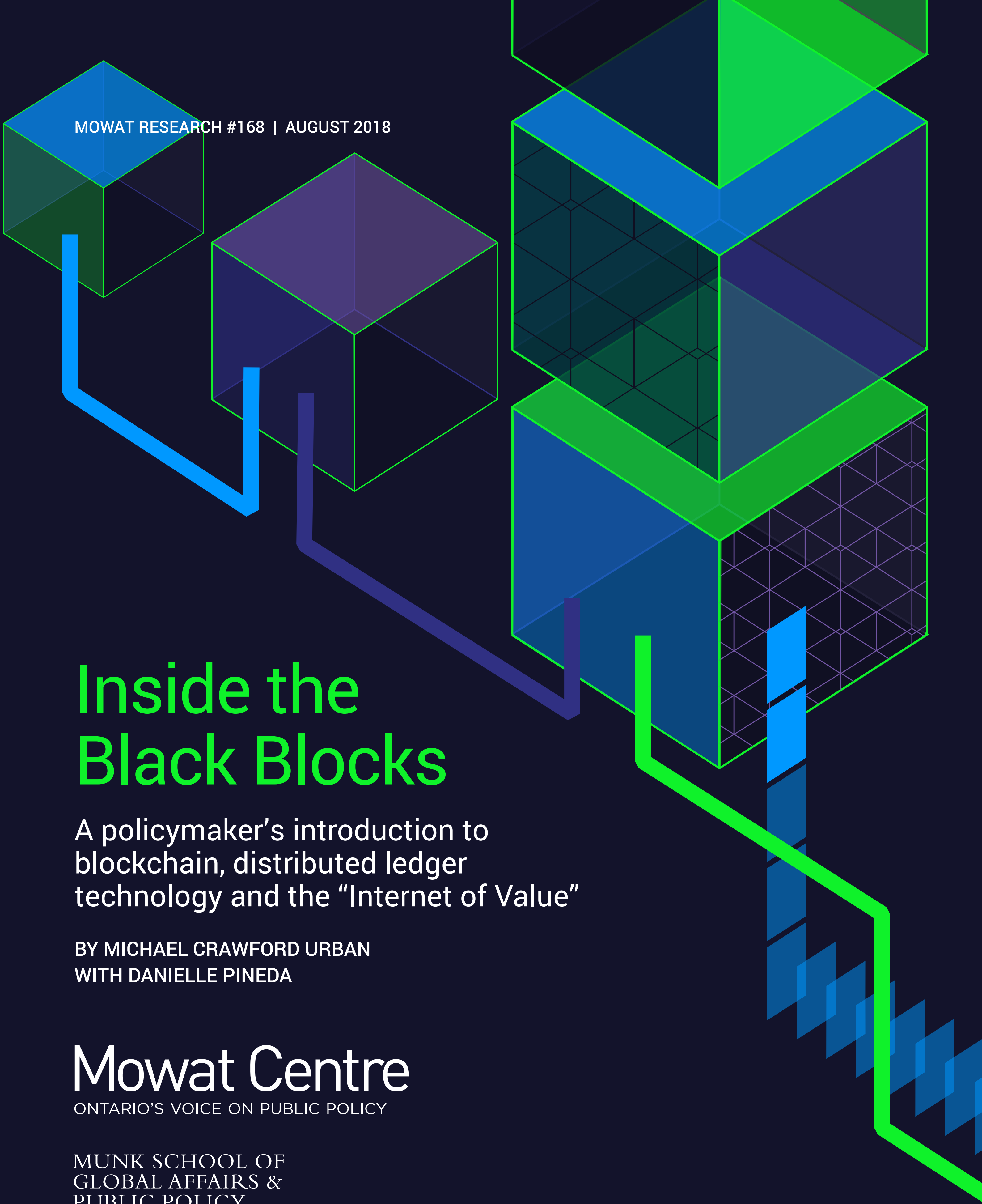
MOWAT RESEARCH #168 | AUGUST 2018



Inside the Black Blocks

A policymaker's introduction to blockchain, distributed ledger technology and the "Internet of Value"

BY MICHAEL CRAWFORD URBAN
WITH DANIELLE PINEDA

Mowat Centre
ONTARIO'S VOICE ON PUBLIC POLICY

MUNK SCHOOL OF
GLOBAL AFFAIRS &
PUBLIC POLICY

Acknowledgements

The authors would like to thank those who participated in this research project as key informant interviewees and anonymous reviewers. A special thanks to Andrew Parkin, Sunil Johal, Kiran Alwani, Catherine Stinson and Reuven Shlozberg for reviewing the paper and for their helpful feedback, as well as Elaine Stam for going above and beyond in her design work for this report. Any remaining errors are the sole responsibility of the authors.

Authors

MICHAEL CRAWFORD URBAN

Practice Lead,
Government Transformation

Michael joined the Mowat Centre as a Policy Associate in January 2016 and took on the role of Practice Lead, Government Transformation in September 2017. He brings a varied set of experiences to his work at Mowat having worked at Global Affairs Canada in Ottawa – most recently as a Cadieux-Léger Fellow – with Elections Canada and in the think-tank and NGO sectors in Toronto and Ottawa. He holds degrees from Queen's University, Carleton University and the University of Oxford.

Disclosure: Michael Crawford Urban owns a small amount of bitcoin and ether.

DANIELLE PINEDA

Policy Intern

Danielle worked at the Mowat Centre as a Policy Intern from May to August 2017. She has also worked for Ontario's Ministry of Health and Long-Term Care, the Legislative Assembly of Ontario and provided teaching and research support at the University of Toronto. She is currently a Policy Analyst at AdvantAge Ontario. Danielle holds a Master of Public Policy and Honours Bachelor of Arts degree in Political Science and Media Studies from the University of Toronto.

Mowat Centre
ONTARIO'S VOICE ON PUBLIC POLICY

The Mowat Centre is an independent public policy think tank located at the Munk School of Global Affairs and Public Policy at the University of Toronto. The Mowat Centre is Ontario's non-partisan, evidence-based voice on public policy.
It undertakes collaborative applied policy research, proposes innovative research-driven recommendations, and engages in public dialogue on Canada's most important national issues.

MOWATCENTRE.CA
@MOWATCENTRE

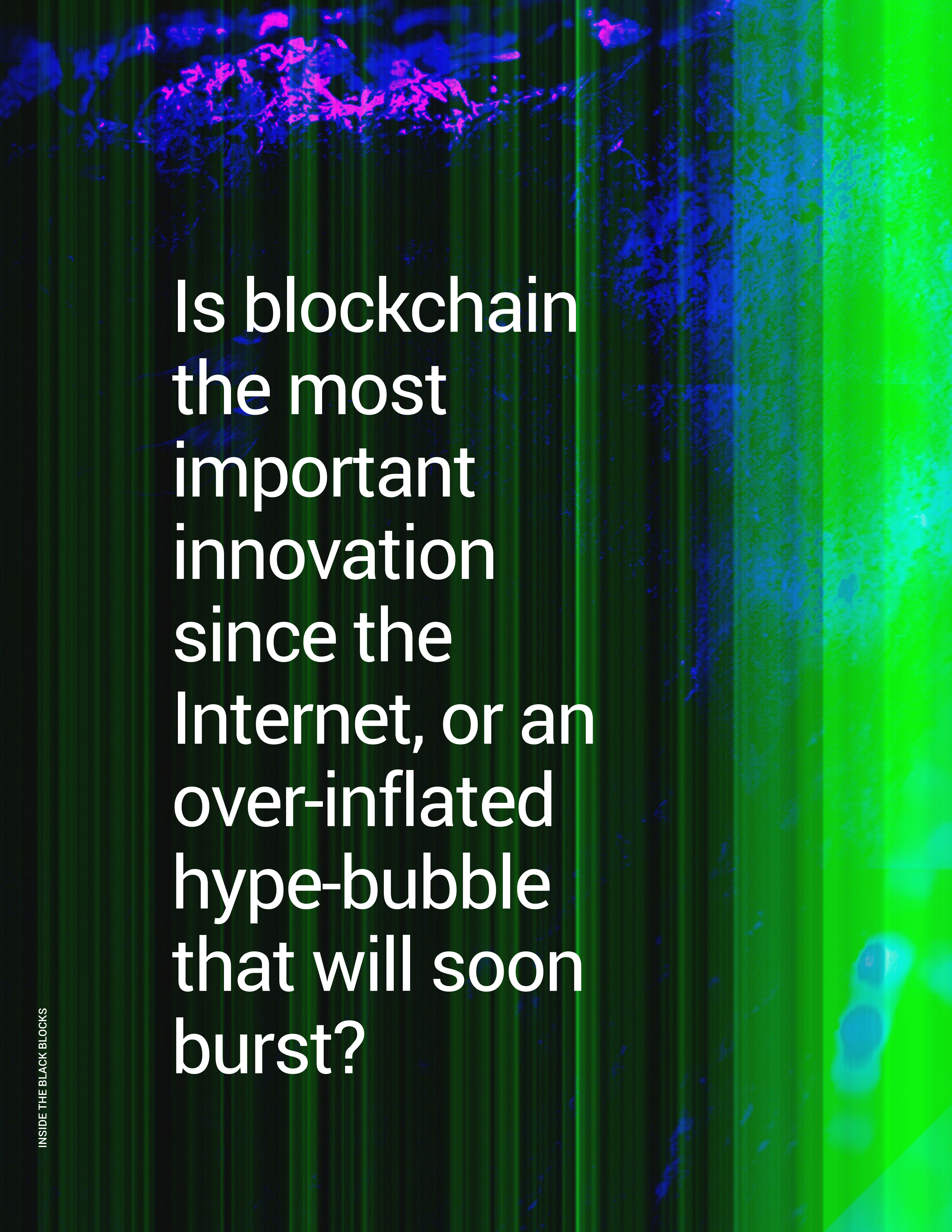
439 UNIVERSITY AVENUE
SUITE 2200, TORONTO, ON
M5G 1Y8 CANADA

MUNK SCHOOL
OF GLOBAL AFFAIRS
& PUBLIC POLICY

UNIVERSITY OF
TORONTO

©2018 ISBN 978-1-77259-068-5

Contents



Is blockchain the most important innovation since the Internet, or an over-inflated hype-bubble that will soon burst?

EXECUTIVE SUMMARY

Is blockchain the most important innovation since the Internet, or an over-inflated hype-bubble that will soon burst? Either way, and even if the truth lies somewhere between these two extremes, rapidly growing interest in blockchain and its potential applications means that policymakers need to quickly develop an understanding of this new technology to guide their engagement with it.

Fortunately, there is no shortage of information about blockchain available to policymakers wishing to learn more about it. Unfortunately, too many of the rapidly growing number of articles, YouTube videos, reports and Twitter threads on the subject are of limited use, for one of two reasons.

On the one hand, many of these pieces are too superficial, speculative or insufficiently rigorous to be of much use to policymakers. On the other, pieces that do engage at a deeper level often end up losing the forest for the trees by focusing too narrowly on blockchain's technical aspects. These accounts intimidate and confuse readers without technical backgrounds while the mass of detail they provide obscures many of the most important aspects of this innovation.

Compounding this problem is the fact that few of either type of report are targeted specifically at policymakers.

This report fills this gap by providing an accessible yet rigorous explanation of how blockchain works and a non-technical but still detailed analysis of the concepts and phenomena that underpin this explanation. It does so with an eye to the significance of blockchain and its potential applications for public policy as well as the potential that exists for governments to use blockchain to advance their own objectives. Throughout, the report also describes potential applications of blockchain and profiles a collaborative blockchain proof of concept conducted by the Government of Canada, the Government of Ontario and the City of Toronto.

We begin with a discussion of what a blockchain actually is and highlight the six essential components of a true blockchain:

» The ability of **multiple collaborators** to make additions to the blockchain.

» A **"write-only" design** that ensures information can only be added to the blockchain and never deleted.

» Hosting of the blockchain on a decentralized **peer-to-peer (P2P) network**.

» The use of a **distributed consensus mechanism** by the network for automatically reaching decisions on whether to accept or reject proposed additions to the blockchain.

» An **incentive structure** integrated into the blockchain's software that ensures that the nodes maintaining it work together.

» The use of **cryptography** to ensure the security, integrity and reliability of the information recorded in the blockchain and of the systems which manage it.

We then provide an accessible and non-technical explanation of how a blockchain actually works. Often glossed over in other reports, we explain the process in simple terms because understanding these foundational details is critical to understanding the larger debates about blockchain's potential and being able to cut through the ubiquitous hype that so often surrounds it.

Building on this explanation, we also identify and explore the fundamental implications of blockchain's emergence. To do this, we analyze the two channels through which blockchain is likely to have its most important impacts: by enabling greater **automation** and greater **decentralization** in both the economy and society. Building on these ideas, we explore a number of potential use cases in the broader public sector, such as **electronic health records, professional and post-secondary credentials**, as well as **government permit issuing and licensing**.

We use this analysis to then identify four critical "Issues to Watch." The first of these, **competition in governance services**, focuses on how blockchain enables a much wider range of actors to participate in the market for services, such as the provision of currencies, previously tightly controlled by governments. Second, we discuss how blockchain, by empowering individuals and networks, may undermine the usefulness of many of the **negative regulatory frameworks** – frameworks designed to block certain activities – that governments have previously used to achieve many of their policy objectives. The third issue to watch concerns the fact that blockchain's spread will likely create a host of **novel legal questions** – such as how to regulate "smart contracting." Finally, we examine the question of how the **governance** of blockchain technology and blockchains themselves will need to evolve.

After identifying these issues, the report offers a set of preliminary recommendations for policymakers as they respond to blockchain's arrival. These include a recommendation to build **internal capacity** so that governments can stay abreast of blockchain's evolution and not be entirely reliant on outside consultants. We also discuss how to **build an attractive environment for blockchain innovation** in Canada. These first two recommendations both depend on, and could help government support, **internal and allied experimentation** with potential blockchain applications so as to ensure that the public sector can access its potential benefits. Insofar as applications of blockchain, such as cryptocurrencies, require regulation we recommend that government take a collaborative approach that **makes greater use of standards and other flexible regulatory tools**. Finally, we strongly recommend that the Government of Canada actively lead the fostering of **national and global governance cooperation** on blockchain.

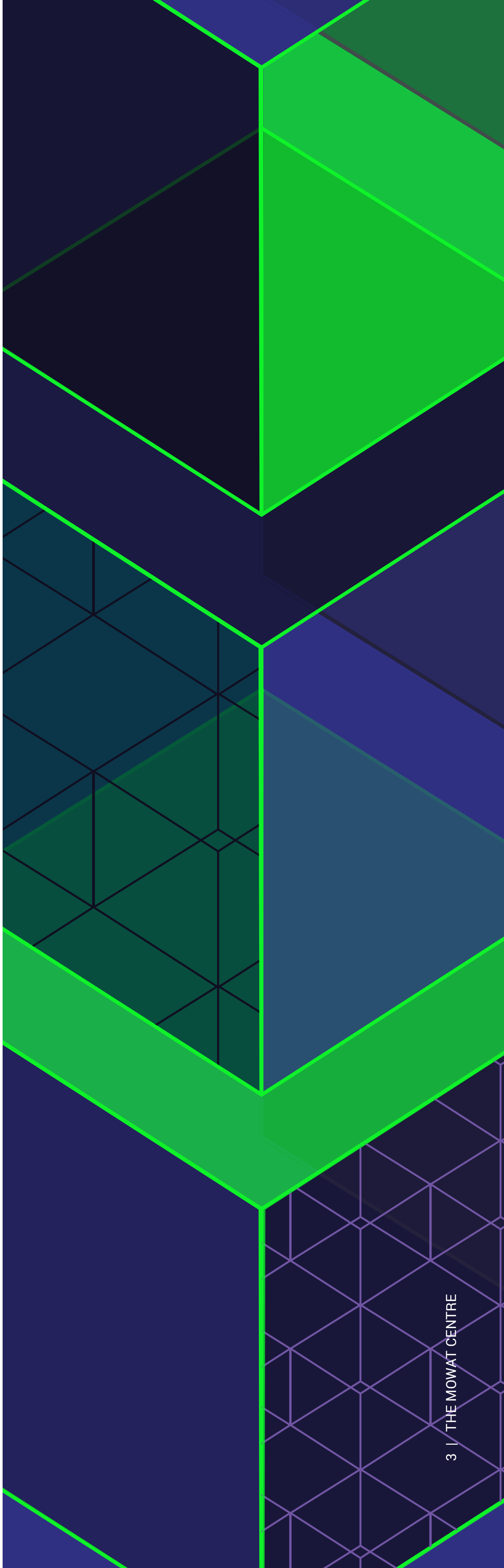
Informed by this analysis, the report closes by identifying three key takeaways for policymakers:

» **Blockchain marks the arrival of the first "digitally native value system."** This in turn lays the foundation for potentially revolutionary forms of automation by enabling software to do many new and important things that it cannot easily do today.

» **Blockchain and associated technologies offer other less revolutionary, but still significant, innovations in terms of organizing and coordinating information systems and tracking a variety of assets.** These implementations will enable greater efficiency and decentralization which could help secure greater privacy and a more even distribution of economic and social power.

» **The most significant implications of blockchain will arise from its interactions with other emerging technologies such as artificial intelligence and the Internet of Things.** Thus, it is critical for government to understand and engage with all of these innovations as part of a wider and interconnected technological revolution which will require a holistic public policy response.

Naturally, there are many other issues related to blockchain that will grow in importance in the future but which are not covered here. We hope that, given this report's analysis of the fundamental concepts and questions raised by this new technology, readers will be better prepared to engage with these issues, ask the right questions and separate what is real from what is hype.



To avoid being caught flat-footed, policymakers will need to understand the basic outlines of blockchain, what it enables us to do that we could not do before and what this means for governments and how they operate.

1 INTRODUCTION

On 31 October, 2008, a mysterious individual, or group of individuals, known only as Satoshi Nakamoto, posted a link to a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* to an obscure mailing list called Cryptography List.[2] In this paper, Nakamoto proposed the creation of what would become known as a blockchain as a means of enabling an electronic payment system that did not require a trusted third party intermediary.

While Nakamoto has never been publicly identified, less than a decade later, Nakamoto's idea has spawned a new class of digital assets whose value, as of January 2018, was estimated at more than $800 billion (USD).[2] Even with a subsequent market correction, the market capitalization of all existing cryptographic assets is, at the time of this writing, somewhere around $300 billion.[3] More than that, transformative applications for the new technology beyond digital cash are being suggested in areas as diverse as securing digital property, administering smart electrical grids, enabling self-driving and self-owning charitable taxis and giving patients vastly greater control over their own health records.

Still, despite the huge investment in this nascent sector, the incredible growth in the markets for digital assets and the massive potential for disruption in a host of industries, blockchain is still absent from many policymakers' radar screens – let alone those of most average citizens. Even for those who have taken notice, few understand the technology much beyond having a vague impression that it has something to do with Bitcoin.[4]

This needs to change because, even if blockchain fails to fulfill its proponents' wildest claims, or the value of a bitcoin[5] drops to nothing, the opportunities and challenges posed by blockchain will offer some of the most significant technology-driven tests faced by governments in

[1] The paper has been preserved at https://bitcoin.org/bitcoin.pdf.

[2] Kharpal , A. 6 February, 2018. "Over $550 billion wiped off cryptocurrencies since record high just under a month ago." *CNBC*. https://www.cnbc.com/2018/02/06/bitcoin-price-over-550-billion-wiped-off-cryptocurrencies-since-record-high.html.

[3] This estimate was made on 25 July, 2018. See https://ca.investing.com/crypto/currencies for an up to date estimate. These are necessarily very rough estimates.

[4] Research conducted on behalf of the Bank of Canada in late 2017 found that 64 per cent of Canadians have heard of Bitcoin but only 2.9 per cent of Canadians actually own any bitcoin. See Henry, C. Huynh, K. and Nicholls, G. December 2017. "Bitcoin Awareness and Usage in Canada." *Staff Working Paper 2017-56 (English).* The Bank of Canada. https://www.bankofcanada.ca/2017/12/staff-working-paper-2017-56/.

[5] In this paper we follow a common convention when referring to bitcoin. When we use the capitalized Bitcoin, we are referring to the Bitcoin network, blockchain or software protocol. When we use the lower-case bitcoin, we are referring to the currency.

the next quarter century. Moreover, because of how they will likely interact with and enable many of the most highly touted technological advances currently under development, such as artificial intelligence (AI) and the Internet of Things (IoT), blockchain and related distributed ledger technology (DLT) will likely represent some of the foundational technologies of the 21st century economy. To avoid being caught flat-footed, policymakers will need to understand the basic outlines of blockchain, what it enables us to do that we could not do before and what this means for governments and how they operate.

A gap in the literature

There is no shortage of information about blockchain. In fact, the Internet is overflowing with explainer articles, videos and reports specifically aimed at explaining what blockchain is and how it works.[6] Unfortunately, too many of these pieces fall into one of two categories. On the one hand, many are too superficial and insufficiently rigorous to be of much practical use. While they may provide a brief impressionistic sketch of how a blockchain works and perhaps catalogue a few industries that many are predicting will be disrupted by it, they lack the deeper analysis that policymakers will need to grapple successfully with the challenges and opportunities that blockchain will create.

Alternatively, many accounts that do seek to engage at a deeper level end up losing the forest for the trees by narrowly focusing on blockchain's technical aspects. These accounts intimidate and confuse readers without technical backgrounds and the mass of technical detail they provide obscures many of the most transformational aspects of blockchain that are of the greatest significance for policymakers. Compounding this problem is the fact that few of either type of these reports are targeted specifically at policymakers.[7]

The critical middle ground that is missing from both these categories is an accessible yet rigorous explanation of how blockchain will actually create the changes that are being described and a detailed but non-technical analysis of the concepts and phenomena that underpin this explanation. This is unfortunate because without such accounts policymakers will not be able to develop the understanding of blockchain required to appreciate its potential implications. Without such an understanding, policymakers will not be able to seize the opportunities presented by blockchain while also avoiding its challenges.[8]

The present report aims to fill this gap by providing the sort of accessible yet rigorous explanation just described. The next section explains blockchain in a straightforward way that will provide the reader with the basic technical understanding needed to engage the larger policy questions discussed later on in the report. The third section builds on this explanation by exploring the fundamental implications of this technical innovation. This third section is aimed squarely at filling the aforementioned gap in the existing policy research literature by providing

[6] Some better examples of these include: MIT Technology Review Editors. April 23, 2018. "What is a blockchain?" *MIT Technology Review*. https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/. Centre for International Governance Innovation. 4 January, 2018. *What is Blockchain?* Centre for International Governance Innovation (CIGI). https://www.cigionline.org/multimedia/what-blockchain.

[7] A notable recent exception: Berryhill, J., Bourgery, T and Hanson, A. 2018. "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector." *OECD Working Papers on Public Governance*. No. 28. http://dx.doi.org/10.1787/3c32c429-en.

[8] It is true that there are some useful book length documents of this type that exist. See Vigna, P. and Casey, M. 2016. *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order*. New York: Picador. and Casey, M. and Vigna, P. 2018. *The Truth Machine: The Blockchain and the Future of Everything*. New York: St Martin's Press.

readers with an examination of blockchain's foundational concepts and implications. If you already know what a blockchain is and how it works, consider skipping directly to this section.

Building on these ideas, the fourth section explores a number of potential use cases in the broader public sector, such as electronic health records and professional and post-secondary credentials. The fifth section then turns to an examination of four "Issues to Watch" which will pose critical questions for policy- and decision-makers. The report closes with a series of five high-level recommendations for governments as they consider how to respond to the emergence of blockchain and DLT. We also offer some brief concluding thoughts.

Importantly, this report is not designed to be comprehensive in its discussion of blockchain or its applications. At this point, it is much more important for policy- and decision-makers – as well as the interested public – to develop an understanding of the foundational concepts and issues that it raises. Thus, our aim is to provide policymakers with the basic intellectual tools they will need to continue their exploration of this new technology with confidence. Ultimately, our success will be measured by the extent to which readers come away with confidence in their ability to ask the right questions about blockchain as it grows in importance.

This report draws on a research project focused on blockchain technology that was initiated by the Mowat Centre in January 2017. It has involved interviews with almost 20 public servants, academics, entrepreneurs, practitioners and thought leaders working in the blockchain sector or in related areas as well as extensive reviews of academic and grey literatures, informal consultations and jurisdictional scans.

Finally, as one of our interviewees pointed out, one of the reasons that there is such a poor general understanding of blockchain is that it is not "the easiest thing to understand." Blockchain, represents a counter-intuitive and potentially radical new way of doing certain things that have been done the same way for centuries or, in some cases, a way of doing things that have never been done before. If anyone is presenting blockchain as simple or easy to understand, it's likely you will come away from this interaction missing some critical pieces of the puzzle.

In the pages that follow we tackle this complexity head on, break it down and provide the reader with the clear exploration of blockchain technology that has been lacking in a public policy context. Ultimately, when someone starts talking about "X" amazing thing that blockchain will do, we want the reader to be able to ask the questions they will need to ask to be able to cut through the hype and determine whether and how "X" might actually impact the work of government.

2 WHAT IS A BLOCKCHAIN ANYWAY?

Ironically, for something so intimately associated with the technology sector and Silicon Valley-style innovation, the creation of blockchain did not involve the invention of anything new. In fact, all the components of blockchain existed for years prior to its invention. What is innovative about blockchain, however, is its unique combination of these pre-existing elements into a novel configuration that produced something that was much more than the sum of its parts.

In this section, we provide a thorough account of what that "something" is and what it can do. For simplicity's sake, the focus in this section is on the Bitcoin blockchain because, as the first blockchain ever created, it set the basic pattern for subsequent iterations. Once a basic understanding of what a blockchain is has been established, we will expand our focus in subsequent sections to exploring other blockchains, how they differ from Bitcoin, and how they have helped further develop this new technology.

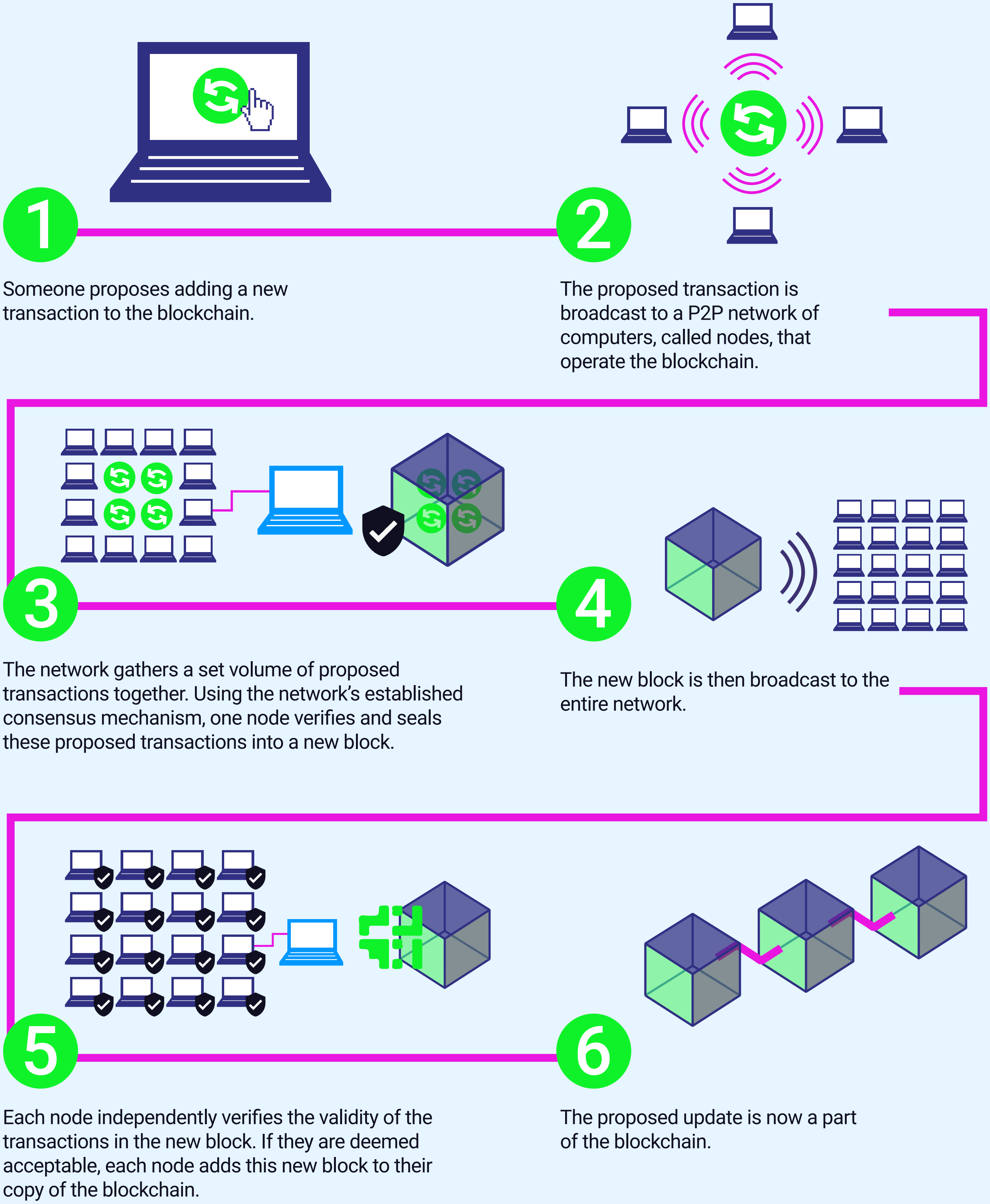
Blockchain basics

A blockchain is, fundamentally, a digital ledger that lists the ownership of a set of assets, as well as an essentially tamper-proof transaction history for those assets. Blockchains are operated by a peer-to-peer (P2P) network of computers in which each of the computers that form a node on the network independently maintains a complete copy of the ledger. Each copy is regularly updated as the nodes of the network work together to record every transaction that occurs on the blockchain in a way that ensures all copies remain consistent with each other.

Blockchains get their name from the process by which new transactions are added to this ledger. When a user wishes to enter a new transaction into the ledger, they must first propose, or "post," this transaction to the network. Once it has been posted, the transaction is grouped together with a number of other transactions posted at around the same time. This group of transactions is then verified to ensure their validity and, if they are confirmed as valid, they are time-stamped and "sealed" into a new "block." Through the use of a technique called "hashing," this new block is cryptographically connected to a "chain" of other blocks which were created earlier and which stretch all the way back to the first or "genesis" block which initiated the blockchain. This process of connecting new blocks to the chain of older ones ensures that once a block has been added to the chain, earlier blocks cannot be tampered with as doing so would break the connection with and invalidate newer blocks (see Figure 1).

FIGURE 1

How a blockchain works



1 Someone proposes adding a new transaction to the blockchain.

2 The proposed transaction is broadcast to a P2P network of computers, called nodes, that operate the blockchain.

3 The network gathers a set volume of proposed transactions together. Using the network's established consensus mechanism, one node verifies and seals these proposed transactions into a new block.

4 The new block is then broadcast to the entire network.

5 Each node independently verifies the validity of the transactions in the new block. If they are deemed acceptable, each node adds this new block to their copy of the blockchain.

6 The proposed update is now a part of the blockchain.

[9] Source: PwC. September 2015. *Money is no object: Understanding the evolving cryptocurrency market.* PwC. https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-evolution.html.

An important feature of the Bitcoin blockchain is that it is public and "permissionless," meaning that it can be viewed in its entirety by anyone and that anyone can transact on it or set themselves up as one of the nodes that helps to maintain it. One important implication of this is that, because every transaction is recorded on the blockchain, it is possible to trace the entire transaction history of each and every bitcoin ever created. For a variety of reasons that we will explore throughout this report, some innovators have also sought to create "private" or "permissioned" blockchains where the abilities to view the blockchain, propose transactions and act as a node maintaining it are restricted in various ways.

Critical features

Based solely on this overview, it can be difficult to recognize what is so special about a blockchain. Further complicating matters is the fact that there has been a purposeful blurring of the already loose definition of a blockchain by a variety of actors seeking to associate their own offerings with the much-hyped technology as a means of attracting financing and attention.[10] Many of these technologies are similar to blockchain, or incorporate some of its component technologies, but differ in crucial respects. Indeed, given the extent to which the term blockchain is contested, some have abandoned the term altogether and refer instead to "distributed ledger technology" or DLT, a broader term that captures blockchains as well as other related technologies.[11]

While DLT is discussed in this report, the core focus is on blockchain. This is because, while DLT has significant potential of its own, it is neither as novel, nor potentially as revolutionary, an innovation. Given that the focus of this report is on understanding blockchain and its potential implications, broadening the focus too much risks further muddying already cloudy waters.[12]

So, what is so innovative about blockchain? Fundamentally, blockchain enables, for the first time, reliable, transparent, searchable and auditable version control of a shared and immutable distributed ledger in real time, without the need for a trusted central authority or intermediary to maintain that ledger. While there is no universally accepted definition of blockchain,[13] we find it useful to define a blockchain as combining the following six features:

» The ability of **multiple collaborators** to write to the ledger without a single central point/entity empowered to accept or decline these proposed additions.

» A **"write-only" design** that allows information to be added to the ledger but not deleted. While the current state of the ledger can continue to be changed, these changes represent updates of the existing record, the entirety of which remains accessible on the ledger.

[10] For an extreme example, see Shapira, A. and Leinz, K. 21 December, 2017. "Long Island Iced Tea Soars After Changing Its Name to Long Blockchain." *Bloomberg*. https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain.

[11] UK Government Chief Scientific Adviser. December, 2016. *Distributed Ledger Technology: beyond block chain*. Government of the United Kingdom. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[12] This is not to say that DLT is not important as in many cases it will actually be a distributed ledger that gets implemented and not a blockchain, properly defined. Nevertheless, this paper focuses on blockchain as a way of exploring the potential of this new technology with as few qualifications, and with the most clarity, possible – even if actual implementation of the technology, in the form of less revolutionary distributed ledgers, will sometimes fall short of this full potential.

[13] We have arrived at this list of features through our own independent research and believe that this represents a robust working definition that side-steps many of the unhelpful technical debates that currently exist and incisively captures the critical features of a true blockchain.

» The hosting of the ledger on a distributed **P2P network** where each full node in this network possesses a regularly updated copy of the entire ledger.

» A **distributed consensus mechanism** by which the network automatically reaches decisions on whether to accept or reject proposed additions to the ledger.

» Some form of **incentive structure** to ensure that the nodes maintaining the blockchain provide the computing power needed to do so. For public blockchains like Bitcoin, this usually takes the form of a "coin" or "token" that nodes can receive as a reward, while private or "permissioned" blockchains employ a greater variety of incentives structures.[14]

» The use of **cryptography** to ensure the security, integrity and immutability of the information recorded in the ledger and the systems by which it is managed.

What problem is blockchain solving?

To understand the capabilities enabled by blockchain, and why they add up to something innovative, it helps to understand the problem that blockchain was created to solve. On the surface, this problem may not seem like such a big deal but, as is explained below, the creation of blockchain technology actually resolved a long-standing problem in computer science in a revolutionary way.

Stated simply, blockchain solves a coordination problem for shared ledgers. Commonly, shared ledgers with multiple collaborators are vulnerable to confusion or tampering leading to errors infiltrating the ledger because it is hard to coordinate the actions of multiple users when they are acting independently. For example, one collaborator could accidentally record a transaction that another had already recorded without realizing it. Alternatively, one collaborator might make a transcription error and since no one else was checking their work, the error would go unnoticed, thus corrupting the ledger.

In some cases, these are problems people are willing to live with. Google Docs is an example of an application where multiple collaborators can make changes to a single file and where errors or disagreements can creep in. Correspondingly, users will often develop systems for how to alter such files that reduce the likelihood that problems like this will arise, for example, by requiring users to "track changes" and use "commenting" functions to propose, discuss and agree on changes before they are implemented in the file. Such systems can work well when a group is relatively small and known to each other – i.e., a trusting community – but they can also be labour

[14] Some purists would argue that permissioned blockchains are not really blockchains at all precisely because they believe that an incentive structure that employs tokens is an essential component of a blockchain. In this report, we do not take this position.

intensive and time-consuming to implement and coordinate properly. Moreover, because they depend on voluntary human actions and are not written into the application's software, such systems are subject to human error and can quickly break down when numbers grow and when anonymous users and users not known to one another begin to participate.

In trusting communities, efforts to solve coordination problems are aimed at keeping errors out of the ledger. In "trustless" communities – the aforementioned communities of anonymous users or users not known to each other – the number of potential problems expands. Users, who must still guard against honest errors, must now also guard against malicious users who are purposefully seeking to add incorrect information to the ledger and potentially seeking to defraud others. It is in these trustless communities that coordination difficulties can mutate from a simple nuisance into a serious security problem and can even block collaboration.

A common solution to the problems posed by coordination in trustless communities is to create a "trusted" intermediary and give them special powers to oversee the ledger.[15] Credit card companies represent an example: you agree to a transaction with a merchant and enter it into a terminal that transmits the proposed transaction to the card company. The company reviews the transaction to see if it appears fraudulent and to determine if the cardholder possesses sufficient credit. If all is well, the transaction is accepted, a new credit is added to the merchant's account, and a new debit to the cardholder's account. If fraud is suspected, the card company will utilize the special information it possesses to confirm whether the transaction is valid – by directly contacting the cardholder for instance. If the transaction is deemed fraudulent, the card company will use its authority over the ledger to reverse the transaction and reimburse the cardholder.

While there are benefits to such a system – refunds for defrauded cardholders for instance – there are a number of drawbacks that such intermediated systems create, including:

Gouging

The granting of special rights and privileges to a central authority creates an opportunity for that authority to overcharge users. Many believe that credit card companies and banks do just that and point to the fact that they are able to extract fees from both the cardholder and the merchant involved in a transaction and are able to make sizeable profits from this business. It is because of how these fees eat into their profits that many small business owners prefer cash or debit payments and why some even decline to accept credit cards at all.

Corruption

Systems that centralize authority enable corrupt individuals and organizations to take advantage of the privileges that their authority provides them. Land registries in countries without a strong rule of law often confront this problem as individuals may need to pay bribes to administrators in order to get their transactions processed, and administrators may steal individuals' title to their land by destroying or secretly altering the records that they maintain.

[15] For the sake of efficiency and convenience, this solution is sometimes attempted in trusting communities as well.

Single points of failure

Centralization also generates a more fundamental structural problem, namely the creation of what are called "single points of failure." These arise when a vital system is operated by, or critical information is stored by, a single entity or in a single place. The 1 June, 2018 crash of the Visa network in Europe provides a recent example of just such a failure.[16] Similarly, while users of Google Docs may be able to log on and edit their shared files from anywhere in the world, a single updated version of the document is maintained by Google. The result of this centralization of storage is that if Google's servers are taken offline by a cyber-attack or natural disaster, this can shut Google Docs down thereby temporarily blocking everyone's access to their shared document.[17]

Honeypots

Centralization, specifically of storage of users' data – something often associated with systems that centralize authority – also creates what are called "honeypots." The term honeypots refers to large accumulations of data held in a single location or database. These centralized stores of data are especially attractive to hackers because of their immense size and potential value. This makes it worthwhile for the hackers to devote significant effort and resources to breaching these stores' defences. Thus, this concentration of data often ends up resulting in massive data breaches, even from highly protected databases, a problem that is becoming increasingly common.[18]

One obvious solution to all these problems is to decentralize the system, that is, create a system where there is no central authority and multiple redundant copies of the information in question are stored in different places by different independent entities. If there is no central authority, it cannot become abusive; if there are multiple copies of the ledger, then taking one of them offline cannot stop users from accessing another copy.[19] But, while an obvious and simple solution in principle, prior to the invention of blockchain, implementing such a decentralized solution for a shared ledger was impossible in the context of a trustless world.

The "double-spend" problem

The biggest reason why no one had been able to solve this problem previously was because no one had been able to solve the "double-spend" problem.[20] To understand the double-spend problem, consider the problem in the context of a digital currency and imagine a digital unit of money which we will call a "token." Because computers are very good at copying things – and also very good at making millions of these copies at low cost – it is not possible to create value-bearing digital files that act the way a physical coin or a dollar bill acts in the physical world. Counterfeiting is simply too big a problem. One way to get around this problem, however, is to avoid bearers of value altogether and opt instead for a centralized ledger that keeps track of what everyone owns and owes. When someone wants

[16] Collinson, P. and agency. 2 June, 2018. "Visa card payments system returns to full capacity after crash." *The Guardian*. https://www.theguardian.com/money/2018/jun/01/visa-card-network-crashes-and-sparks-payment-chaos?CMP=Share_iOSApp_Other.
[17] It is true that companies like Google try to alleviate this problem by backing up files, but in principle, because these files are controlled by a single entity, they are still vulnerable to the single point of failure problem – for example, should Google go bankrupt.
[18] A recent example is the September 2017 Equifax data breach.
[19] Note that decentralized systems also tend to limit the amount of data in the copies of the shared ledgers to the absolute minimum necessary for the system to function. This makes them much less attractive targets for hackers.
[20] The double spend problem is most easily understandable in the context of a digital currency, but the same problem can be transposed to other forms of ledgers as well. In order to make the explanation as clear as possible, we concentrate on the currency-related form of this problem here.

to make a purchase, they don't exchange tokens. Instead, they simply notify the keeper of the ledger to shift some tokens from their account to someone else's. In this scenario, a token becomes less analogous to a physical thing like a coin and more like a unit for measuring how much of something you possess, like a kilogram or a millilitre.

As already discussed, this solution works well if there is a trusted intermediary to maintain the ledger and keep track of transactions. For a variety of reasons, the inventor(s) of Bitcoin and its early adopters were unhappy with the fact that such a payment system required them to rely on an intermediary.[21] Thus, the Bitcoin blockchain represents an attempt to create a functional equivalent of the sorts of ledgers that card companies use to enable electronic payments, but to do so without a centralized authority. Instead, a decentralized network would operate the ledger, thereby ensuring that no single entity would be able to exploit a privileged central position.

The problem that this creates, however, is that removing the intermediary re-introduces the double-spend problem, albeit in a different form. Without a central authority empowered to coordinate the updating of the authoritative central ledger, this network needs a new way to ensure that malicious users are not able to spend the same funds more than once by entering different transactions for their funds into the multiple copies of the ledger distributed around the network.

In other words, any decentralized system needs to find a way to ensure that all the various copies of the ledger remain consistent and are regularly reconciled in a way that reliably ensures that legitimate transactions can be distinguished from illegitimate ones and only legitimate ones accepted. Prior to the creation of the Bitcoin blockchain, no one had been able to solve this problem; blockchain's key innovation lies in how it manages to do so.

How blockchain works

Blockchain's key innovation lies in how it creates a system for coordinating the maintenance of a shared ledger by a decentralized network such that all the copies of the ledger across the network can be reliably updated in a timely manner and in a way that ensures their consistency.

How does blockchain accomplish this previously impossible task?[22] We explained earlier that blockchains are updated when a new block of transaction information is time-stamped, sealed and added to the chain of blocks that comprise the ledger. A block is simply a package of information of a pre-determined size. In principle, this information can record any sort of transaction, ranging from the transfer of ownership of a digital asset like a bitcoin to the transfer of ownership of a physical asset like a diamond that has been registered on a

[21] Bitcoin's creator(s) seem to have wanted to be able to transfer funds digitally with the same level of anonymity and ease that cash enabled in the physical world and they resented the power that the managers of existing ledgers, such as banks, enjoyed because of their privileged position – a position that also enabled them to profit from their management of the ledger. See Vigna, P. and Casey, M. 2016. *The Age of Cryptocurrency*. Chapter 2.

[22] For this section, and many of the other technical aspects of this paper, we have relied on the helpful and accessible explanation offered at Nielsen, M. 6 December, 2013. "How the Bitcoin protocol actually works." *DDI: Data-driven Intelligence*. http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ as well as the helpful comments of our anonymous reviewers.

blockchain.[23] The way this works is that when users want to make an addition to the ledger – i.e., make a transaction – they announce it to the blockchain's network. These proposals are validated and grouped together into a block and the blockchain's distributed consensus mechanism is then used to add this block to the ledger.

In the case of the Bitcoin blockchain, the consensus mechanism that is used is based on a technique called "proof-of-work" (PoW).[24] PoW is essentially a competition held between the various nodes that make up the Bitcoin network in which each node strives to be the first to guess a random number –called the nonce – that happens to solve a difficult mathematical puzzle. There is no way to find the nonce other than by guessing a number and running an equation to see if that number produces the correct answer. This "guess and check" approach, also called brute force computation, is similar to trying to open a combination lock by trying every possible combination one at a time.[25] And just like with a combination, it is easy to prove to someone else that you have succeeded in solving the problem by simply telling them the combination and having them test it themselves – which is how other nodes can check to ensure that the winner of the competition actually found the nonce.

The prize for winning the competition is actually the nonce itself which the winning node is then able to use as a special cryptographic key that enables them to seal the next block of validated updates and attach it to the rest of the blockchain (see Box 1). The various nodes on the network compete to perform this task because the node that wins the competition is rewarded with a set number of new bitcoins for doing so. Taking part in this competition – i.e., engaging in this computational work – is called "mining" and the nodes that do it are called "miners."[26]

[23] Volpicelli, G. 8 June, 2016. "Beyond bitcoin. Your life is destined for the blockchain." *Wired*. http://www.wired.co.uk/article/future-of-the-blockchain. The big difference between transferring digital and physical assets, however, is that while recording the transfer of bitcoin on the Bitcoin blockchain actually effects and completes the transfer, when recording the transfer of a physical asset that transfer must still be effected in the physical realm.

[24] PoW serves two necessary functions in the Bitcoin blockchain: on top of being a consensus mechanism, it also ensures the security of the system, as we explain below.

[25] The authors would like to thank Matt Jackson for suggesting this comparison.

[26] Note that all of this activity occurs automatically. Human involvement in the mining process is normally limited to setting up a mining "rig" – the computer or network of computers used to do the mining – and periodically checking on it to make sure it is still working properly. That said, the potential deviations described below would involve human interference with a normally automated process.

BOX 1
Hashing

Hashing is a term that refers to the use of an algorithm – called a hash function – to convert a piece of information into an alphanumeric string of characters like this:

e9ffc424b79f4f6ab42d11c81156d3a17228d6b1edf4139be78e948a9332d7d8

Hashing is a commonly used technique in computer science and cryptography. Hashes are useful because they possess a few important properties. First, hashes are extremely sensitive to any change in the information from which they were generated. For instance, if the hash above was the result of the text of a book being hashed, the simple act of removing even a single period from that text and then hashing the text again would result in the generation of an entirely new and unpredictably different string of characters.

Second, some hash functions – such as SHA-256, the hash function used by Bitcoin but also many other common digital applications – are very useful for cryptographic purposes. While it is easy to apply the function to a piece of information and generate a hash, it is essentially impossible to do the inverse and figure out what the underlying information is simply by inspecting the hash itself. Thus, if you have access to the underlying information used to generate a hash, it is easy to determine if the person who generated it does as well, while if you only have the hash itself, you will be unable to determine what that underlying information actually is.

In the Bitcoin blockchain, hashing plays a critical role. The number guessing competition that constitutes mining is actually a competition to guess a number (called the nonce) that, when added to the transactions in the proposed block and hashed using the SHA-256 hash function, will generate a hash starting with a specific number of zeros. The specific number of zeros required is automatically set by the Bitcoin software and varies depending on the "hashrate" of the Bitcoin network. The "hashrate" of the network is a measure of how much computing power is being devoted to maintaining the network at that particular point in time. The Bitcoin software automatically varies the difficulty of the competition depending on the network's hashrate so as to maintain an average interval between block creation of about 10 minutes.[27]

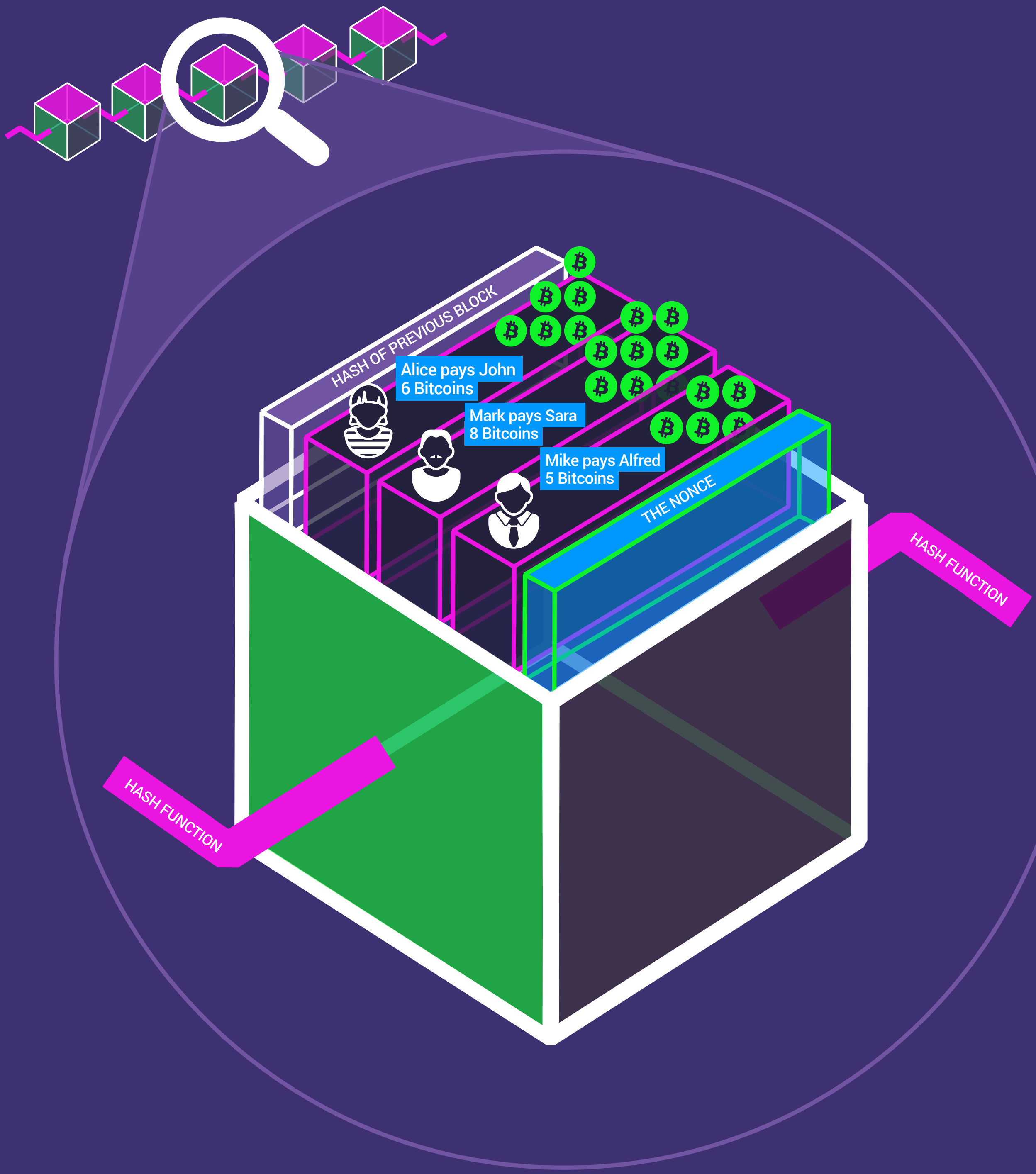
Once the nonce has been guessed correctly, it is then hashed again alongside the transaction information for the block being sealed and the hash of the preceding block (see Figure 2). It is in this way, namely hashing all the information in a block and then using this hash as a part of the information that produces the next block, that Bitcoin makes itself essentially tamper-proof. Any attempt to go back in time by tampering the record of historical transactions will alter the underlying information of the hash of the block in which this transaction was recorded, thereby invalidating the hashes of subsequent blocks and breaking the chain.[28]

[27] In reality, the average time per block has been slightly below 10 minutes for most of Bitcoin's history. See https://data.bitcoinity.org/bitcoin/block_time/all?f=m10&t=l.

[28] For a more detailed explanation of hashing see 3Blue1Brown. 7 July, 2017. "Ever wonder how Bitcoin (and other cryptocurrencies) actually work?" *YouTube*. https://www.youtube.com/watch?v=bBC-nXj3Ng4 and Nielsen, M. 6 December, 2013. "How the Bitcoin protocol actually works."

FIGURE 2

Blockchain detail


HASH OF PREVIOUS BLOCK
Alice pays John 6 Bitcoins
Mark pays Sara 8 Bitcoins
Mike pays Alfred 5 Bitcoins
THE NONCE
HASH FUNCTION
HASH FUNCTION

This mathematical puzzle is important because it serves three key functions:

- It makes participation in the competition costly by requiring participating nodes to dedicate significant computing power to maintaining the network.
- It yields an answer that is easy to confirm after the fact but essentially impossible to uncover without winning the competition.
- Because the nonce can only be found by guessing random numbers, it is basically impossible to predict who will win any given round of the competition, thereby randomizing which miner gets to seal each block.

While dedicating additional computing power to finding the nonce will improve a miner's chances of winning, doing so does not guarantee victory – especially because all the other competitors are trying to do so as well. In other words, the competition is like a lottery and while adding computational power will improve a miner's odds of winning because it will allow them to guess and check more numbers more quickly – similar to buying additional tickets – the winner of the competition will still be determined by random chance.

Once a miner finds the nonce and seals the block, the next step is to broadcast this new block to the rest of the network. It should be noted that prior to sealing the block, prior even to searching for the nonce, the miner will have automatically validated all the pending transactions that it had gathered to put into this new block. The process of validation is fairly straightforward and consists of the copy of the Bitcoin software that operates the miner's node checking to see if there are any inconsistencies within the proposed transactions that make up the proposed block. For example, the Bitcoin software does not allow a user to transfer the same asset to more than one other user simultaneously (an obvious form of double-spending). Nor would it validate proposed transactions that are inconsistent with the pre-existing state of the database – e.g., a user attempting to transfer an asset that they do not own.

Once they have sealed the block, the winning miner broadcasts this new block to the rest of the network and each of the other miners update their copies of the blockchain by adding this new block. Before doing so, however, each miner will independently verify that the solution that the competition winner found to the mathematical puzzle is correct and that the additions to the blockchain proposed in the new block are compatible with their copies of the blockchain. This step is important because technically the winner of the competition could try to introduce improper transactions that benefited them into the blockchain when they seal the block and broadcast it to the rest of the network. But any such attempt would immediately be noticed by the other nodes when they received the proposed new block with the result that this new block would be promptly rejected by the network and the process would be re-run. Because it is so easily caught, attempts like this are not a regular occurrence.

What the fork?

One of the interesting things about Bitcoin is that, while a new block is created every ten minutes, most users of Bitcoin do not consider a transaction to have been completed until an additional five blocks have been added to the blockchain. In order to understand why this is the case, we need to explain one additional feature of blockchains, namely something called "forking."

Because blockchains are maintained by a decentralized worldwide network of computers, it is possible for more than one node on the network to independently solve the mathematical puzzle and win the competition to seal the next block at basically the same time. When this occurs, more than one node will broadcast a new block to the network essentially simultaneously. While communication between nodes takes place very quickly, it is not instantaneous because geographical location, routing of the information on the Internet, and the quality of the transmission infrastructure will impact transmission speed. Thus, the spreading of new blocks across the network will proceed unevenly and at different rates. This uneven spreading can result in a situation where multiple nodes on the network may accept one new block while other nodes, having received an alternate new block from a different node first, will have accepted a different block and added it to their blockchains.

The Bitcoin software manages this "forking" of the blockchain – the name given to situations when the blockchain has been split into multiple branches as just described – by using the following rule: all nodes simultaneously keep track of both branches of the chain but only work on extending the branch containing the new block that they accepted first. The result is that there are temporarily two competing versions of the blockchain (see Figure 4).

FIGURE 3

Normal blockchain growth

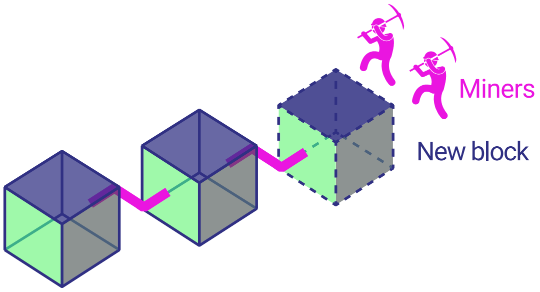
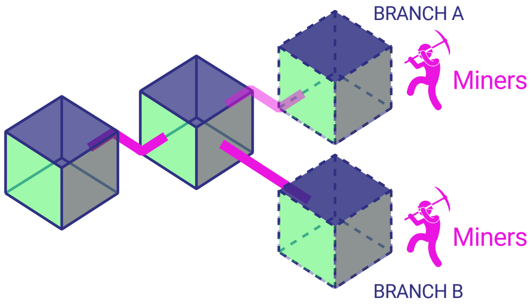


FIGURE 4

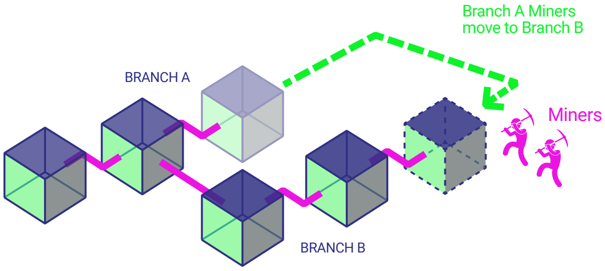
Forked blockchain



Normally, however, this competition between branches does not last long because the Bitcoin software contains another rule designed to resolve it: the longest branch of the blockchain is considered the official branch and miners should only work on extending the official branch. Thus, as soon as one of the competing branches successfully adds another block to the chain, this now longer branch becomes the official branch. Once nodes that were working on the other, now shorter, branch are informed that there is now a longer branch, they will automatically stop working on extending the shorter branch and transfer their attention to the now official branch (see Figure 5). The blocks in the shorter chains that have been abandoned are called "orphan blocks."

FIGURE 5

Forked blockchain being resolved

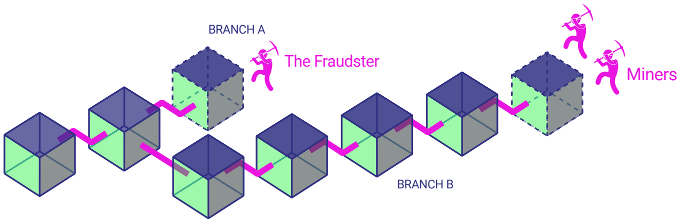


While not unusual or problematic, forking does enable the double-spend problem to re-emerge in a new form. In this context, double-spending refers to a scenario in which a fraudster completes a transaction with another user and then, at some point later in time after they have secured the benefit of this first transaction – say taken possession of the pizza they purchased through that transaction – seek to remove the record of this transaction from the blockchain. In other words, by erasing the record of their transaction, they are seeking to destroy the evidence that it occurred and return the official blockchain to the state that existed before they transferred the bitcoins used to make the purchase out of their account, thereby allowing them to spend these same bitcoins again in the future. The result would, in some ways, be similar to passing a bad cheque.

The way that a fraudster would try to do this is by waiting until they have secured the benefit of the transaction and then return to a point on the blockchain, usually the block just prior to the one in which the transaction in question was recorded, and then fork the blockchain by proposing a new block in which that transaction no longer exists.[29] In other words, the fraudster would go back in time on the blockchain and propose a new block that contained a new transaction history for the bitcoins in question in which they never transferred these bitcoins to their counterparty. The idea being that if they can get the rest of the network to accept this new transaction history they can recover the funds they spent while still enjoying the benefits of the transaction.

FIGURE 6

Attempt to fork a blockchain retroactively



The only way that such a manoeuvre would be successful is if the fraudster were somehow able to convince the rest of the network that their new and fraudulent branch of the blockchain should be accepted as the official branch. Otherwise the fraudster would simply be operating their own private branch of the blockchain with no one else paying any attention to them or engaging in any transactions with them. Essentially, it would be a bit like trying to spend your own homemade currency at the grocery store.

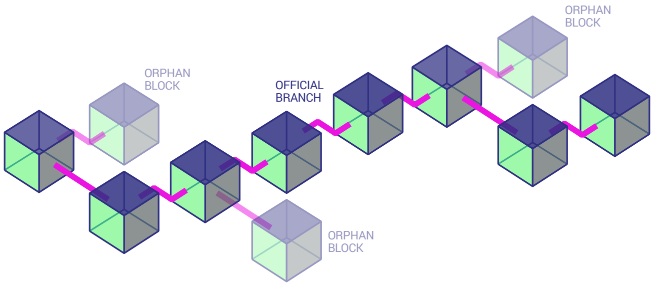
[29] Note, in this scenario all the other transactions in the block would remain the same – only the transaction of interest to the fraudster would be altered.

To be successful, the fraudster would need to extend their new fraudulent branch of the chain such that it overtakes the legitimate chain – the one that includes the original transaction – in length. While theoretically possible, the Bitcoin blockchain is specifically designed to make such a scenario essentially impossible. The main defence that is built into the Bitcoin blockchain is PoW. While it is possible for anyone to fork the Bitcoin blockchain at any time, once they have created the first block in the new branch, they will have to seal each subsequent block in this new chain themselves. This is because, until they overtake the official branch the rest of the network will still be focused on extending the longer official chain.

Given that the difficulty of finding the nonce will be the same for the fraudulent actor and the rest of the network against which they are still competing, it is tremendously unlikely that the fraudster will be able to seal enough blocks fast enough to overtake the original branch and displace it as the official branch.[30] While they could reasonably expect to get lucky and seal a block or two faster than the rest of the network, being able to do so for an extended period of time becomes so unlikely as to be essentially impossible. That is why users of the network usually wait until five additional blocks have been added to the chain before assuming that their transaction has been completed: the assumption is that once that many blocks have been added, it is so improbable that the transaction could be overtaken by a fraudulent branch of the blockchain that they can now rest assured that it has been permanently added to the blockchain.

FIGURE 7

Blockchain with forks and orphan blocks



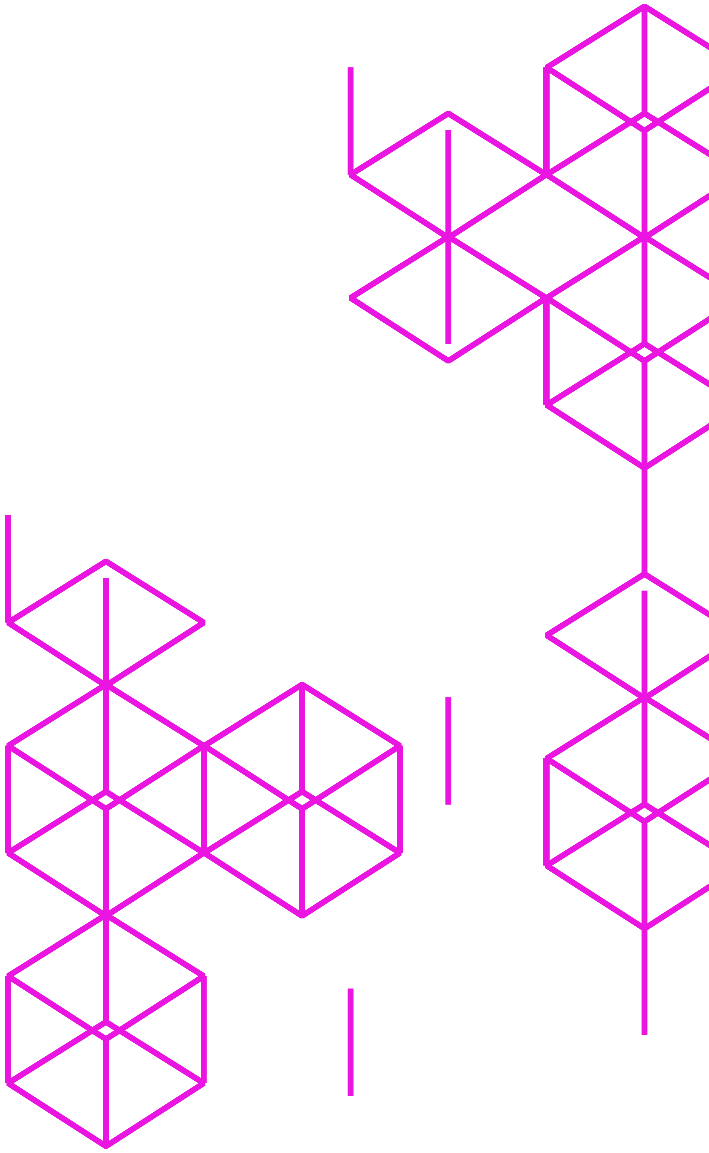
Why mine?

A final key point to note about blockchain design is the role played by the distributed P2P character of the network. The consensus mechanism relies on the fact that each node has access to its own copy of the blockchain to ensure that whoever wins the competition is able to independently validate the new block of transactions. This makes it is essentially impossible to corrupt the ledger by hacking it. In the first instance this is because, given that each block in the chain contains a hash of the preceding one, it is essentially impossible to alter the record as doing so would break the modified block's connection with subsequent blocks and create a fork in the chain (see Box 1). Additionally, the fact that each node has its own copy of the ledger means that it would be simply too difficult to simultaneously hack enough nodes for the hacker to be able to alter sufficient copies of the ledger to overwhelm the non-corrupted versions of the blockchain.

[30] The integrity of this system would be threatened, however, if a single entity came to control a sufficiently large percentage of the computing power dedicated to the network that they could, essentially, guarantee their ability to win the lottery. This hypothetical problem is referred to as a "51 per cent attack," though there are some who argue that one could probably mount such an attack with less than 51 per cent of the network's computing power. At the moment, the Bitcoin blockchain does not appear to be vulnerable in this way. For a more in-depth discussion, see Hertig, A. 8 June, 2018. "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular." *Coindesk*. https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/. and Eyal, I and Gün Sirer, E. No date. *Majority is not Enough: Bitcoin Mining is Vulnerable*. Cornell University. https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf.

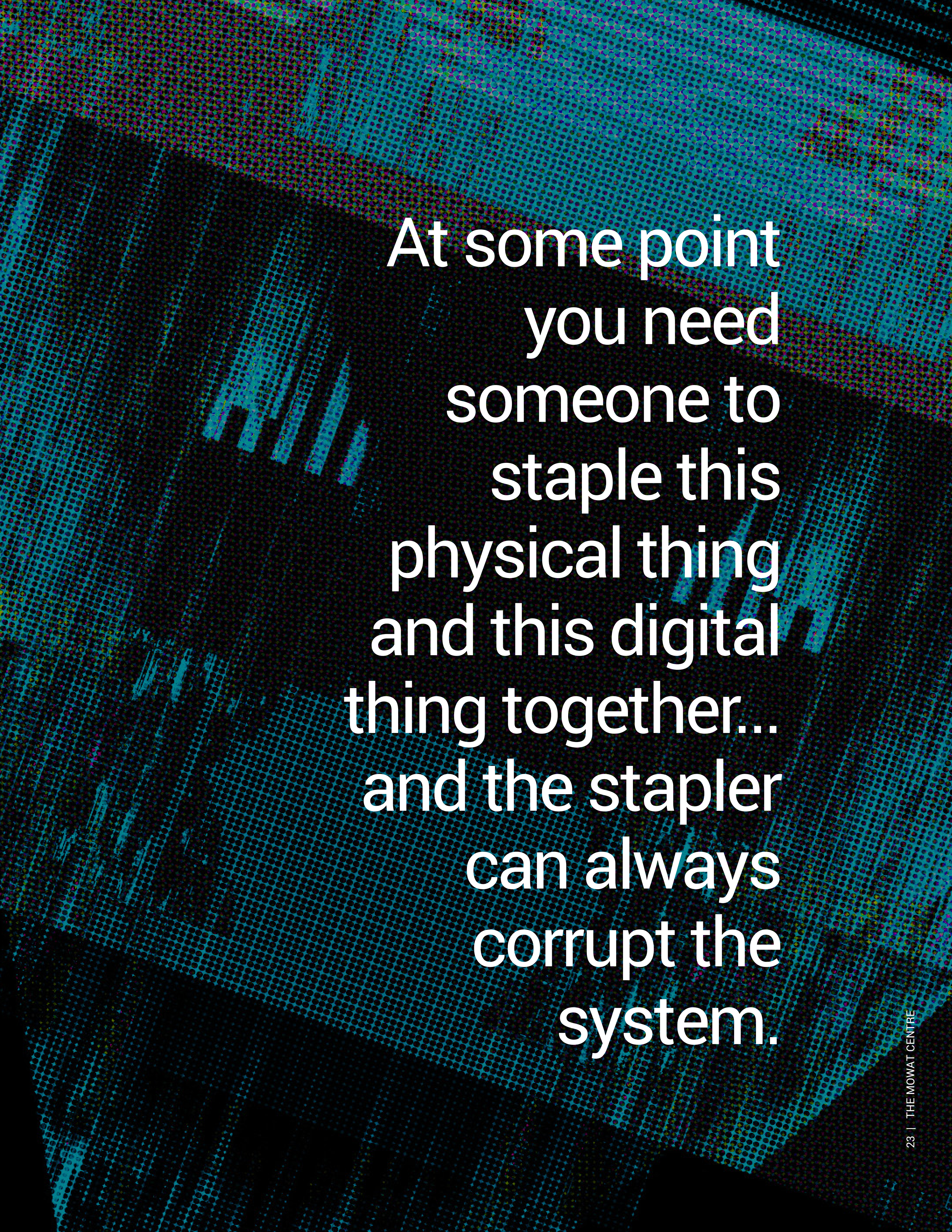
The major drawback to this otherwise ingenious scheme for preventing corruption of the ledger is that the entire system relies heavily on redundancy and is thus quite inefficient. The difficulty of winning the competition to seal the next block is automatically tied to the amount of computing power that nodes have dedicated to maintaining the network. While it was initially possible to successfully mine bitcoins using only a standard laptop computer, the amount of computing power competing to seal the next block, and the costs involved in purchasing the electricity to enter this competition, are now so high that attempting to mine bitcoins using anything other than specially designed hardware is a money losing proposition.[31]

But, if participating in this competition is expensive, why does anyone compete? The answer is twofold. First, blockchains usually include a system that incentivizes participation by providing the winner of the competition with a reward, usually in the form of a token. In the Bitcoin blockchain, this reward is a set number of bitcoins.[32] Second, when users notify the network of their proposed update and request that it be included in the next block, they can also offer a fee for processing their update. During the first few years of its operation, these fees were minimal or non-existent on the Bitcoin blockchain. But as the volume of updates has grown there are now often more proposed updates than space for these updates in many blocks. Thus, users will now often offer modest fees alongside their proposed transactions in order to induce miners to include their proposed transaction in a block in a timely manner. