Blockchains could help to ensure that benefits reach their intended beneficiaries and are not diverted (UK Government Office for Science, 2016).

2.6.7. Contract and vendor management

76. As discussed previously, in permissioned ledgers, perfect transparency can be given to system and transactions while only authorised users are able to record transactions. This enables the potential for Blockchain technology to be leveraged as a tool for transparency and accountability in government spending, which is often executed through federal contracts.[25] Things such as tracking and paying vendors, managing purchase commitments and transactions, and monitoring schedule performance could all be done in a way the is accessible to all relevant players, as well as the public, as appropriate. In addition to the transparency and accountability angle, Blockchains can make government contracting more efficient by eliminating a significant amount of

[23] Examples of Blockchain technology being used for land title registry can be found in the BenBen and Sweden Land Registry on Blockchain case studies in Appendix A.

[24] An example of Blockchain technology being used for asset tracking can be found in the Vehicle Wallet case study in Appendix A

[25] An example of Blockchain technology being used for contract and vendor management can be found in the Blockchain Talent Hackathon case study in Appendix A

overhead and automating processes that lend themselves to the logical "if/then" workflows of smart contracts.

2.6.8. Energy utilities

77. Public energy utilities may benefit from Blockchain technologies for managing of smart energy grids.[26] Blockchains allow for the "recording of autonomous, machine-to-machine transactions regarding electricity use" (Yaga, 2017). Blockchains could also be used to managing and tracking contributions from different power plans into a smart grid to ensure each power generator is credited appropriately for their contribution (Yaga, 2017).

2.6.9. Copyrights

78. Governments often allow for the registration of copyrights or need to adjudicate disputes related to copyrights. As content becomes so multidisciplinary and copyright ownership becomes ambiguous, Blockchains are excellent tools to "timestamp [artists' and content producers'] work, keep a 'vigilant' eye out for anyone violating their copyright, create a permanent record of their work and issue their clients a time-stamped copyright certificate" (Willms, 2016). In this sense, they also serve as proof of ownership and proof of existence.

2.6.10. Voting

79. Blockchain technologies have the potential to enable new methods of voting[27] by transforming what often remains a paper-based process in countries, or an electronic process with limited validation and auditability capacities. This can enhance the convenience and confidence for citizens. By ensuring that individual votes are eligible and counted correctly, use of Blockchains also has the potential to help prevent voting challenges such as ballot rigging, which still persist in many countries. These challenges, if not overcome, can result in a lack of trust in democratic processes and can enable election results that do not reflect the wishes of the public. (Foroglou and Tsilidou, 2015).

2.6.11. Mitigating and identifying fraud

80. Through verifications of things such as land ownership, other assets, and identities, Blockchain technologies can assist governments in mitigating the risk of fraud, as well as identifying fraudulent transactions that do manage to get through. One major example of this would be for assessing and collecting tax payments.

2.6.12. Streamlining interagency and cross-sector processes

81. Conducting transactions across different governmental organisations can sometimes be challenging, especially if tasks are paper-based or use information systems that have limited interoperability. With traditional information systems, data is often duplicated over and over again, or centrally located but involving redundant processes for

[26] An example of Blockchain-enabled electricity grid management, although private sector, is the Brooklyn Microgrid (http://brooklynmicrogrid.com).

[27] An example of a Blockchain-enabled voting experiment conducted with Colombian expatriates can be found in OPSI's *Embracing Innovation in Government: Global Trends* 2017 report. See http://oe.cd/eig.

reconciling data (UK House of Lords, 2017). Blockchains and smart contracts can automate some transactions and make interagency processes more efficient and effective by removing the need for third-parties and automating transaction handling (ACT-IAC, 2017). In addition, "agencies that are part of a Blockchain network can securely and seamlessly share information stored on a shared ledger" (ACT-IAC, 2017), which can help ensure agencies across government work with the same trustworthy information, lessening the chance of inconsistencies, as there is a common source of reference data.

82. Importantly, this allows governments to work efficiently and effectively without the need for strict centralisation or overly burdensome standards. Blockchains can "enhance efficiency, security, transparency and engagement, while allowing each of their entities to run their own processes with their own technology stacks, regardless of the processes and technologies of any other entity" (Marchionni, 2018). This allows one agency to focus on the mission and tasks they know best with less of a need to understand the processes and information systems of other organisations.

83. These same benefits can also help reduce friction for the privates sector when interacting with government. As noted by the UK Government Office for Science (2016), "one of the greatest potential benefits of DLT is its ability to remove barriers and friction in the market and enable the creation of new forms of information marketplaces… [T]he sharing of information between economic entities through distributed ledgers would enable new forms of innovation to emerge. This would allow ministers to achieve policy outcomes centred on assisting [small and medium-sized enterprises] achieve economic growth through effective use of technological innovation."

3. Challenges, limitations and other consideration of Blockchain technologies in government

84. Naturally, the use and implementation of Blockchain technology presents some challenges, and Blockchains are not a solution to every problem in the public sector. This section seeks to make sense of such challenges and understand where technological limitations lie.

3.1. Immutability

85. Immutability is one of the most core characteristics and benefits of Blockchain technologies, but is perhaps also its biggest limitation in terms of practical applicability. A Blockchain is essentially a list to which information can only be added. Unlike the traditional databases used by the public sector today, there is no way to remove data that has been entered into the Blockchain. In instances where updating and/or deleting data is a regular occurrence, using Blockchain technology may not be the best option. Decision makers would need to decide if the benefits of using Blockchains outweigh the inability to update and delete data and must ask themselves whether immutability is practical for the type of data they use (Yaga et al, 2018).

3.2. Transparency, Confidentiality and Decentralisation

86. Permissionless Blockchains allow for perfect transparency, where "decentralised architectures generally rely on the disclosure of everyone's interactions" (DeFilippi, 2016). Confidentiality settings are close to non-existent. Yet confidentiality and privacy mechanisms, at a time when the storing of personal information becomes more likely, are of paramount importance. Rules and laws insist on the absolute protection of such information. For example, the EU's right-to-be-forgotten principle stipulates that an individual may request the removal of information about themselves, potentially including within some government records (see Gabison, 2016). Because of its immutability, if information about an individual is stored on a Blockchain, right-to-be-forgotten is essentially unenforceable. However, this problem may only be relevant to the public sector in certain instances, as citizens do not have the right to request the removal of their information from all government databases. For example, no one can ask for a government to delete his identity information or judiciary records. Only specific applications of right-to-be-forgotten may apply. In addition, many, if not most, public sector applications of Blockchain technology would be permissioned ledgers, which give public officials the ability to control access.

87. In addition, the consequences of the European Union General Data Protection Regulation (GDPR) on Blockchain technology are not yet fully understood. As noted by the UK House of Lords, "The interaction of DLT with data protection laws such as GDPR requires close analysis. Compliance may require 'permissioned' or access-controlled DLT… GDPR issues include reconciling 'immutable' ledger entries

with the data subject's rights to rectification and erasure and with the need to ensure that international data transfers are lawful." Data covered by such regulations may need to be private or stored off-chain to meet the law (Van Humbeeck, 2018), while other data may be better on-chain to meet mandatory data retention rules, as the immutability of Blockchain technology is suited for this task.

