BLOCKCHAINS UNCHAINED: The Implications of Blockchain Technologies for the Public Sector

Draft Working Paper

Observatory of Public Sector Innovation

Reform of the Public Sector Division (RPS)

Directorate for Public Governance (GOV)

OECD

26 February 2018

Prepared by Théo Bourgery, Intern, opsi@oecd.org

This draft paper is shared online on the OPSI blog (http://oe.cd/opsi-blog) for public comments from 26 February 2018 through at the 20 March 2018. Interested individuals are are invited to REVIEW and COMMENT on the paper by 13 March 2018 through the collaborative document at http://oe.cd/blockchainunchained or by editing the document in tracked changes and emailing revisions to opsi@oecd.org.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Table of Contents

Table of Contents 2

Foreword 3

Acknowledgements 5

Executive Summary 6

Introduction 8

What blockchains actually mean: Concepts behind blockchain technologies 12

Applications of blockchains in the public sector: Case studies 19

Blockchain technologies an governments: challenges 35

Conclusions and a way forward 39

Appendices 42

References 54

Foreword

At the OECD Observatory of Public Sector Innovation (OPSI) we aim to make sense of innovation trends across government administrations. We shine a light on the work of agencies and public servants to create more efficient, effective and tailored public service delivery. At the same time, we accompany teams and departments in exploring and implementing all forms of innovative processes: emerging and disruptive technologies, big data analytics and open data, innovation skills, citizen-driven policies and services, innovative procurement and human resource management, among others. All in all, we seek to understand the dynamics of innovation to create and fuel systemic change in the public sector.

OPSI has published an annual series of reports on global public sector innovation trends. The *Embracing Innovation in Government: Global Trends* reports[1] are the results of extensive research into the field of innovation and global Call for Innovations crowdsourcing exercises that have surfaced over 400 compelling innovation initiatives – stemming from a wide range of administrations, agencies and issues to resolve. Through analysing this large number of case studies, these reports identified key trends that will shape the public service of tomorrow. In both reports, we saw innovative uses of blockchain for the public good. In particular, our 2018 trends report identified the public-private ID2020 partnership, which demonstrates the potential for blockchain 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 blockchain 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]

This increasing interest and questions surround in the government application of blockchains is OPSI's motivation for developing this new *Blockchains Unchained* guide. Further, we intend for this guide to be the first in a series of straight-forward, easily accessible guides that leverage our Call for Innovations and our *Global Trends* work to do deep-dives into

[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.

specific topics of interest bubbling to the surface in the public sector, including emerging technologies.

Acknowledgements

We would like to deeply thank Justin Herman, Axelle Lemaire, Emmanuel Noah, Noah Raford, Tess Rinearson, Björn Segendorff, Tomicah Tillemann, Mats Snäll and Stanley Yong for taking the time to answer the questions of the Observatory. From Blockchains specialists to entrepreneurs and regulators, their interventions were key in insuring the quality of this report.

A special thank goes to Rodrigo Mejia Ricart, formerly of the OECD’s Digital Government Team, who supported the project from day one, and Matthieu Crepy, for his technical revision of Part I of this report.

Executive Summary

Blockchains have become a *buzz* word, yet ambiguity remains around what they truly are. Their impact on the public sector is at best misunderstood, most often ignored. Technical complexity skews public debate. As current security processes predominantly involve governments or banks as only trusted third-parties to certify transactions or official multi-party interactions, questions over the vulnerability of such single points of failure arise. Blockchains may offset some of government's existing worries and issues. This guide aims to provide public servants with the necessary tools to understand what the Blockchain architecture is, the impacts it could have on government services, and challenges governments will face as a result.

Section I defines the Blockchain architecture as a distributed data store that acts as an open, shared and trusted public ledger that nobody can tamper with and that everyone can inspect (OECD, 2016, p.107). For the sake of clarity, this section looks at the technology from the angle of financial transactions. Blockchains' underpinning assumption is that all transaction will be visible to all actors in the system – citizens – at all times. In other words, all actors will hold identical 'ledgers' of transactions. This enables a key feature of the Blockchain architecture: omniscient actors are in turn expected to confirm the validity of transactions that occur on the platform, and flag inappropriate dealings when necessary. This state of perfect information in turn responds to two security queries:

- Is the correct information, or fund, being transmitted?
- Are the identities of the two transacting parties involved valid?

Then comes security. One must imagine a Blockchain as, quite literally, a chain of blocks in which specific transactions are stored. Once transactions are agreed upon by actors, they are stored in blocks which cryptography and complex mathematical constructions secure. Due to its chain-like architecture, blocks are fundamentally dependent on one another, such that changing the information of one ultimately changes the link it has with all other blocks on the chain. The inherent chained structure ensures that the information contained in the ledger is not tampered with, so that transactions are inherently trusted.

Interestingly, this further suggests that banks and governments would no longer be required as trusted third-parties. This is the real value of Blockchains: the development and growth of automated and decentralized decision-making systems that do not require centralized bodies or datasets.

While Blockchain technologies have so far most often been applied to the financial sector, and specifically deal with monetary transactions, this powerful data storing technology could also be used for non-monetary matters. E-identification, proof of land ownership, digital signatures, even voting, are only a fraction of the disruptive impacts Blockchains could have on the public sector. Section II provides the reader with a number of different case studies of Blockchain uses in the public sector – from across the world, and across a variety of departments and agencies. It takes Blockchains out of the world of technical complexity into the real world.

Section III focuses on the challenges that this technology poses, and is expected to pose, to public administrations. These take many shapes and forms, be it over matters of data protection, governance and confidentiality of information. The format that some Blockchains take today have in-built limitations, be it the outrageously high levels of energy required to power the system, as well as the slow pace of transactions processes. Coding constraints also add to the complexity of governance mechanisms. These challenges must be understood quickly by public servants, public officials and regulators as Blockchains expand out of the private sphere into the public sector.

The Observatory aims to accompany public decision-makers in understanding the technology and the associated opportunities in order to help them make better-informed decisions when the time comes. It is not enough to delegate to developers because "only they know". As technical as it first may appear, it is important that policy-makers grasp the topic and its implications. This is what this guide aims to do.

Introduction

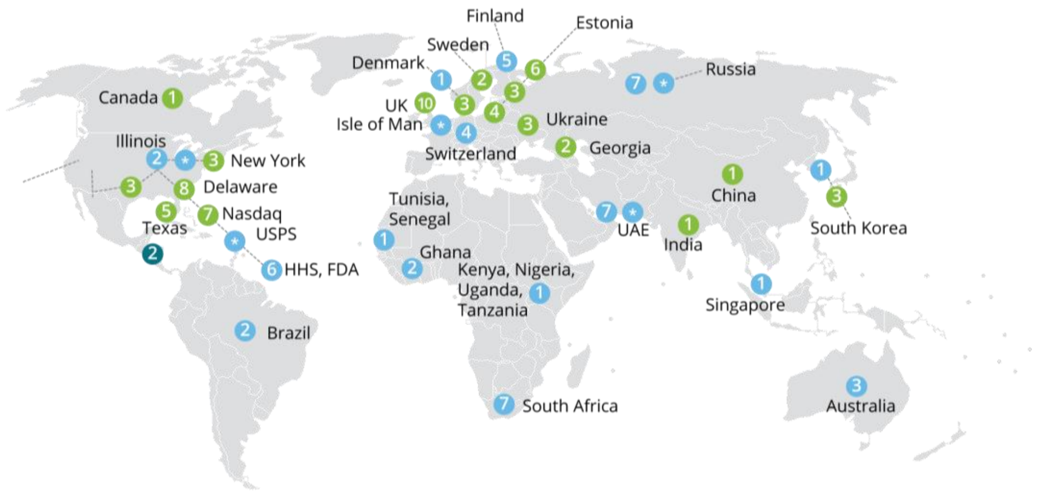
Blockchain today

Blockchain technologies are for many as revolutionary an invention as the rise of the Internet ("Is Blockchain Technology the New Internet", n.d.) or, more soberly, a new "trust machine" (Snäll, n.d.). While their developments have been extensive in the financial services industry[5], the use of Blockchains is also emerging in many sectors of the public sphere (see Figure 1). Estonia has implemented the first nationwide Blockchain system to safeguard data such as health records (Marshall, 2017). Sweden is experimenting with Blockchains for its land registry management (Snäll, n.d.) – while BenBen, a Ghanian start-up, has partnered with the Ghanian Land Commission to develop secure land transaction recordings and improve Government's public service delivery (Stawinska, 2017). Communities of practices at different levels of government are emerging, such as with the General Services Administration's Emerging Citizen Technology program for US federal government agencies (GSA, 2017), and the Global Blockchain Council powered by the Dubai Future Foundation (Dubai Future Foundation, 2017). Public financial institutions such as Central Banks are also looking at the opportunities of Blockchain technologies to develop and secure digital currencies, at a time when debates over cashless economies expand (Segendorf, 2017).

[5] See Dalal *et al*, 2017 and the 'Project Ubin' case study *infra*

Figure: Blockchain in the public sector, as of March 2017

Blockchain experiments in the public sector are accelerating globally, with a concentration in the US and Europe.



Top 10 most active public sector use cases*

1. Digital currency/payments
2. Land registration
3. Voting (elections)
4. Identity management
5. Supply chain traceability
6. Health care
7. Voting (proxy)
8. Corporate registration
9. Taxation
10. Entitlements management

* Measured by observing the number of public sector blockchain experiments planned, in progress, or stalled globally

Color coding key

● In progress
● Planned
● Announced

Source: Deloitte analysis in conjunction with the Fletcher School at Tufts University.

Deloitte University Press | dupress.deloitte.com

In more general terms, “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, p.1). They are essentially a form of *distributed ledgers technologies*, which translate as a data store “that is 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]” (Walport, 2016, p.17). 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 SMEs (*ibid.*, p.65).

While Blockchain technologies act as systems of information storing and allow for highly secured transactions, they inevitably rely on a number of platforms to develop[6]. The most

[6] Please refer to the “Blockchain as a platform?” section for more information

(in)famous of these platforms is *Bitcoin* – with a cryptocurrency of the same name – which has seen its use and operability increase massively in the last few years. The value of Bitcoin has attained record-breaking values in recent months, reaching a peak value of nearly USD 20 000 per bitcoin and a total value of 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 take place on the Bitcoin platform[7] – as opposed to an average of 105 million over other 'conventional' means.

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" (Farell, 2015, p.2).

Finally, more is done across government institutions to best present and introduce Blockchains to policy-makers. While the current work on Blockchains in Government remains fundamentally "pre-legal" (Raford, 2017), efforts have been made to make senior public servants aware of the technology and its impacts. The organisation of a roundtable on Blockchains and cryptocurrencies at the EU parliament for MEPs in April 2016 (Patrick, 2016); the first *Forum Parlementaire de la Blockchain* for French MPs in October 2016; and the recognition of Blockchain as a legal construction by the French Ministry of the Economy for specific private equity transactions (Ordonnance n. 2016-520, 2016) are indications that policy makers are trying to keep up to date with the technology.

Misunderstanding and Oncoming Challenges

Despite what seem to be promising advances, Blockchains are still misunderstood technologies to citizens at large. Many factors may account for this lack of clarity, and scepticism, around the Blockchain architecture.

Blockchain technologies are often introduced in all their technical complexity. Distributed and decentralised ledgers, hashing, mining, securing blocks through consensus mechanisms,

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

and the development of Smart contracts are blurry and messy concepts. The very code in which Blockchains are embedded also raises important questions: who codes? What do algorithms allow for, and what do they prevent from happening? How do democratic governance mechanisms fit into the 'DNA' of Blockchains? Only a fraction of the existing literature (which still rests in its majority in open-sourced blog posts) aims to make sense of the technology in accessible ways[8], and far fewer focus on its applicability to the public sector[9].

Furthermore, Blockchains are often linked to the scandals of the Bitcoin platform, and the types of goods and services it gives easier access to than before – drugs, pornography, weapons, etc. [10]. The general misunderstandings of the technology, along with an out-of-legal-boundaries view attached to it, make it easy prey for tech sceptics. Yet, while Blockchains have flaws that should not be ignored, and from a public policy standpoint need to be taken into account, they are also *much more* than Bitcoin. This guide will spend time explaining ways in which Blockchains can move from a tool prone to defiance, to a true political and administrative bargain.

The goal of this guide is thus to provide some clarity and objectivity in the analysis of Blockchain technologies. The technicalities of Blockchains, their applications to the public sector and the challenges it poses as a result will be covered. The following questions will be tackled:

- What does it mean to run a Blockchain-based transaction?
- How can one ensure, and measure, the integrity and security of Blockchains?
- Is confidential information *really* confidential?
- Are there specific examples of Blockchain being applied in the public sector?
- Where would Blockchain technology be most useful in the public sector – if at all?
- Can personal data be protected?
- What can we expect as the next big steps in the development of the technology – and how can public servants get involved in such developments?

All in all, the guide aims to:

- *Explain* what Blockchain is;
- *Explore* what is already occurring in the Blockchain space for the public sector;
- *Make sense* of its impacts on the public sector, and *anticipate* future developments.

[8] See for example Rinearson, 2017a and 2017b, and Mamoria, 2017
[9] See Cheng *et al*, 2017 and Ølnes, 2015
[10] See "The promise of the Blockchain: The Trust Machine", The Economist

What blockchains actually mean: Concepts behind blockchain technologies

Current problems

It is crucial to understand what the problems are *now* with regards to data management and secured transactions, and the relevant solutions Blockchains can bring forth. The next subsection looks at two specific existing issues, in the form of analogies:

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

The e-mail analogy

The *status quo*: It is a common process to share documents among peers and colleagues through the use of e-mails. This translates 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.

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 blurs: which document becomes the correct one? Which one must be relied upon to 'state the truth'?

The bank analogy

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

- It is indeed the sender, 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 we aim for, and not someone else.

In other words, we expect the bank to confirm the feasibility of the transaction; and *only banks* can run such confirmation for matters of security. In this content, the bank acts as the only trusted third party.

The issue: This single ledger held by the bank *and the bank only* ultimately creates 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 (see 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 distributed 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).

Thus two issues must be resolved:

i. Data management, and history, must become completely immutable, and;

j. 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.

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 actors with whom no prior transacting relationship was established.

Blockchains Introduced

Blockchains, and more largely distributed ledgers, can respond adequately to issues of trust and data protection. This next section looks at the specific attributes of the new technology in the most accessible way possible. For the sake of clarity, the example of a monetary transaction will be used.

A point of clarification: distinguishing blockchain platforms from blockchain technologies

Blockchains are technologies with specific, and rather unique, attributes. Such technologies are then applied to specific platforms. Hundreds of these platforms have seen the light of day since the creation of Blockchains and the *Bitcoin* platform[11] - the first one to have existed.

[11] See the original paper by Nakamoto, 2008.

Many of them enable secured transactions through their own virtual ‘cryptocurrencies’.

The Most Important Features of Blockchain Technologies

The OECD (2016, p.107) provides the most basic definition of Blockchain technologies as a distributed data store that acts as an open, shared and trusted public ledger that nobody can tamper with and that everyone can inspect.

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

Blockchains by nature ensure perfect transparency over:

- All actors’ – known as nodes; they can be citizens signed up to any platform;
- All validated transactions on the platform;
- Consequentially, all nodes in the system have information about all parties’ willingness and ability to pay and carry out transactions.

Once a transaction is requested between two parties, it is broadcasted to all nodes, whose responsibility it is to process the request and approve/disprove it through computational means. 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 agencies nowadays. The trust effectively shifts from the centralised authority to the actors of the system. Levels of checks and balances, along with security levels to protect both transactions and the confidentiality of nodes, are so advanced that they are inherently trustworthy. Centralised authorities become essentially irrelevant in the context of Blockchain technologies. A specific discussion of security protocols can be read in Appendix A.

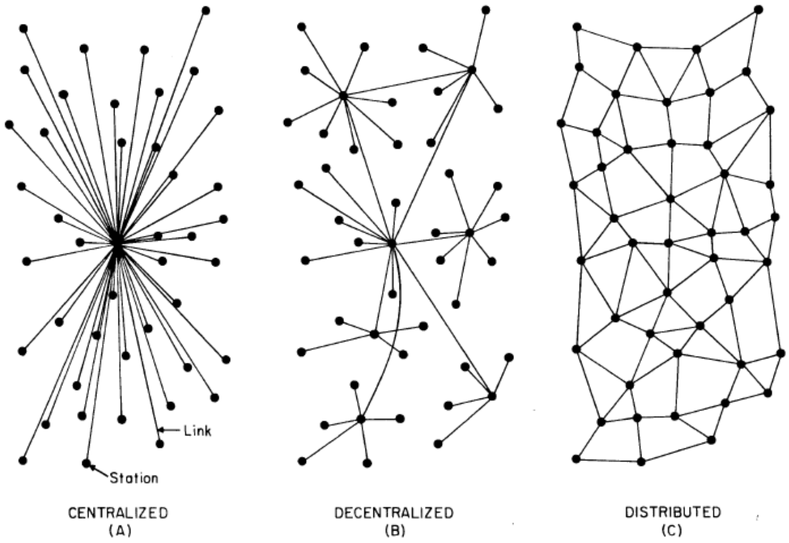


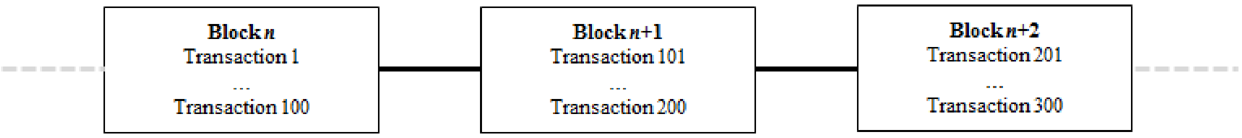
Fig. 2: Centralised, decentralised and distributed networks (Baran,

The only way in which a contradictory decision could see the light of day is if a majority of actors actively collaborate against a specific transaction. Due to the highly distributed model on which Blockchains are built, and the anonymity of actors across the globe, it becomes particularly hard for a contradictory consensus to be reached. The probability that this happens falls as the number of actors increases on the platform.

Blockchains: Chains of Blocks

Blockchain technology, as the name suggests, is a mere chain of blocks, each containing a unique set of transactions. They essentially insulate a set number of validated transactions from the rest of the system, in such a way that the information remains accessible but cannot be tampered with. However, blocks are not independent of one another. Quite the contrary, all blocks are intrinsically related insofar as they are the continuation of one another – hence the concept of a chain.

Figure: Blockchain – a chain of blocks



The creation of blocks requires mathematical processes called *hashing* (see Appendix B for technical details). Hashing is a cryptographic solution that generates a unique code to interconnect blocks together and make them almost-perfectly immutable through digital fingerprints and padlocks called hashes.[12] Each block includes its own unique hash code, as well as the hash code for the previous block. This links the blocks together to form a chain. If anyone tried to alter the contents of one of the blocks, it would result in a change of the unique hash code, which would be easily discoverable to the entire network.

Cryptography

Cryptography involves complex mathematical protocols that ensure security over the sharing of information across two parties and prevent third parties from getting involved.

Blocks are not added to the chain automatically. Once submitted by a node (i.e., a user), blocks wait in a queue until they are added to the chain through a process called "mining" (see Appendix C for technical details). Mining is a validations exercise conducted by mining nodes. Mining nodes do extra work to validate that the transaction was cryptographically signed (through the use of a private key) by the sender. If mining nodes reach consensus that validation is successful, the nodes publish the block to the chain. The mining nodes not accept a block if it contains any invalid transactions (Yaga *et al*, 2018). In some blockchain systems like Bitcoin, these mining nodes are compensated financially for doing this work.

Permissioned and Unpermissioned Ledgers

While Bitcoin is a public network, to which all can have access, other Blockchain platforms can take the form of private networks, which only allow co-opted nodes in. This draws an important distinction between *permissioned* and *unpermissioned* ledgers. Unpermissioned 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, p.17). Permissioned ledgers, on the other hand, limits access to specific.

Figure: General permissioned status of example cryptocurrencies

[12] A hash is a mathematical padlock that applies to a specific block to ensure that it cannot be falsified.

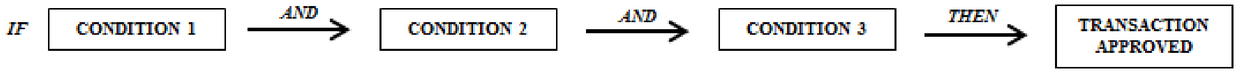
UNPERMISSIONED / PUBLIC	BITCOIN ETHEREUM MONERO DASH LITECOIN
PERMISSIONED / PRIVATE	MONAX MULTICHAIN

The exact same logic 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, actors 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; actors within that space are trusted by essence; and the space's integrity is ensured only by co-opted actors.

Smart Contracts

Smart contracts take transactions protocols to a new level: they enable transactions that follow several preceding logical steps, such that "if *x* then *y*":

Figure: The logic behind smart contracts



They are in some ways the digital representation of legal contracts, whereby a series of necessary and binding steps must be taken before the outcome is reached, or the contract ends,[13] with the notable exception that unlike legal contracts, smart contracts cannot be stopped once executes. The most developed platform today for smart contracts is *Ethereum* – one on which inter-bank payments and e-identification mechanisms are currently being tested.

[13] The complexity of such logical construction can be replicated on specific Blockchain platforms with *Ethereum* as the most advanced one today.

In the context of the public sector, we can imagine smart contracts to determine and govern times at which social aid would be granted, and conditions under which it must continue or stop; taxation payments as conditioned on pay remittances etc. The logical steps that today apply to our relationship with the State would be automatized. Permissioned ledgers and controlled access to data would respond adequately to issues of confidentiality.

Conclusions

Blockchains are immense, hypersecured data stores where decision-making is distributed, transparent and accessible to all. When two parties wish to make a transaction, they broadcast their request across the network. All nodes then verify and confirm the request, before funds are transferred. Smart contracts are an advanced way to confirm a transaction under specific conditions specified in advance. To enhance data security, a distinction is made between unpermissioned ledgers – accessible to all – and permissioned ones – co-opted nodes only. This creates safety silos around sets of information and sensitive data, such that only authorised persons can have access to it and amend when necessary.

At a time where governments integrate cost-effectiveness as a key signal for sound policy-making, while responding to the call for more transparency and accountability, Blockchains could provide viable solutions over the long-run. It is not sure where the technology will go, and what will be made of it by public and private actors. Assuming that there is a critical mass to ensure security and efficiency, it is not sure at what level it stands and whether it will ever be reached. In spite of these unknowns, Blockchain technologies have a potential to develop public service delivery and internal government strategies radically. While the State will no longer – or at least on specific issues – be the centralising authority, it will provide the legitimacy and credibility for such new technology to be trusted.

Different uses of the Blockchain in the public sector will be exemplified and contextualised in the next section. Part II is a far-from-exhaustive collections of initiatives, experimentations and running Blockchain-powered government projects from across the World. From there this report will seek to summarise the key advantages and limitations to Blockchain in, and for, the public sector.

Applications of blockchains in the public sector: Case studies

This list of case studies presented below offers a non-exhaustive view of what currently happens with Blockchains in the public sector. This is only a small fraction of a large number of innovations that are sprouting every day across the world to make Blockchains more understandable and pertinent technologies. Consortiums of stakeholders – from both public and private spheres – create their own platforms, tailored to the needs of their members. Smart contracts are developing and making e-identification, provision of social services and aid, but also inter-bank payments over Blockchains, a reality. Issues as complex as voting and decentralised democratic institutions through new technologies are now being discussed and their possible implementation evaluated. There seems to be a growing understanding across senior public officials that Blockchains can turn from a technological hassle to a safe political bargain. Countries prone to earthquakes, wars or corruption are seeing the importance of the technology to secure information in spite of dangerous unknowns. Democracies could use Blockchains to separate the truth from the fiction.

Case study 1

Name: BenBen

Founder & CEO: Emmanuel Buetey Noah

Launched: 2015

Where: Accra, Ghana

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

THE PROBLEM

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

- Determining the legal existence of parcels, and subsequent land ownership titles seem to be running 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.

THE SOLUTION

BenBen provides an *Ethereum*-run data store of all land registries across Ghana. It is able to certify land information through the cross-cutting 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, the latter *by essence* uses 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.

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.

RESULTS AND IMPACTS

BenBen uses three key metrics to evaluate its impacts and successes: the number of digitalised records, and 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 data store – with a fraction of that 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.

KEY POINTS TO HIGHLIGHT

- 70% of court disputes in Ghanaian national courts are land-related
- Average time to receive to confirm land entitlement: 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: one month. This has been reduced to a minimum of 3 days with BenBen's services

Case study 2

Name: Global Blockchain Council

Organisation: Dubai Future Foundation

Project lead: Noah Raford, COO

Launched: 2016

Where: Dubai, UAE

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

THE PROBLEM

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.

THE SOLUTION

The development of a large, multi stakeholders 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.

RESULTS AND IMPACTS

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 seen the light of day, 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 strategy, has prepared 14,000 public servants to data science and technological literacy.

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 more developed countries, he claims that the Global Blockchain Council redefines the landscape of possibility *vis-à-vis* emerging technologies. It sets goals other national administrations can tend towards and perceive as tangible reality.

KEY POINTS TO HIGHLIGHT

- 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."

Case study 3

Name: Intragovernmental Emerging Citizen Technology Program

Organisation: General Services Administration (GSA)

Lead: Justin Herman

Launched: 2017

Where: USA

Website: https://www.gsa.gov/portal/category/101958

THE PROBLEM

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.

THE SOLUTION

After a pilot consultation on Artificial Intelligence (AI), the GSA's Emerging Citizen Technology Programme aims to consult, gather and make sense of agencies' experience with Blockchain 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 digestable ways. Whenever possible it encourages the input of private start-ups and companies to develop a striving eco-system between public and private sectors. Finally, it adopts the long-run aim to change the narrative surrounding Blockchain technology to dissociate it from the mistrusted Bitcoin platform.

RESULTS AND IMPACTS

Following a successful forum in July 2017, the emerging citizen technology program 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.

LIMITATIONS AND THINKING AHEAD

There is still some form of misunderstanding between Blockchain technology and the scandals of the Bitcoin platform in the general public. More must be done to change the narrative over Blockchain in the public sector and thus instill 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 may not be well-fitted to target specific problems an agency may be experiencing. An analysis of other emerging trends and technologies remains crucial.

POINTS AND QUOTES TO HIGHLIGHT

- One hundred 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 tracable. Right now it’s open – and that’s fantastic – but it does not mean it’s real.”

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

THE PROBLEM

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 Blockchain could serve the purpose of more efficient, cheaper and faster inter-bank payments for cross-border monetary and government securities transactions.

THE SOLUTION

The 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 Singaporian 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.

The prototype uses the *Ethereum* platform to make best use of smart contracts. Furthermore, it makes full use of the MAS MEPS+, a Singaporian-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.

RESULT AND IMPACTS

By the end of Phase 1 in December 2016, Project Ubin demonstrated that a working interbank transfer protoype 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.

LIMITATIONS AND THINKING AHEAD

Due to the very nature of financial transactions, some levels of privacy is required to protect transactional actors. There is a crucial need to develop some types of privacy settings within a system – Blockchain – 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 – e.g. zero-knowledge proofs – that exist, at this point in time, as mere prototypes and beta versions[14].

POINTS TO HIGHLIGHT

- Due to the required checks and balances, cross-border transactions occur on an average of two hours every day, with constant participation of banks. Such figure will 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 Blockchain 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.”

[14] Please see Appendix ## for a technical overview of zero-knowledge proofs

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

THE PROBLEM

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.

THE SOLUTION

Granted that Blockchain 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.).

The project is split in three phases. Phase 1 developed a theoretical understanding of i/ what Blockchain is and how it works, and ii/ 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*.

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).

RESULTS AND IMPACTS

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

LIMITATIONS

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

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

KEY POINTS TO HIGHLIGHT

- “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”

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/

THE PROBLEM

The founding organisations made sense of 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.

THE SOLUTION

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 e-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.

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.

RESULTS AND IMPACTS

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.

LIMITATIONS

Tomicah Tillemann finds two clear hurdles in the healthy development of Blockchain in the public sector and for social causes. One is technical, and lies in safely determining the identities of actors 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's daily lives clear. The education of constituencies to unleash the full power of the Blockchain thus appears necessary.

KEY POINTS TO HIGHLIGHT

- "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."

Case study 7

Name: Vehicle Wallet

Founder & CEO: The Danish Tax Administration (SKAT)

Launched: as Proof of Concept (PoC) in 2017

Where: Copenhagen, Denmark

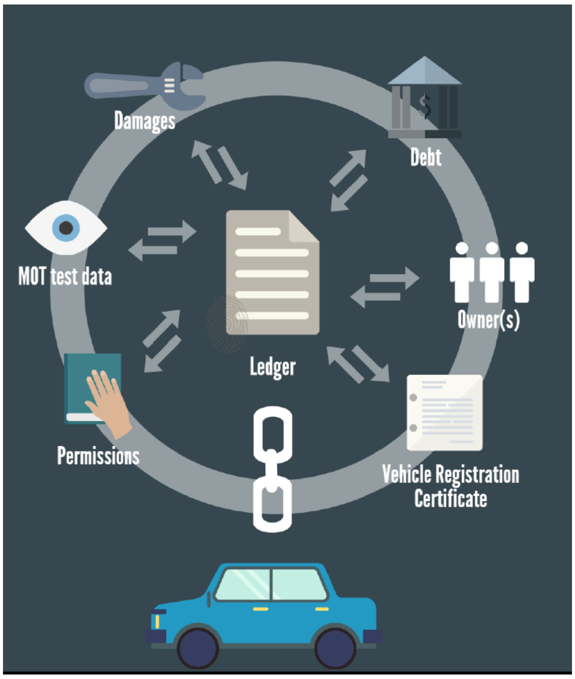
Website: N/A

THE PROBLEM

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.

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 levies.

When trading a car an imbalance appears between seller and buyer. Buyer must believe that the seller provides him with the correct registration certificate. This implies an inherent risk of the car being undesirably re-build, in dept or even stolen property. Seller on the other hand have to trust that 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.



THE SOLUTION

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.

The government regulator creates and populates the registration for the new vehicle, which is loaded onto the blockchain. The smart contract ensures that only the regulator can do this. The regulator then transfer 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.

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 are 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.

RESULTS AND IMPACTS

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 affordances in order to create a clear business case concerning utilization 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 authorization 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 minimize existing operational costs.

KEY POINTS TO HIGHLIGHT

- 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.

Blockchain technologies an governments: challenges

The implementation of Blockchains does not come without challenges. While its applications in the public sector are numerous, they are not always evident. It is *not* the case that Blockchains answer all of governments' problems. The next section seeks to make sense of such challenges and understand where technological limitations lie.

Transparency, Confidentiality and Decentralisation

Public Blockchains allow for perfect transparency, where "decentralised architectures generally rely on the disclosure of everyone's interactions" (DeFilippi, 2016, p.1). 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. This is particularly well exemplified by the EU's right-to-be-forgotten principle, which stipulates that an individual may ask to have her record deleted from government databases (see Gabison, 2016).

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 centralised governance models (permissioned Blockchains) while "radical transparency" (DeFilippi, 2016, p.0) will bring risks to the exploitation of personal data, but remains closer to the Blockchain technology's underlying aim to function independently of centralised authorities.

Coding and Governance Models

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. DeFilippi & Loveluck (2016), in the specific context of the Bitcoin platform, decipher two layers of coordination:

- "The *infrastructural layer:* a decentralised payment system based on a global trustless peer-to-peer network which operates according to a specific set of protocols;
- Layer of *architects*: a small group of developers and software engineers who have been entrusted with key roles for the development of this technology" (p.10).

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

Blockchains, are ultimately constrained in what the code of each and every platform allows for.

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, and constrain room for change on the platforms to what is deemed feasible and democratically acceptable.

Talking About Blockchain – Separating Blockchain from *Bitcoin*

There seems to be a large consensus across Blockchains specialists that *talking about Blockchains* to citizens is one of the most complex part of their jobs. In the words of Justin Herman (2017), Emerging Citizen Technology Programme 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".

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."

Along with this defiance, and almost paradoxically, the expansion of the *Bitcoin* platforms has been significant in recent years – in terms of market cap, value of the *Bitcoin* against the US Dollar, or the number of recorded daily transactions. More may need to be done to explain and convey the possibilities before blockchain technology can be used widely and become accepted.

Copyrights

Copyrights can be apprehended from two different perspectives when integrated to any Blockchain architecture:

As content becomes so multidisciplinary and copyright ownership blurs, 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.

On the other hand, "[o]nce a copyrighted work of art is recorded on the ledger, it will become virtually impossible to take down because no central server can be disconnected and no individual can be stopped." (Gabison, 2016, p.6). Any erroneous information, if confirmed on a blockchain and added to a secured block – for malicious purposes, but also due to nodes' ignorance – will indeed not be mutable or destroyed.

This is of issue in legal terms – who then will be penalised for the provision and use of illegal content? While original infringers (illegal providers of content) may be held liable – and will most likely be more easily traceable than in the current system – they may quickly become judgment-proof. This is particularly true when "a copyright holder attempts to recovery for every download for each upload" (*ibid.*), making original infringers unsolvable in front of Justice. Instead, copyright holders may be more inclined to file injunctions to block access to links rather than *deleting* such links (Gabison, 2016, p.7) – thus going after subsequent infringers (illegal content users) instead. At the same time, it may prove necessary to think of new governance mechanisms to control what goes into Blockchains with regards to protected content – in the form, for example, of accredited observers.

Public-Private Partnerships

The numerous communities of practice that are emerging across administrations share an effort to bring public agencies and private firms together in developing Blockchain systems.

Large consortiums such as *R3* or IBM's *Hyperledger*[15], but also the Crypto Valley Association in Switzerland, the Blockchain Trust Accelerator in the US, or the Blockchain and Virtual Currency Association of India aim to bring all actors into one same community with similar goals and aims with regards to Blockchain. In an interview with the Observatory, Justin Herman, who heads one such community of practice, explains that "public-private partnerships [*PPPs*] are not only desired; they are encouraged" (2017). Since the creation of the Global Blockchain Council in early 2016, 15 Blockchain-related projects have seen the light of day, a large majority of which are PPPs (Raford, 2017). More specifically there seems to be a trend where private firms *assist* government agencies with the technological aspect of the work. The most influential model of PPPs in this sector is most likely to be the *ID2020* initiative, which aims to provide a digital identification to all refuges and stateless individuals through signed partnerships with UN sister agencies and private companies such as Microsoft and Accenture.

This rapid development in PPPs, and stronger links between private and public spheres, is also due to the lack of subject-matter knowledge *within* governments. While there is understanding around Blockchain at different levels within the public sector, coding proficiency remains limited. In the words of Axelle Lemaire (2017), talking about 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.

Costs and Scalability

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 DLT/Blockchain are as yet unclear" (Deshpande *et al.*, 2017, p.15). 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" (*Ibid.*, p.16).

[15] Though this is more geared towards the private sector and the developer's community

Conclusions and a way forward

The aims of this short guide were threefold:

- *Explain* what Blockchain is;
- *Explore* what is already occurring in the Blockchain space for the public sector;
- *Make sense* of its impacts on the public sector, and *anticipate* future developments.

It is no easy task – Blockchains are, by essence complex tools, and the existing literature focuses more on its technicalities than its implications in “the real world”. Furthermore, the technology is closely related to the infamous *Bitcoin* platform, and splitting the two is now more than essential.

At the same time, the infrastructure has “immense powers” (Rinearson, 2017) that are waiting to be unleashed. More specifically, “the key advance from Blockchain technolog[ies] is distributed trust – removing the need to rely on a specific single trusted third party […] to facilitate transactions” (Hanson, 2017). The public sector could reach levels of data security never reached before – in fact, it may be the case that data can be *perfectly* safe through Blockchain technologies.

As the technology grows in its applicability and services, it is of paramount importance to introduce and analyse the matter in an objective way, irrespective of what debates in political and civil society scenes there may be – while not becoming insensitive to them. This report has aimed to strike the right balance between those two conflicting forces.

Section I focused solely on explaining the technology in what we believe to be accessible ways. It presents its main features and contextualises Blockchains: how it develops on specific platforms, the rise of Smart Contracts and the security protocols necessary to ensure information on Blockchains cannot be tampered with. It provides the necessary tools to best understand why, and how, Blockchains act as hypersecured ledger which allow for transactions without the certification of an official, trusted third-party – indeed, the very trust shifts from the central authority to the *system* and the consensual decision-making process that it allows. The credibility and security of any Blockchain-run platform is fully contingent on the reliability of actors to take the right decision at all times.

Further, we made clear that the mathematical construction of the Blockchain through a mere chain of blocks of transactions allows for ability to have an immutable history of changes. This is particularly important in a digital era which allows for untraceable changes to any document, thus affecting the very notion of truth.

Section II moved from the technicalities to the implementation of Blockchain services in, and for, government. A number of case studies were presented to have a better grasp as to what the technology truly *means* for the public sector.

Section III is a logical follow-up of Section II, for it seeks to bring a more thorough understanding of what it means for government sectors to be disrupted. On a number of topics, it looks at the challenges of the technology – be it from technical, regulatory or governance aspects. It leads the way to the conclusion that despite its potential great impacts, Blockchains face numerous challenges, from a policy perspective, that concerned stakeholders must address relatively urgently. It is now the work of regulators to understand the technology to protect sensitive information on the one hand, while leaving room for innovation and trying new things on the other.

A number of other questions are brought to the fore as a result of this guide: how will regulation adapt, and at what pace? How will the technology develop – and towards which ends? Will the growing political willingness be sustained – even as the technology requires the redefinition of State prerogatives? Will public servants and citizens-at-large be willing to adopt the new technology? Finally, will there be cases and situations in which Blockchain will *not* be the answer – which implies that cost and benefit analyses must adapt to the new tool?

These are hard questions to find suitable responses too – only because it would come down to betting against the unknown. However they are important questions that one must bear in mind as Blockchains develop and enter the realm of the public sector – and public life.

It is not enough to push the issue away in light of its technical complexity. It is not enough for regulators and policy-makers to give all powers to developers on mere grounds that “they understand it”. As Blockchains develop and may indeed become the new Internet, a lot of work must be done to make such technologies accessible to all, and its impacts on the public sector investigated and known. The rise of Blockchains must not override the necessity for experimentation and evidence to ensure that it is relevant and that it meets the criteria of confidentiality, security, decentralisation to only name a few – along with the creation of some form of government-wide governance framework. This has never been done in the realm of the public service for Blockchains. This guide is a first step in this very direction.

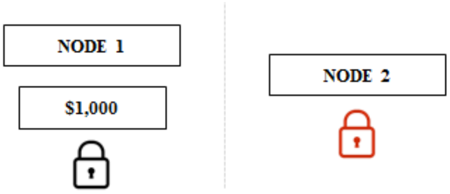
Appendices

Appendix A: Public and private keys

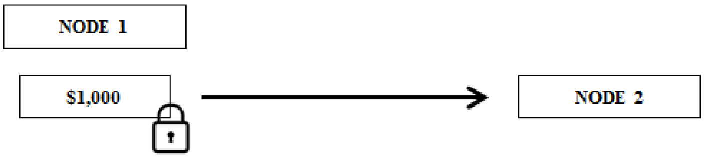
Public and private keys are a cryptographic protocol that confirms or infirms the identity of each party in a Blockchain-based transaction. Indeed, the mere nature of a distributed system allows for two parties who have never met to transact. Further they must do so without the approval of a centralised third-party, as discussed in Section I.

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. Furthermore, they are prone to change as more efficient protocols see the light of day.

We will start with the assumption that the two parties actually *know and trust each other*. More specifically, each party knows it is dealing with the correct second party, in which it can place its trust. Let's now assume that the first party, **Node 1**, wishes to transact $1,000 to **Node 2**. Both have padlocks with the corresponding key, and each only has the key to her own padlock, such that[16]:

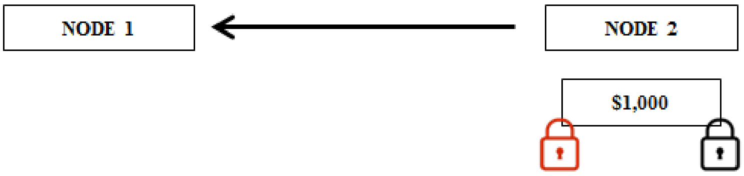


In order to start the transaction, **Node 1** will send the $1,000 to **Node 2** – say, in the form of a sealed package – with **Node** 1's padlock. This ensures that the transaction can securely reach the second party.

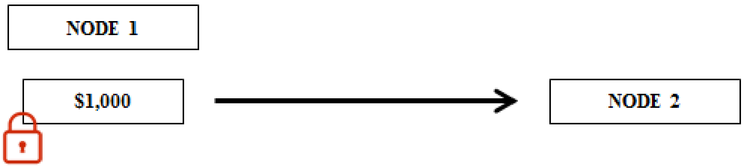


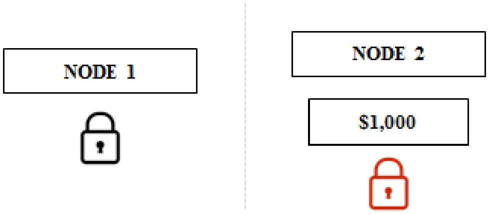
[16] This next section is inspired from Rinearson, 2017b

Once successfully sent over, **Node 2** will add her padlock to the package and send it back to **Node 1**.



Upon reception, **Node 1** unlocks her padlock and sends the package back to **Node 2**. The latter is then able to unlock her padlock and terminate the transaction. Note that the process remained secured at all stages.



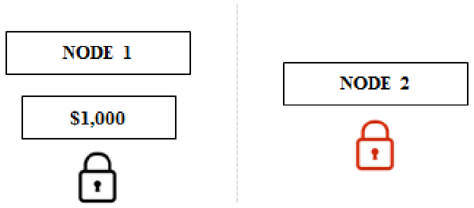


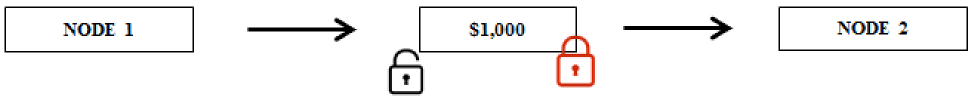
The problem is naturally different when information about one of the party is not perfect. This is particularly relevant when a transaction is sought with a party with whom there was no prior interaction. There must be a way to shift the trust logic from the party to the system. This is the problem public and private keys successfully resolve.

Public keys are cryptographic padlocks in the form of complex strings of numbers, unique to each actor in the network. These can be viewed by all nodes but can only be unlocked by their owner through the means of a unique private key. This acts as a signal that the actor one wishes to transact with *indeed is the actor one wishes to transact with* – ultimately replacing the role of the bank to confirm the identity of the parties.

When a transaction is sought, **Node 1** will forward the correct amount *along with her public key and that of **Node 2*** – thus determining in a unique fashion who the transaction targets.

This is not all: **Node 1** will prove her identity by unlocking her public key with her private key (that she only has access to). This acts as a signal that the two parties are indeed fit for transaction.





Appendix B: Hashing

Hashing is the process of compressing any input – a video, written document, a piece of music, etc. – into a mathematical cryptographic output, a hash, of a fixed size. The document essentially becomes a line of numbers and letters, and is *unique* to this document: such that a same input will always produce the same hash[17], and no other input will ever give the same hash. The input is processed through a hash function, which translates as some mathematical equation.

To better clarify, a small paragraph from the Observatory's website will be used as an input to be hashed:

Input

> The OECD has developed an Observatory of Public Sector Innovation (OPSI) which collects and analyses examples and shared experiences of public sector innovation to provide practical advice to countries on how to make innovations

Once processed by the hash function, it provides this hash:

Hash

```
9bb11726ad25d7deb9fe1bcebca51550d19c7cb80d2170a7ca6e8e95f
```

This output acts as a *digital fingerprint* of this specific input. Not only is it unique, but a minimal change in the input will provide a very different output. Thus should the first letter of the text be decapitalised, such that:

[17] Given one same hash function – see Faife, 2017 for a detailed and technical explanation

Input

the OECD has developed an Observatory of Public Sector Innovation (OPSI) which collects and analyses examples and shared experiences of public sector innovation to provide practical advice to countries on how to make innovations

It follows that, once processed, the output is rather different. In this particular case, we find:

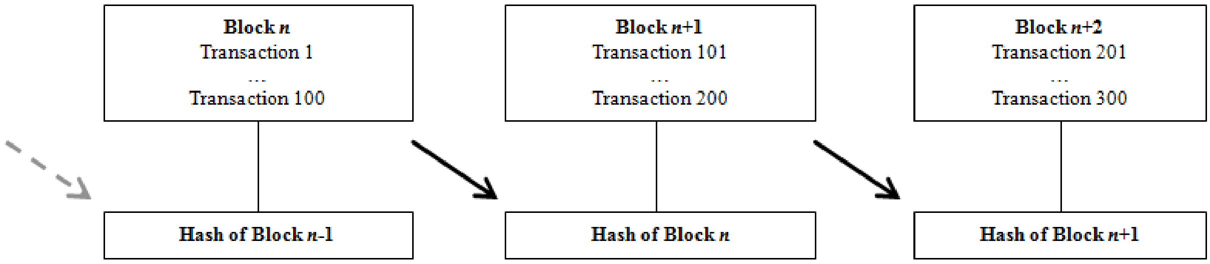
Hash

1705df4533240034bd8dda3be4c46081c543250c10ef955ed278c2833

For the sake of clarity, below is the former hash again. Note that there can be no logical relationship between the former and the new hash:

9bb11726ad25d7deb9fe1bcebca51550d19c7cb80d2170a7ca6e8e95f

This concept becomes particularly important as it is used to secure a set of transactions into blocks. A given set of transactions, when hashed, provide a hash that acts as a unique digital padlock – thus creating a safe block. To increase security levels, the Blockchain infrastructure adds a layer of complexity: the hash of any block is the sum of the hash of the content of the block *and* the hash of the previous block[18].

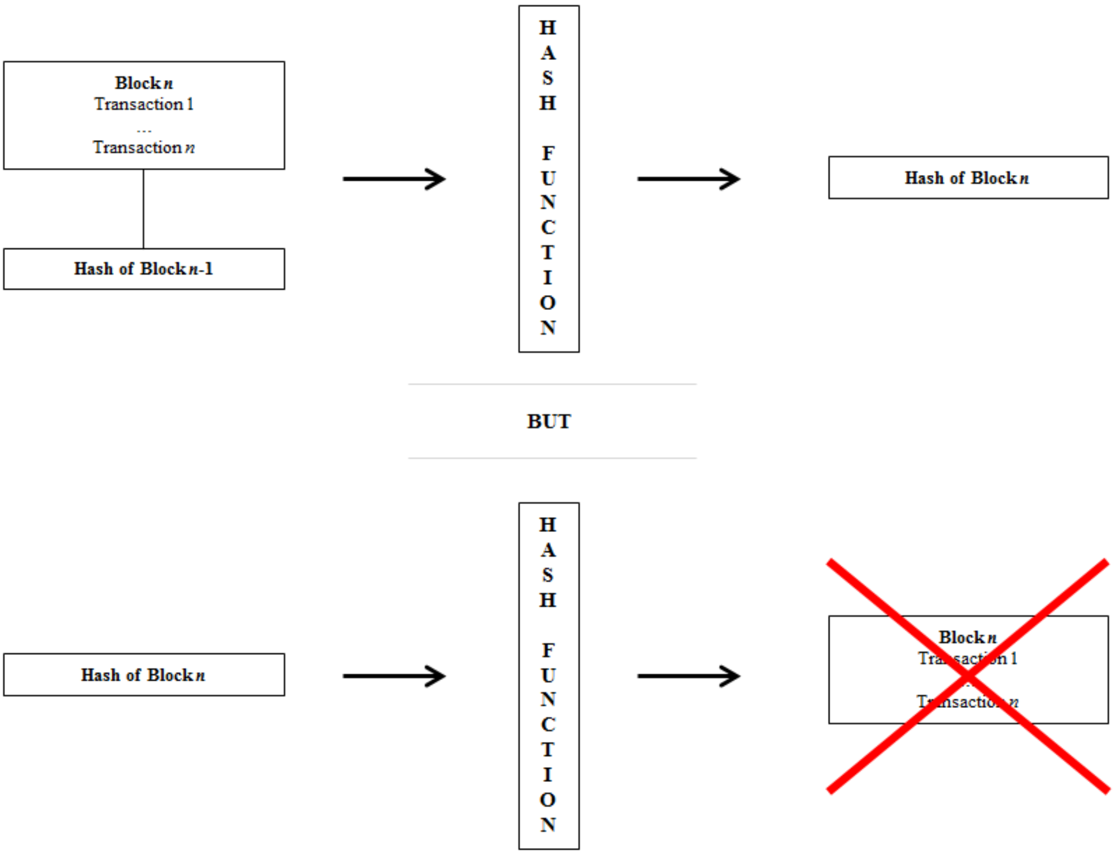


Hashing – The interdependence of blocks (David, forthcoming, p.8)

[18] In some platforms, the hashing process is even more complex, for greater security levels. This protocol, known as *Proof-of-Work*, is presented in Appendix C

Any aim to tamper with a transaction in *Block n* will ultimately modify the *Hash of Block n*. Logically, the *Hash of Block n+1*, which is the sum of *Block n+1* and the *Hash of Block n+1*, will also change – and so on and so forth. It follows that once the hash of Block *n* is associated to the Block *n*+1, Block *n* becomes ultimately immutable – and its content with it. Else it would imply that the entire chain changes accordingly at a faster pace than it takes to create the subsequent block, which is practically impossible to do.

It is also important to note that hashing is only a one-way process: in other words, while the input provides its own unique hash – in fractions of a second –, the hash *does not* provide the input it has essentially compressed. The cryptographic hash only works as a padlock, but at no point does it play the role of a key. It ensures that the mere possession of the valid hash does not open the way to accessing the block and potentially changing its content.



Hashing – From the input to the hash

The hash is the proof that something indeed *occurred* – that a block was successfully created. Moreover, remember that each node holds identical ledgers – thus it must hold identical hashes for each block of transactions, too. The hash acts as a proof of consensus:

If all nodes produce the same identical hash given an identical hash function, it follows that they had identical inputs to start with. This tests and confirms that there is perfect and identical information on the Blockchain.

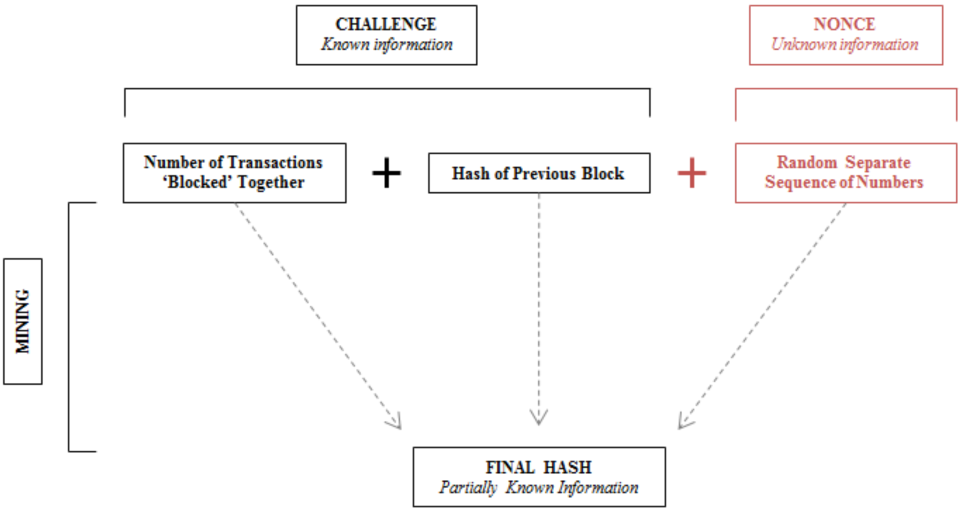
Creating the hash is an essential feature of many Blockchain platforms. It is introduced in Appendix C.

Appendix C: Mining

To best understand the mining process, it is important to take a step back, and dive again into the different steps of a Blockchain transaction:

1. Two parties wish to carry out a transaction, and broadcast their demand onto the entire network;
2. Nodes check their ledgers to ensure that the transaction is feasible and confirm the transaction
3. Once a certain number of transactions have occurred, they must be safely secured within blocks – this is where mining comes into play.

Miners – i.e. powerful computers – aim to find the safest hash / padlock possible. In order to do so – and for a set hash function, as determined by the platform at hand – it takes a set number of transactions that will be 'blocked' together as well as the hash of the previous block – which has been shared on the distributed network hence is known by all nodes. The sum of these two variables is called a *challenge* and, put together, form an input of their own. As we know from hashing – see Appendix B – such input, if compressed by the hash function, would provide a unique output: a hash.


CHALLENGE
Known information
NONCE
Unknown information
Number of Transactions 'Blocked' Together
+
Hash of Previous Block
+
Random Separate Sequence of Numbers
MINING
FINAL HASH
Partially Known Information

The mining process on the Blockchain

Platforms such as *Bitcoin*[19] take security a step further and require another separate sequence of numbers, a *nonce*, to be added to the challenge. This nonce takes the form of a random sequence of numbers that, when added to the challenge, will logically provide a new unique hash. Most importantly, *Bitcoin* requires miners to produce a final hash with one specific characteristic: it must have a set number of zeros in its prefix, such as:

```
0000000007fc18bc577e227ec7d65a3ced26546bdb2466529ae6149f
```

It follows that the probability of finding the correct hash diminishes as the number of zeros increases, for a fixed hash function and thus a hash of a fixed size.

With a known challenge, it is the role of miners to find the right nonce such that it fits the hash requirements. This can only be achieved through a trial-and-error mechanism: miners 'simply' try an immense number of combinations until the right fit is found. Such process requires computers to try a high number of potential nonces every second and uses up incredibly large amounts of energy.

Once the correct hash is found by a miner, it is automatically broadcasted to the entire network, and all nodes – with identical information – try the nonce for themselves. This is important: while producing the correct hash from a set hash function and input is complex, verifying the validity of this very hash can be done very quickly – and requires little energy. Once confirmed, the block of transaction is finally sealed, and miners go on to seal other blocks of new transactions. This entire process is called a *proof-of-work*: it is the process of proving that the mined hash is indeed valid in light of the three main constraints:

- A set input, in the form of a list of transactions. This is identical among ledgers;
- A set hash function, predefined by the platform once performs transactions on;
- Known hash requirements, also defined by the platform.

This process allows for high levels of security on the Blockchain and thus ensures the immutability of transaction information. Furthermore, the 'winning' miner – the first miner to find the correct proof and broadcast it to the distributed network – receives a set amount of

[19] Things are different on *Ethereum* – see Kasireddy, 2017

Bitcoins[20]. This creates an incentive for the mining process to keep on going, thus by essence securing the network by even larger extents. This amounts to a powerful self-reinforcing securisation protocol.

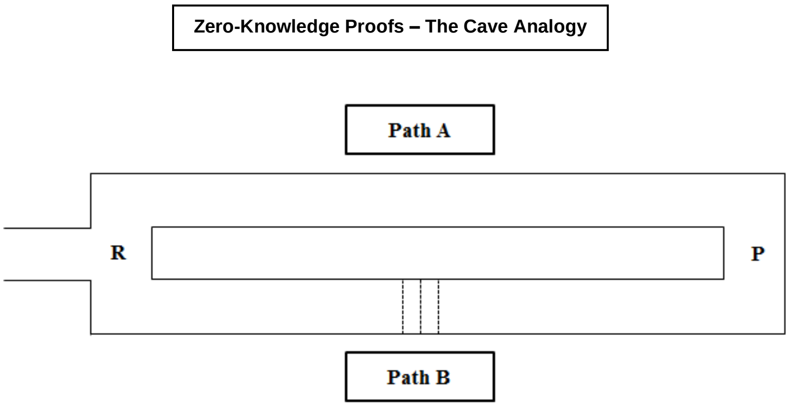
[20] At the time of this report, it amounts to 25 BTC

Appendix D: The zero-knowledge proof

The Zero-Knowledge Proof is a mathematical construction that responds to the following set of issues:

1. One party (the prover) must prove to another party (the receiver) that a transaction is valid and has occurred;
2. The receiver is *not able* to see the transaction;
3. The receiver must believe without the shadow of a doubt that the prover is saying the truth;
4. There must be no central authority holding any certification role.

This rather counter-productive idea of proving something by the mere act of stating that it is true is better understood with the common analogy of the cave (see Guillou *et al*, 1998). *The Prover (P)* claims that she holds a secret password to open a door that stands in the way of Path B (represented by three dotted lines). However, she is at no point allowed to give the password to the second party, *the Receiver (R)*. A way must be found for *P* to prove that she holds the password, and can take any of the two paths to go around the cave and reach safely to *R*.



In order to do so, *P* enters the cave using either path and stands opposite to *R*. *R does not see* which path *P* takes upon entering the cave. Once both are set, *R* calls on *P* to randomly take either of the two paths to return. If *P* says the truth and holds the password, it follows that she can walk back on either of the desired paths. However if she lies and can only return through path A, then *P* only has a 50% chance of returning – that is, there is only a 50% chance that *R* calls Path A. Should this process repeat a large number of times, the likelihood that Path A only is chosen becomes radically small[21]. If *P* continues to return safely to *R* at all times, it logically follows that there is an extremely high probability that *P does* hold the secret password.

Zero-knowledge proofs come down to setting a binary probability with one of the options conditioned on the transaction being valid and having taken place. As the number of tests increases, the probability that the prover lies becomes so extremely small that the transaction can indeed be safely trusted with a high degree of confidence.

[21] The probability that *R* always calls Path A is equal to 0.5^n, where *n* is the total number of reiterations

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. 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

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

3. 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*

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

5. “Bitcoin Energy Consumption Index”, 2017, *Digiconomist,* Online, last accessed 30 August 2017, https://digiconomist.net/bitcoin-energy-consumption

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

7. 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/

8. 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

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

10. David, Torben, forthcoming, “Distributed Ledger Technology: Leveraging the Blockchain for ESA”, *European Space Agency*

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

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

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

14. “Emerging Citizen Technology”, 2017, *General Services Administration*, Online, last accessed 24 August 2017, https://www.gsa.gov/portal/category/101958

15. Farell, Ryan, 2015, “An Analysis of the Cryptocurrency Industry”, *Wharton Research Scholars*, 130

16. Gabison, Garry, 2016, “Policy Considerations for the Blockchain Technology Public and Private Applications”, *Bepress*, European Commission

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

18. 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

19. 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

20. 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

21. 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

22. “Is Blockchain technology the new internet? A step-by-step guide for beginners”, n.d., Online, last accessed 23 August 2017, https://blockgeeks.com/guides/what-is-blockchain-technology/

23. 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

24. 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

25. 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

26. Nathan, Oz; Pentland, Alex; Zyskind, Guy, 2015, “Decentralising Privacy: Using Blockchain to Protect Personal Data”, *IEEE Security and Privacy Workshops*

27. OECD, 2016, “OECD Science, Technology and Innovation Outlook 2016”, *OECD Publishing*, Paris

28. OECD, 2017, “Embracing Innovation in Government: Global Trends”, *OECD Publishing*, Paris

29. 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

30. “Ordonnance n.2016-520 du 28 avril 2016 relative aux bons de caisse”, 2016, *Journal Officiel, 29 avril 2016, texte n.16*

31. 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/

32. “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

33. 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

34. 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

35. 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.

36. Snäll, Mats, “Blockchain and the Land Register – A New ‘Trust Machine’?”, n.d., Submission n.572

37. Stawinska, Karolina, 2017, “Meet 10 Millenia 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

38. “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

39. “The Social Smart Contract: An Open Source White Paper”, 2017, *Democracy Earth Foundation*, Online, last accessed 31 August 2017, file:///C:/Users/Bourgery_T/Downloads/The%20Social%20Smart%20Contract.pdf

40. Walport, Mark, 2016, “Distributed Ledger Technology: Beyond Block chain. A Report by the UK Government Chief Scientific Advisor”, *UK Government*

41. 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

42. 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/

43. 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/

44. 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