88. A necessary trade-off will have to be struck between levels of decentralised decision-making and privacy settings. Higher levels of privacy will require more formal governance models (permissioned Blockchains) while "radical transparency" (DeFilippi, 2016) (e.g., permissionless Blockchains) could bring risks to the exploitation of personal data, but remains closer to the Blockchain technology's underlying aim to function independently of centralised authorities. Governments may also have to consider carefully which information is stored on a Blockchain, and is therefore immutable, and which information is stored off of chain, perhaps with only a link or a reference existing on the Blockchain. Public officials will need to consider privacy at the technical level as part of the design process of developing Blockchain technologies for their organisations.

3.3. Data Storage

89. Public and private sector entities often use databases as a means of storing large amounts of data, in the form of documents, images, videos, and applications, among many others. A Blockchain is more generally a list of transactions, and at most contains small pockets of data used to execute and guide smart contracts. They are not designed for general data storage. Large amounts of data, however, can be stored off of the Blockchain and linked to from within a block transaction. (Yaga et al, 2018). If government team is only looking for data storage, Blockchain technology may not be the best fit. However, if they are looking for a way of maintaining a distributed and trustworthy record of transactions, Blockchain technology may be a viable solution. It is entirely possible that a hybrid approach is needed, where both Blockchain technology and a data storage solution are both pursued, which provide the ability to link Blockchain transactions with data held off the chain and stored elsewhere.

3.4. Data Quality

90. Just like traditional information systems, the quality of the data that is input at the origin will directly affect quality of the data on a Blockchain and the quality of the results derived from that data. In other words, "No amount of analytics can compensate for a lack of accurate, timely and authoritative data at the point of input. Bad data cannot be made good, just through analytics." (UK House of Lords, 2017).

3.5. Coding and Governance Models

91. One of the most often discussed benefits of Blockchains is that is that they can eliminate the need for a central authority. However, this is not entirely true, even for permissionless ledgers that anyone can access and conduct transactions. Blockchains do not appear out of thin air – they must be built and governed by code developers, engineers, and other decision makers who have been entrusted with key roles for the development of a Blockchain platform. These developers are a de-facto central authority, and their composition and actions and underlying decisions coded into a Blockchain may not be as transparent as the transactions themselves. This raises and important question. Who, or what, is the legitimate governing entity of Blockchains, be it public or private?

As greater accountability on all spheres of public life is demanded by civil society, decisions over who controls Blockchains is of importance.

92. Levels of decision-making, and the integration of such decisions in the platform's code, are thus contingent on the code previously drafted. Power dynamics, even in public sector Blockchains, are ultimately constrained by what the code of each and every platform allows for.

93. As governments bring their attention to Blockchains and further development occurs, it might be that there will need to be an added focus on the level of government intervention versus room for a consensus-based way forward. It will ultimately require government entities to be familiar with the process of coding, even if the actual practice of coding is outsourced, to ensure the appropriateness of, and to assume the responsibility for, the resulting Blockchain product. In addition, governments must consider the governance structures for their use of Blockchain technologies and the decisions that go into them. This ranges from high level decisions on government-wide Blockchain strategies and uses, down to the governance and permissions for architecting and implementing individual Blockchain protocols, networks, and applications.

3.6. Talking About Blockchain

94. There seems to be a large consensus across Blockchain technology specialists that talking about Blockchains to citizens is one of the most complex parts of their jobs. According to Justin Herman (2017), Emerging Citizen Technology Office lead at the US's General Services Administration, "The technologies of Blockchains are supposed to increase trust. And yet, […] either within Government or within the Blockchain community itself, there is an inherent distrust. That's one of the most important things we have to work on". Similarly, Tomicah Tillemann (2017), co-founder of the Blockchain Trust Accelerator at the New America think tank, considers the lack of education about the technology to be one of the main hurdles facing the Blockchain community: "Blockchains are technologies that are very misunderstood, it is complicated technology. We spent a year and a half with some of the best thinkers and the best communicators in the World, trying to come up with new strategies for explaining the technology. We have made some progress there, but the basic reality is that this is not a simple technology".

95. At the same time, Emmanuel Noah (2017) of BenBen speaks quite differently of his introduction of Blockchains to senior public officials: "What spoke most to the authorities when we introduced our Blockchain solution were the benefits that the solution brought in terms of public service delivery, along with the possibility to maximise revenue generation […]. The Government has revenue targets, customer satisfaction reviews – these were the main arguments we used with the Government". On a rather different page still, Mats Snäll (2017) of the Land Registry Authority argues that he "should not be forced to explain [Blockchain technologies] because no one should even care about that. By essence it is complicated to explain a technology if you are not a technician. You are not asked to explain how a medical diagnosis works if you are not a doctor." Regardless of exactly how it is explained, more will need to be done to convey the possibilities before Blockchain technology can be used widely and become accepted.

3.7. Costs

96. Higher short-term costs associated with a still-emerging technology prevent its widespread use for the time being. While these costs are particularly daunting for firms,

the political nature of government-run Blockchains must also be taken into account as initial investments are discussed, and cost-benefit analyses are run. As found in a number of studies, "running costs associated with the adoption of [distributed ledger technology] DLT/Blockchain are as yet unclear" (Deshpande et al., 2017). Limited long-term visibility over the feasibility of Blockchains also remains: "currently, the return on investment for businesses is unclear, which could make it more difficult to argue a case for investing in DLT/Blockchain solutions" (Deshpande et al., 2017). A relatively new emergence of Blockchain-as-a-service solutions in the market has the potential to make experimentation with Blockchain technology easier and faster, which much of the technical underpinnings already accounted for (ACT-IAC, 2017).

3.8. Challenges related to "Proof of Work" Consensus Model

97. The Proof of Work consensus model is the most common method for adding new blocks on permissionless Blockchains (see previous section on "Different types of Blockchain ledgers: Permissioned and Permissionless"). Appendix C of this guide contains definitions and details that are important for understanding consensus models, including the Proof of Work and other models.

98. However, public sector applications of Blockchain technology may be more likely to leverage permissioned Blockchains that are more suited to models such as Proof of Authority. This is because a Blockchain structured in this way would allow for role-based permissions for accessing and adding new information on a Blockchain.

99. Although it may unlikely for a government to use Blockchains that use the Proof of Work model, it is important for government decision makers to be aware of this model and its associated challenges. This is especially true because many of the commonly discussed challenges of Blockchains, such as the ones listed below, apply only to the Proof of Work consensus model and do not apply with others. These challenges are often raised as blockers or reasons why Blockchain technology should not be pursued, even when most of the time they are not at all relevant.

3.8.1. Energy consumption

100. Publications and discussion about Blockchain often mention energy consumption associated with using the Proof of Work consensus model, and most particularly of the mining processes on the Bitcoin platform.[28] As of early March 2018, Bitcoin's estimated annual electricity consumption amounted to 58 Tetra Watthours (TWh) and growing rapidly. This is the equivalent of over 5 million American homes, and roughly the same energy consumption as countries such as Kuwait. This represents .26% of the world's annual consumption,[29] and is clearly an unsustainable practice for environmental reasons. As discussed in Appendix C, this is due to the intentionally intensive processing power required in order to mine new blocks on platforms using the Proof of Work consensus model.

101. However, this extreme energy consumption applies only to Blockchain platforms using Proof of Work. It is likely that the majority of public sector applications of

[28] See examples at https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency and https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that.

[29] See https://digiconomist.net/bitcoin-energy-consumption for current figures.

Blockchain technology would leverage different consensus mechanisms, especially ones such as Proof of Authority that are designed for permissioned ledgers, for which energy consumption would not be an issue.

3.8.2. Scalability

102. Permissionless Blockchains using Proof of Work can encounter scalability issues that limit their usefulness. This is a scenario where the platform is not capable of processing transactions as quickly as is needed and can reach a processing capacity maximum. This is especially evident in currency platforms like Bitcoin. Bitcoin is only capable of processing roughly seven transactions per second, which would never compete with more traditional financial companies such as Visa (1,667 transactions per second) or PayPal (193 transactions per second) (Rosic, 2018).

103. These issues are due to the time is takes to add transactions to a block, and the time it takes to publish a block to the chain through mining through the use of a consensus model (see Appendix C). As a platform becomes more popular, the problem grows as (1) more users want to send more transactions, and (2) the data for these transactions must be propagated throughout the entire growing Blockchain network. (Rosic, 2018).

104. A number of technical fixes to this limitation have been proposed, but none have been successfully implemented to solve the problem (Rosic, 2018). Without a fix, Blockchains using the Proof of Work consensus model swill struggle to scale sufficiently to compete with existing proven technologies, such as the ones used by Visa and PayPal.

3.9. Conclusion

105. In conclusion, Blockchains are simply ongoing, immutable, and distributed lists of transactions, with a lot of technical features that ensure a list can be trusted.

106. The technology is in its infancy in terms of public sector exploration and applications, but Blockchains have “immense powers” (Rinearson, 2017) that are waiting to be unleashed. In the future, centralised authorities could become increasingly irrelevant in the context of Blockchain technologies, or their role could shift to providing a platform and governance for decentralised services rather than being at the centre of every transaction. It is imperative that the public service builds its knowledge in this area and consider its possible applications and how it may affect its role.

107. For now, at a time where governments are deeply focused on cost-effectiveness and accountability, and see these aspects as key features of sound policy-making, Blockchains need to be understood in order to understand the potential solutions to a range of challenges or areas of work in this sector. Of the case studies that already exists, it is possible to say that Blockchain technology has the potential to allow the public service to:

- Improve effectiveness,
- Reduce friction between agencies,
- Reduce bureaucratic barriers,
- Better share knowledge, and
- Foster automation through smart contracts.

108. At this emergent stage, it is not possible to make any decisive claims about the future of Blockchain technology or any clear-cut recommendations about where it should be used and precisely how. The only clear recommendation that can be made is that governments should invest in building its knowledge of this technology and explore, and even experiment with, its possible applications. It should also not do this alone, but identify and collaborate with partners from other parts of government, from other governments, and from other sectors. Blockchain technology has the potential to catalyse a major shift in public service delivery and internal government strategies. In some instances, it could even results in government no longer serving in the same central authority role, but instead shift to being responsible for providing the legitimacy and credibility for such new technology to be trusted. Even if 'in-house' technical capability is currently low in government, and it is likely much of the short to medium-term applications of Blockchain in the public sector would be outsourced, it is still critical to strengthen the level of in-house knowledge to ensure resources are handled efficiently and securely and that the underlying assumptions and decisions that are coded into the Blockchain technologies are understood and achieve the desired effect.

109. The following Appendix A moves from the technicalities to the implementation of Blockchain services in, and for, government. A non-exhaustive set of case studies are presented to demonstrate the kinds of Blockchain-centred initiatives, experiments, and communities from across the world that OPSI has observed so far.

4. Appendix A: Case studies of Blockchain applications and communities in the public sector

110. The case studies presented in this appendix offer a non-exhaustive view of how the public sector is currently using Blockchain technology. Consortia of stakeholders – from both public and private spheres – create their own platforms, tailored to the needs of their members. Smart contracts are enabling new forms of digital payments and provision of social services and aid over Blockchains. Complex issues are now being discussed and their possible implications evaluated.

4.1. Case study 1

Name: BenBen

Founder & CEO: Emmanuel Buetey Noah

Launched: 2015

Where: Accra, Ghana

Website: http://benben.com.gh/

4.1.1. THE PROBLEM

111. BenBen tackles two structural issues related to land registry in Ghana:

- Determining the legal existence of parcels and associated land ownership titles are long-standing issues. The lack of adequate and systematic tracking, along with the absence of digital information storing prevents authorities and property owners from having clear certainty and visibility over what belongs to whom;
- The tryptic relationship between property owners, government agencies (more specifically the Ghanaian Land Commission) and financial institutions appears to be weak and inefficient. In the words of Noah (2017): "you have to physically go to the Land Commission to search in existing registries, then bring the correct documents to the bank". In turn, it could take up to a year or more before collateral is registered – thus presenting huge risks to both lenders and borrowers.

4.1.2. THE SOLUTION

112. BenBen provides an Ethereum-run digital register system of all land registries across Ghana. It is able to certify land information through a combination of satellite imagery and on-the-ground verifications, working hand-in-hand with local stakeholders in the land market. It aggregates all the information such that financial institutions and the Lands Commission have real-time access to the data. Based on a business-to-business

(B2B) model, BenBen does not directly work with property owners. Rather, businesses use the BenBen platform as they refer to both the Lands Commission and financial institutions to trigger a transaction, confirm a sale, access credit and prove true ownership. In this light, BenBen acts as a risk-mitigation tool to financial institutions, governments and property owners during the entire land transaction process.

113. The use of digitised and incorruptible ledgers on land ownership records and land titles in Ghana has also led to the User Committee of the Commercial Courts in Ghana to explore the use case of BenBen as an expert witness in land related commercial disputes. It provides instant, reliable and untampered-with information to determine the legality of a claim on land ownership.

4.1.3. RESULTS AND IMPACT

114. BenBen uses three key metrics to evaluate its impacts and successes: the number of digitalised records, the number of transactions logged on the Blockchain; and the number of records verified with on-the-ground confirmation and satellite imaging. As of 2017, BenBen counts 10,000 records integrated to its digital register – with many leading to successful transactions. Public and financial institutions also support the BenBen initiative and several pilots have now been run with the Land Commission and Barclays Bank of Ghana.

4.1.4. KEY POINTS

- 70% of court disputes in Ghanaian national courts are land-related.
- Average time to receive to confirm land entitlement: was one year. This has been reduced to an average of three months with BenBen's services.
- Average time to receive real-time land information from the Lands Commission: was one month. This has been reduced to a minimum of 3 days with BenBen's services.

4.2. Case study 2

Name: Global Blockchain Council

Organisation: Dubai Future Foundation

Project lead: Noah Raford, COO

Launched: 2016

Where: Dubai, United Arab Emirates (UAE)

Website: http://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/

4.2.1. THE PROBLEM

115. As Blockchain technology develops in what Noah Raford calls the 'pre-legal stage', companies and administrations in Dubai lack a clear strategy and way forward to develop its use at systemic levels. There is a need for some form of centralising platform that opens the way for knowledge sharing and best practices.

4.2.2. THE SOLUTION

116. The development of a large, multi-stakeholder Global Blockchain Council, where both private firms and public agencies are invited to understand the technology better, its implications and impacts, and the way forward in terms of experimentation, institutional support, and drafting the future of regulation. Furthermore it provides ways to talk about Blockchain in accessible ways to non tech-savvy managers and decision-makers, by focussing on what the technology enables rather than what it is. It facilitates the development of public-private partnerships (PPPs) while creating in substance a new eco-system around Blockchain – always asking the question "how can Blockchain be useful to you?". Within this new space, the Dubai Future Foundation aims to ensure and enhance the governance structure of this eco-system to ease relationships with the city of Dubai and open the way for experimentation in both public and private sectors.

4.2.3. RESULTS AND IMPACT

117. The Council board is now made of 46 leaders in the field from both private, technology-geared firms and public agencies from Dubai and the UAE. Fifteen experimentation pilots have been introduced, almost all of which are PPPs, with firms taking the role of technical and technological providers. Furthermore, the city of Dubai is now ready to have 100% of monetary transactions run through the Blockchain within the next three years. For this to occur, the Smart Dubai Office, in charge of the implementation of the Blockchain technology strategy, has trained 14,000 public servants in data science and technological literacy.

118. The impacts are not limited to Dubai and the UAE. While Noah Raford easily recognises that the size of the Emirates' public service is nowhere near that of larger countries, he claims that the Global Blockchain Council redefines the landscape of possibilities with regard to emerging technologies. It sets goals other national administrations can look to and see that it can be done.

4.2.4. KEY POINTS

- 14,000 public servants trained for data science in the past 18 months.
- 15 pilot projects supported by the Dubai Future Foundation in the past 18 months.
- "Out of our ethnographic research, [we found] among our partners, which include everything from the state-owned bank to the major companies to the tourism board of Dubai, that cryptocurrencies in general were beginning to have a disruptive effect on banking and finance. But then, with a little more research, we realised that the fundamental technologies beneath that, the distributed ledger approach, had profound implications for just about every other sector of the economy and society. It is fundamentally new way of rearranging and administering information."

4.3. Case study 3

Name: Intragovernmental Emerging Citizen Technology Office (ECTO)

Organisation: General Services Administration (GSA)

Lead: Justin Herman

Launched: 2017

Where: United States

Website: https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology

4.3.1. THE PROBLEM

119. Government agencies across the US federal public system are inclined to dive into, and use, Blockchain technology to provide a solution to unresolved issues. However, "there are no policies, there is no guidance, there is no White House support, there is no contracting vehicle" (Herman, 2017). A centralised platform is missing for government agencies and public servants to share best practices, make sense of use cases and go forward with the technology in more proficient manners.

4.3.2. THE SOLUTION

120. After a pilot consultation on Artificial Intelligence (AI), the GSA's Emerging Citizen Technology Office aims to consult, gather and make sense of agencies' experience with Blockchains and ways in which the technology could be better understood within the federal public sector. It brings the subject-matter expertise of many public servants to the fore, while presenting the technology to others in digestible ways. Whenever possible it encourages the input of private start-ups and companies to develop an eco-system between public and private sectors. Finally, it has an aim to change the narrative surrounding Blockchain technology to dissociate it from the mistrusted Bitcoin platform.

4.3.3. RESULTS AND IMPACT

121. Following a successful forum in July 2017, ECTO gathered over 200 use cases from across the federal public service and triggered the launch of a government-wide community of practice on Blockchain technology. Further it actively works with concerned stakeholders to introduce Blockchain technology to public servants and citizens-at-large in new, practical and easily-accessible ways.

4.3.4. LIMITATIONS AND THINKING AHEAD

122. There are still some misunderstandings related to Blockchain technology and the challenges associated with the Bitcoin platform in the general public. More must be done to change the narrative over Blockchain in the public sector and thus instil trust in the population. Furthermore, while Blockchain may be the answer to unresolved issues, it is not the one and only. The study of use cases explicitly shows that Blockchain is not always well-suited to target specific problems that an agency may be experiencing. An analysis of existing products and other emerging trends and technologies remains crucial.

4.3.5. KEY POINTS

- Over 100 different agencies registered to the Federal Blockchain Forum in 24 hours
- "We hear a lot of people today taking the role of open data advocates. And I ask: what is the intersection between open data and Blockchain? Well, you can open data, and add a new layer of Blockchain to ensure that the data is trusted and traceable. Right now it's open – and that's fantastic – but it does not mean it's real."

4.4. Case study 4

Name: Project Ubin

Organisation: Monetary Authority of Singapore (MAS), in partnership with Deloitte

Project Lead: Stanley Yong

Launched: Phase one was run from November to December 2016 (six weeks)

Where: Singapore

Website: http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx

4.4.1. THE PROBLEM

123. The Monetary Authority of Singapore (MAS), as part of its mandate, ran an industry study on industrial and financial problems Blockchain technology could bring a possible answer to. It was found that Blockchains could serve the purpose of more efficient, cheaper and faster inter-bank payments for cross-border monetary and government securities transactions.

4.4.2. THE SOLUTION

124. MAS partnered with R3 – a consortium of banks and regulators specialised in digital ledger technologies – to develop and apply a Blockchain-based transaction process with a digital Singaporean dollar. This would not only allow incorruptibility through a decentralised trust system, but it would allow transactions to run 24 hours a day with no centralised – i.e. human-based – checks required. It invited a number of different banks – the main beneficiaries – to participate in the early development and trials of the technology.

125. The prototype uses the Ethereum platform to make best use of smart contracts. Furthermore, it makes full use of the MAS MEPS+, a Singaporean-run system that enables real-time and irrevocable transfer of funds and Singapore Government Securities. Project Ubin thus uses what already exists in terms of digital transaction mechanisms (MEPS+) and adds a Blockchain 'layer' for higher security and efficiency – both time and costs – of transactions.

4.4.3. RESULT AND IMPACT

126. By the end of Phase 1 in December 2016, Project Ubin demonstrated that a working interbank transfer prototype on a private Ethereum network was successfully built, and a Smart Contract codebase developed. More importantly, it managed to fully integrate existing technologies on digital transactions with a rather new Blockchain technology.

4.4.4. LIMITATIONS AND THINKING AHEAD

127. Due to the very nature of financial transactions, some level of privacy is required to protect transactional actors. There is a crucial need to develop some types of privacy settings within a system – Blockchains – which very principle is full information in a decentralised decision-making context. Phase 2 of the project thus aims to develop such privacy settings and answer the complex question of: How can I prove that a transaction

has occurred and the necessary funds to the transaction are indeed present, without showing you the transaction, and without having to refer to a centralised authority? Answers reside in the drafting of complex mathematical protocols that exist, at this point in time, as mere prototypes and beta versions.

4.4.5. POINTS TO HIGHLIGHT

- Due to the required checks and balances, cross-border transactions occur during an average time window of two hours every day, with constant participation of banks. Such figure can increase to 24 hours a day once Blockchain systems are set up and secured
- It made full use of existing technologies, and added a block of complexity through the development of Smart Contracts
- "Why is it that our trading systems do not operate 24 hours a day [but only two hours]? This is where Blockchains would come into use. One reason we do not do 24 hours operations for banks is because you need to run operations every day to make sure that everything worked out properly. And those processes cannot just be removed overnight. You don't need a change in operating hours, but in what you do with the system in place, and how you reform it."

4.5. Case study 5

Name: Sweden Land Registry on Blockchain

Organisation: Swedish Land Registry Authority

Project Lead: Mats Snäll, Chief Digital Officer

Launched: 2017

Where: Sweden

4.5.1. THE PROBLEM

128. The Sweden Land Registry seeks to go beyond existing digital systems to record land transactions and ownership – for more efficient, faster and tailored services to citizens. From a more general perspective, the centralised system of information-storing that was developed in Sweden no longer respond to the demands from greater transparency and accountability. Finally, it appears to be of necessity for Swedish government agencies, including the Land Registry Authority, to be on top of the digital and technical scene.

4.5.2. THE SOLUTION

129. Granted that Blockchain technology is the "best and most advanced technology available" (Snäll, 2017) the Land Registry Authority seeks to "explore and investigate if the Blockchain may be an alternative to support the process of a real property transaction; sale and purchase; finance and mortgage; apply and register title/ownership; instead of having the traditional technical database and web application solutions" (Snäll, n.d.).

130. The project is split in three phases. Phase 1 developed a theoretical understanding of what Blockchain technology is and how it works, and why it would be relevant in the context of the Land Registry Authority. Phase 2 aimed to develop the technology to best respond to needs and demands from title owners and the Government. Both these phases

were successfully completed. The last phase to come is one of experimentation, with the goal of developing a working and efficient Proof-of-Concept.

131. Finally it allows digital actors in the Swedish public sector to learn more about the technology – it is a way to be "on the frontline even if we don't implement the Blockchain technology right now" (Snäll, 2017).

4.5.3. RESULTS AND IMPACT

132. Clear impacts on land transaction and ownership are not yet clear – though Blockchains theoretically responds well to the demands of a secured and transparent system of information sharing and gathering by a governmental agency.

4.5.4. LIMITATIONS

133. At this point in time, there is no legal recognition of digital signatures on Smart Contracts. Though Blockchains as a system may work, they would not have a legal value – transactions and contracts signed on a Blockchain may not be legally binding. More must be done on this regulation aspect.

134. It also remains fairly unclear how the governance framework would work around the Blockchain – which is likely to be a more "theoretical and legal issue" (Snäll, 2017) and focus on questions of prerogatives and the role of the State in the development of the technology

4.5.5. KEY POINTS

- "At this time, no one knows what Blockchain means" (Snäll, 2017)
- "The biggest challenge (about Blockchain technology) is probably to try to explain how it works. It is not the concept that is complicated, but the technology in itself"

4.6. Case study 6

Name: Blockchain Trust Accelerator

Organisation: New America, in partnership with BitFury and the National Democratic Institute

Co-Founder: Tomicah Tillemann

Where: Washington D.C., USA

Website: https://www.newamerica.org/bretton-woods-ii/blockchain-trust-accelerator

4.6.1. THE PROBLEM

135. The founding organisations observed a broken public infrastructure in the US and a non-existent feedback loop between citizens and government agencies. At the same time, demand was growing for some form of accelerator and a larger community of practice around the topic of Blockchain technologies.

4.6.2. THE SOLUTION

136. BTA co-founders first turned to the Estonia for ideas. Indeed, the Estonian public service had been driven by digitalisation for the past 25 years, creating a powerful and

successful digital government. While the public architecture of Estonia could not be replicated in the US federal system and the technology used would be too expensive, the BTA aims to create a similar ecosystem, better fitted to the needs of the system and easily scalable. Under the auspices of the New America think-tank, the BTA develops as a form of independent Blockchain lab to promote and accompany accountable and transparent technologies – and the development of like-minded policies. More importantly, "we are at a time when people around the world are struggling to make sense of what is real and what is fake. [Blockchain] is an immensely powerful tool to give citizens confidence in the institutions in order for them to establish those core facts" (Tillemann, 2017). The permanent and distributed attributes of the technology make it a tool of reliability and factual information-sharing that fails to efficiently exist today.

137. Furthermore, the BTA seeks to best bring together what Tomicah Tillemann considers to be the four main stakeholders behind Blockchain: Governments; the tech industry; civil society; and funders (be it foundations or financial institutions). It creates a trusted ecosystem across all stakeholders and across national administrations – in the US and abroad.

4.6.3. RESULTS AND IMPACT

138. The BTA has carried a number of projects for national administration across the world, including the digitalisation of the Democratic Republic of Georgia's public land registers. As a result, the time required for a land transaction moved from days to an average of ten minutes. A number of other projects are seeing the light of day on topics of corruption and money laundering. Work is also underway to make Blockchain technology more accessible to public servants and citizens at large – and make sense of the technical complexities that the technology may involve.

4.6.4. LIMITATIONS

139. Tomicah Tillemann finds two clear hurdles in the healthy development of Blockchains in the public sector and for social causes. One is technical, and lies in safely determining the identities of users involved on Blockchain platforms. The second point is one of education, whereby not enough is made to best present the technology to all, in simple words and yet make potential impacts on citizens' daily lives clear. The education of constituencies to unleash the full power of Blockchains thus appears necessary.

4.6.5. KEY POINTS

- "There absolutely an incredible need for expertise in the public sector. What we're finding is that in most cases, it is easier to harness private sector expertise, and deploy it within the public sector, than it is to try to create native expertise within the public sector. Hopefully that will change but at the moment, the demand for Blockchain solutions is so intense, and the pool of talents is so small, that it is very difficult to keep the best developers in the public sector."

4.8. Case study 7

Name: Vehicle Wallet

Founder & CEO: The Danish Tax Administration (SKAT)

Launched: as Proof of Concept (PoC) in 2017

Where: Copenhagen, Denmark

4.8.1. THE PROBLEM

140. During its lifecycle a car undergoes various phases and activities such as MOT test, repair, loan, insurance and shift of ownership. As this often includes registrations and levies, the Danish Tax Administration (SKAT) is a frequently involved stakeholder.

141. One of the critical activities related to a car's lifecycle is the shift of private ownership when a car is traded and the ownership changes from one person to another. For this to happen, the involved parties are required to fill out an official re-registration so that SKAT knows the owner, and thus are able to collect the associated taxes.

142. When trading a car an imbalance of information appears between seller and buyer. The buyer must believe that the seller provides him or her with the correct registration certificate. This implies an inherent risk of the car being undesirably re-build, in debt or even stolen property. The seller on the other hand has to trust that the buyer re-register the car. Among other things this implies a risk of the buyer driving on levies paid by seller or further that buyer uses the car for undesirable matters, in worst case illegal matters.

4.8.2. THE SOLUTION

143. Vehicle Wallet is a joint project between the payment service provider Nets and SKAT where Blockchain-based innovation is used to co-create a PoC on registered digital asset management for handling a vehicle's life cycle process. All data concerning the car is saved in one distributed ledger and creates one agreed and shared record of the vehicle history as it is transferred across the supply chain. This means no vehicle information inconsistency, leading to increased efficiencies, improved resilience with mitigation from cybersecurity and fraud risks. At all stages security, integrity and validity of vehicle information is assured using proven cryptographic services.

144. The government regulator creates and populates the registration for the new vehicle, which is loaded onto the Blockchain. The smart contract protocol ensures that only the regulator can do this. The regulator then transfers the ownership of the vehicle to the manufacture by invoking a transaction on the Blockchain. The transaction is verified if consensus exists, i.e. if all relevant parties agree. The manufacturer adds the make, model, VIN, etc. to the vehicle template, as permitted by the smart contract. This update is visible to all members of the supply chain with the right permission. This process continues across the supply chain.

145. Transfer of a vehicle's ownership is done securely through Vehicle Wallet when seller initiate the transfer by using the VIN number of the vehicle, the receiver's personal id or VAT and the terms of transfer such as price and time of expiration. Thereby the receiver is notified in his or her own wallet and is able to upload a bank guarantee and accept the deal or decline. When receiver fulfils all terms, an "Approve-button" will

appear and sender of the vehicle can seal the deal. Hence, the vehicle will be transferred to a new owner and appear in his or her Vehicle Wallet.

4.8.3. RESULTS AND IMPACT

146. The development of a PoC concerning Vehicle Wallet is a part of a greater research project focusing on the use of Blockchain technology within the Danish Tax Administration. The PoC had several valuable outcomes:

- Hands-on experience with Blockchain technology and its benefits in order to create a clear business case concerning utilisation of Blockchain technology within the Danish Tax Administration.
- A clear demonstration of how Blockchain technology has the potential to enhance confidence and trust between seller and buyer when a car changes ownership. This is done through cryptography, consensus mechanisms, real time transactions and completely transparency of the history of the vehicle.
- Proof of how SKAT can reduce fraud concerning Vehicle Registration Certificates and other activities such as MOT test and repair through the use of Blockchain technology since uploading and authorisation of false or non-existing data will not be possible.
- From SKAT's point of view, a Blockchain solution will most likely eliminate manual processes tied to re-registration and thus minimise existing operational costs.

4.8.4. KEY POINTS

- During a one-month sprint, Vehicle Wallet was developed in a co-creation process between Nets and SKAT and included four developers and one designer. Furthermore, several relevant professionals provided the project team with input and advice.

4.9. Case Study 8

Name: Blockchain Talent Hackathon

Founder & CEO: Ministry of Public Administration and the Coordination of the National Digital Strategy through the Digital Government Unit

Launched: as a result of the pilot project of the Blockchain MX initiative and the winning idea of the Vertical Digital Government of Talent Hackathon 2017

Where: Mexico

Website:
https://www.gob.mx/cms/uploads/attachment/file/269552/Folleto_blockchain_HACKMX_oct2017_v6.pdf

4.9.1. THE PROBLEM

147. The World Economic Forum issued a recommendation to Mexico to explore the use of Blockchain technology in the Mexican government, and government officials wanted to kick-start their efforts in this area.

THE SOLUTION

148. The Ministry of Public Administration and the Coordination of the National Digital Strategy held the five-day "Talent Hackathon of Campus Party 2017". The hackathon included an exercise which consisted of a series of problems that demanded the development of technological solutions based on Blockchain technology. The winning team developed a prototype of public tenders smart contracts based on Blockchain that allows the public bidding process to be reliable, allows for citizen participation, and helps to ensure that the winner of the tendering process is the one that generates greater social benefit.

149. The evaluation criteria for the hackathon included factors such as using and promoting: open source, enhanced governance, advanced smart contracts development capacity, private Blockchain implementation, and transaction reliability.

150. As a result of the analysis, and with the help of the Blockchain Advisory Board (a group of experts that advise on the development of the initiative), it was determined that the solution that meets the necessary characteristics is the open source platform built using the Ethereum platform, a decentralised Blockchain platform capable of executing smart contracts, as discussed previously in this guide, as well as allowing the establishment of the appropriate authentication mechanisms.

4.9.2. RESULT AND IMPACTS

151. One of the actions executed in the first phase of development of a functional prototype for the public tenders Blockchain.

152. Governance of the Network model has also been developed to guarantee its structure and good use. The creation of this model is vital to establish who can be part of the network and what actions should be taken.

153. Six smart contracts, which correspond to each of the phases of the Mexico's contracting process, have been created to codify the rules of the business in a programmable language, and thus guarantee the optimal recording of the information in the different stages of the public tender.

4.9.3. KEY POINTS TO HIGHLIGHT

- The objective of the smart contracts is for the public tender process to be reliable and transparent to citizens.
- Currently, the process is in the Alpha stage of development, which will be followed by the Beta stage, where tests will be carried out with a real case study, to later arrive at a functional version of the system.

5. Appendix B: Digital signatures and public and private keys

154. The nature of a distributed system allows for two parties who have never met to transact. Further they must do so without the approval of a central authority. Public-private key cryptography (also known as asymmetric-key cryptography) is a cryptographic protocol that is used to confirm the identity of each party in a transaction, thus allowing users to both send and receive a transaction. There are two ways that public and private keys can be used to carry out a transaction:

5.1. Encrypting a Transaction

- Public keys can be made public and are often used as an address by which one can be the recipient of a transaction. A sender of a transaction can encrypt a transaction using someone else's public key, which can then only be opened by the other person using their private key.
- Private keys are secret keys that can be used by an individual to receive a transaction that was encrypted using the individual's public key.
- Digital signatures are used in somewhat of a reversed way:

5.2. Digital Signature Use and Authentication

- Private keys can also be used to encrypt a transaction that can then be opened by anyone who has the encrypting user's corresponding public key. This is considered a digital signature.
- The corresponding public key can then be used to unlock the transaction described in the previous bullet. This thereby confirms the identity of the sender (e.g., the person who encrypted the transaction with the private key) because no one else could have encrypted it.

155. Public and private keys are not unique to Blockchain technology – in fact they are a rather common protocol to secure information travelling across an unsafe environment. Visually, both keys are generally just a long string of letters and numbers.

6. Appendix C: Consensus models

156. As discussed previously, an important aspect of Blockchain technology is that a majority of nodes must review and approve the transactions in a block before the block can be verified and recorded. This way, nobody can tamper with the ledger, everyone can inspect it, and it can be trusted (OECD, 2016). This is called "reaching consensus". Another aspect of consensus is determining which mining node has the right to public the next block in the linear Blockchain. There are several models for achieving this that are appropriate for different contexts (Yaga et al, 2018), especially as related to the level of trust users of a platform have in each other.

157. Blockchain technology was initially developed under the assumption that, in general, users would not know each other and, as a result, have a mutual distrust in each other. Blockchain technology is also intended to be distributed and self-policing, which ensures a central authority is not needed and that transactions costs are kept low. Consensus models are what allow mutually distrusting users to conduct transactions among themselves and to achieve this state of self-policing (Yaga et al, 2018). However, many different applications of Blockchain technology have been developed or envisioned for the future, which have varying levels of pseudonymity and trust. This includes the concept of permissioned ledgers, where some level of trust is likely to exist.

158. The following are major Consensus Models that exist today. In practice, software handles these models automatically with no need for manual intervention (Yaga et al, 2018).

6.1. Proof of Work Consensus (PoW) Model

159. The PoW model—the most common consensus model used, including for the Bitcoin platform—requires that for a mining node to post a block to the Blockchain, they must expend processing resources in order to solve a difficult puzzle. Their accurate solution to the puzzle serves as proof that they conducted the work needed to publish the block. The process to solve the puzzle is intentionally costs money in terms of processing time and electricity, but the process to confirm that the solution is correct is intentionally very easy. (Yaga et al, 2018).

160. Once a user completes the work, they send their block to the other nodes on the network. The other notes then verify that the work has been completed and that the block and its transaction contents are valid. If so, the nodes add the block to their copy of the ledger, and distribute the block throughout the network (Yaga et al, 2018).

161. The PoW model is well suited for permissionless ledgers, which allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. Since anyone can contribute, there is a mutual distrust among users. The PoW model helps to ensure that each user has roughly the same likelihood of being able to solve the puzzle, thereby preventing certain users from being able to control which blocks are added to the chain (Yaga et al, 2018).

6.2. Proof of Stake Consensus Model

162. The Proof of Stake model is premised on the concept that users with more stake (i.e., the relative amount of cryptocurrency the user has on the platform) as the determinant the system uses for deciding which user has priority in adding new blocks to the chain. The assumption is that users with the most stake in the platform will also have a strong desire for the platform to succeed and will make decisions that are in the best interest of the platform (Yaga et al, 2018).

163. There are a number of ways of practically implementing Proof of Stake. Some methods include randomly choosing users proportionate to their level of currency in the platform, voting, and "coin aging" where users with older cryptocurrency are given priority over those with newer money. With coin aging, once a user created a block, the age of their currency resets to "0" to help prevent some users from gaining too much decision making power (Yaga et al, 2018).

164. Like the PoW model, proof of stake is well suited for environments where there are high levels of mutual distrust, such as in permissionless ledgers. Unlike PoW, intensive processing resources are not needed.

6.3. Proof of Authority Consensus Model

165. Proof of Authority provides the ability to validate and publish new blocks to the Blockchain for authorised users, called *validators*. Unlike consensus models like Proof of Work and Proof of Stake, a user's identity must be known and verified. This is critical, as identity is the sole verification of a user's authority to add new blocks to the chain. When compared with Proof of Work, Proof of Authority is a much faster model for processing new blocks, as there is no need for lengthy and resource intensive computer processing (POA Network, 2017). Proof of Authority could be used in both permissionless and permissioned ledgers. The logic with this model is, "Individuals whose identity (and reputation by extension) is at stake for the securing of a network are incentivised to preserve the network" (POA Network, 2017).

166. This consensus model may seem the most familiar to users who have experience working with databases in which only specific authorised users may edit or add data to a database. Thus, it may be the most applicable for many applications of Blockchain technologies in the public sector, as it can be adapted to represent the complexity of government review and decision-making processes (Marchionni, 2017).

6.4. Round Robin Consensus Model

167. When some level of trust exists among users, such as on permissioned ledgers of known users, concerns related to potential tampering or subversion are lessened. In such systems, a Round Robin approach, where users take turns or are randomly selected to publish blocks, may be appropriate.

168. Unlike other models, Round Robin would not work in permissionless ledgers and can only function well in permissioned Blockchains. It is perhaps the combination of permissioned ledgers applying a Round Robin consensus model that is the most applicable for use in the public sector. In such a construct, access to view the transactions in a Blockchain could remain public while the ability to create new transactions and blocks is reserved for authorised users.

7. References

Interviews

- Herman, Justin, 16 August 2017
- Lemaire, Axelle, 11 August 2017
- Noah, Emmanuel, 2 August 2017
- Raford, Noah, 21 August 2017
- Rinearson, Tess, 6 September 2017
- Segendorf, Björn, 8 August 2017
- Tillemann, Tomicah, 29 August 2017
- Mats Snäll, 24 August 2017
- Yong, Stanley, 10 August 2017

Bibliography

1. ACT-IAC, 2017, "Enabling Blockchain Innovation in the U.S. Federal Government: A Blockchain Primer", Online, last accessed 6 April 2018, https://www.actiac.org/system/files/ACT-IAC%20ENABLING%20BLOCKCHAIN%20INNOVATION_3.pdf

2. Atzori, Marcella, 2015, "Blockchain Technology and Decentralised Governance: Is the State Still Necessary?", SSRN e-Library, Online, last accessed 30 August 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

3. Baran, Paul, 1964, "On Distributed Communications: Introduction to Distributed Communications Networks", United States Air Force Project Rand, pp.1-2

4. Barr, Dan; Fedesova, Kate; Filipova, Mariya; Housman, Dan; Israel, Adam; Killmeyer, Jason, Krawiec, RJ, Nesbitt, Allen; Quarre, Florian; Tsai, Lindsay; White, Mark, 2016, "Blockchain: Opportunities for Healthcare", Deloitte

5. Brandon, Guy, 2017, "Can the Blockchain Scale?", Due, Online, last accessed 30 August 2017, https://due.com/blog/can-the-blockchain-scale/

6. "Bitcoin Energy Consumption Index", 2017, Digiconomist, Online, last accessed 30 August 2017, https://digiconomist.net/bitcoin-energy-consumption

7. "Bitcoins in circulation", 2017, Bitcoin.info, Online, last accessed 24 August 2017, https://blockchain.info/charts/total-bitcoins?timespan=all

8. Buterin, Vitalik, 2015, "Visions, Part 1: The Value of Blockchain Technology", Ethereum Blog, Online, last accessed 23 August 2017, https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

9. Cheng, Steve; Daub, Matthias; Domeyer, Axel; Lundqvist, Martin, 2017, "Using Blockchain to Improve Data Management in the Public Sector", Digital McKinsey, McKinsey & Company, Online, last accessed 25 August 2017, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

10. Dalal, Darshini; Yong, Stanley; and Lewis, Antony, 2017, "The Future is here – Project Ubin: SGD on Distributed Ledger", Monetary Authority of Singapore & Deloitte

11. David, Torben, forthcoming, "Distributed Ledger Technology: Leveraging the Blockchain for ESA", European Space Agency

12. Deane-Johns, Simon & McLean Sue, 2016, "Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero?", Morrison & Foerster LLP, pp.1-8

13. De Filippi, Primavera (2017), "The Interplay Between Decentralisation and Privacy: the case of Blockchain technologies", Journal of Peer Production, Alternative Internets 7

14. Deshpande, Advait; Gunashekar, Salil; Lepetit, Louise; Stewart, Katherine (2016), Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospect for Standards

15. The Economist (2015), "The trust machine: The technology behind bitcoin could transform how the economy works", The Economist, 31 October 2015. https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

16. Farell, Ryan, 2015, "An Analysis of the Cryptocurrency Industry", Wharton Research Scholars, 130

17. Foroglou, G., and Tsilidou, A. L. (2015). "Further applications of the blockchain", *In 12th Student Conference on Managerial Science and Technology*

18. Gabison, Garry, 2016, "Policy Considerations for the Blockchain Technology Public and Private Applications", Bepress, European Commission

19. "Global Blockchain Council", 2017, Dubai Future Foundation, Online, last accessed 24 August 2017, http://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/

20. Guillou, Louis & Quisquater, Jean-Jacques, 1998, "How to Explain Zero-Knowledge Protocols to Your Children", Advances in Crytpology – CRYPTO 1989: Proceedings, vol. 435, pp.628-631

21. Hanson RT, Reeson A, Staples M, 2017, "Distributed Ledgers: Scenairos for the Australian Economy Over the Coming Decades", Commonwealth Scientific and Industrial Research Organisation, Camberra

22. Hartung, Adam, 2017, "A Bitcoin Is Worth $4,000—Why You Probably Should Not Own One", Forbes Online, Online, last accessed 23 August 2017,

https://www.forbes.com/sites/adamhartung/2017/08/15/a-bitcoin-is-worth-4000-why-you-probably-should-not-own-one/#2b8dc5843b08

23. Hutt, Rosamond, 2016, "All you need to know about blockchain, explained simply", World Economic Forum, Online, last accessed 11 April 2018,

https://www.weforum.org/agenda/2016/06/blockchain-explained-simply

24. Kasireddy, Preethi, 2017, "Blockchains don't scale. Not today, at least. But there's hope", Medium, Online, last accessed 30 August 2017, https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

25. Mamoria, Mohit, 2017, "The ultimate 3500-word guide in plain English to understand Blockchain", LinkedIn blog, Online, last accessed 23 August 2017, https://www.linkedin.com/pulse/blockchain-absolute-beginners-mohit-mamoria

26. Marchionni, Pietro, 2018, "The Next Generation e-government", Online, last accessed 9 April 2018, https://www.linkedin.com/pulse/next-generation-e-government-pietro-marchionni/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_post_details%3BXf7wGwZzRtaDNp95WZkzZg%3D%3D

27. Marshall, Johnathon, 2017, "Estonia Prescribes Blockchain for Helathcare Data Security", PWC blog, Online, last accessed 23 August 2017, http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html

28. Nakamoto, Satoshi, 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System", www.bitcoin.org, Online, last accessed 25 July 2017, https://bitcoin.org/bitcoin.pdf

29. Nathan, Oz; Pentland, Alex; Zyskind, Guy, 2015, "Decentralising Privacy: Using Blockchain to Protect Personal Data", IEEE Security and Privacy Workshops

30. OECD, 2016, "OECD Science, Technology and Innovation Outlook 2016", OECD Publishing, Paris

31. OECD, 2017, "Embracing Innovation in Government: Global Trends", OECD Publishing, Paris

32. Ølnes, Svein, 2015, "Beyond Bitcoin – Public Sector Innovation Using the Bitcoin Blockchain Technology", International Conference on Electronic Government and the Information Systems Perspective, Springer, pp.253-264

33. "Ordonnance n.2016-520 du 28 avril 2016 relative aux bons de caisse", 2016, Journal Officiel, 29 avril 2016, texte n.16

34. Patrick, Gabrielle, 2016, "Europe's Regulatory Blockchain Shift on Display at Private Parliament Event", CoinDesk, Online, last accessed 23 August 2017, https://www.coindesk.com/the-eu-regulatory-blockchain-shift/

35. "Police Need Power to Tackle Virtual Money Laundering: Europol", 2014, Reuters, Online, last accessed 30 August 2017, http://www.reuters.com/article/us-bitcoin-europol-money-laundering-idUSBREA2N1A420140324

36. Rinearson, Tess, 2017a, "Making Money: Bitcoin Explained (with Emoji), Part 1", Medium, Online, last accessed 23 August 2017, https://medium.com/@tessr/making-money-530d2bb2b8f7

37. POA Network, 2018, 'Proof of Authority: consensus model with Identity at Stake", Medium, Online, last accessed 9 April 2018, https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

38. Ray, Shaan, 2017, "Blockchains versus Traditional Databases", Online, last accessed 7 May 2018, https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79

39. Rinearson, Tess, 2017b, 'Making Money Trustworthy: Bitcoin Explained (with Emoji), Part 2", Medium, Online, last accessed 23 August 2017, https://medium.com/@tessr/making-money-trustworthy-6c552a1cfc25

40. Rosenfeld, E. and E. Cheng (2017), "Bitcoin sees sudden, sharp spike after smashing through $10,000", CNBC, 29 November 2017, www.cnbc.com/2017/11/29/bitcoin-sees-sudden-sharpspike-after-smashing-through-10000.html.

41. Rosic, Ameer, 2017, "Blockchain Scalability: When, Where, How?", Online, last accessed 7 May 2018, https://blockgeeks.com/guides/blockchain-scalability/

42. Rosic, Ameer, 2016, "Is Blockchain technology the new internet? A step-by-step guide for beginners", Online, last accessed 23 March 2018, https://blockgeeks.com/guides/what-is-blockchain-technology/

43. Snäll, Mats, "Blockchain and the Land Register – A New 'Trust Machine'?", n.d., Submission n.572

44. Stawinska, Karolina, 2017, "Meet 10 Millenial Entrepreneurs Who Are Rethinking Industries", Medium, Online, last accessed 24 August 2017, https://medium.com/swlh/meet-10-millennial-entrepreneurs-who-are-rethinking-industries-5f064cd37343

45. "The promise of the Blockchain: The trust machine", 2015, The Economist, Online, last accessed 23 August 2017, https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

46. "The Social Smart Contract: An Open Source White Paper", 2017, Democracy Earth Foundation, Online, last accessed 31 August 2017, https://github.com/DemocracyEarth/paper.

47. UK Government Office for Science, 2016, "Distributed Ledger Technology: beyond block chain", Online, last accessed 13 June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

48. UK House of Lords, 2017, "Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation", Online, last accessed 13 June 2018, http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf

49. Van Humbeeck, 2018, "The Blockchain-GDPR Paradox", Online, last accessed 13 June 2018, https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

50. Walport, Mark, 2016, "Distributed Ledger Technology: Beyond Block chain. A Report by the UK Government Chief Scientific Advisor", UK Government

51. Webb, Steve, 2016, "Why Central Banks Are Getting Serious About Blockchain", Medium, Online, last accessed 25 August 2017,

https://medium.com/@InnFin/why-central-banks-are-getting-serious-about-blockchain-19b695095e98

52. Willms, Jessis, 2016, "Is Blockchain-Powered Copyright Protection Possible?", Bitcoin Magazine, Online, last accessed 30 August 2017, https://bitcoinmagazine.com/articles/is-blockchain-powered-copyright-protection-possible-1470758430/

53. Willms, Jessis, 2016, "Is Blockchain-Powered Copyright Protection Possible?", Bitcoin Magazine, Online, last accessed 30 August 2017, https://bitcoinmagazine.com/articles/is-blockchain-powered-copyright-protection-possible-1470758430/

54. Yaga, Dylan; Mell, Peter; Roby, Nik; and Scarfone, Karen, 2018, "Blockchain Technology Overview", United States National Institute of Standards and Technology (NIST), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf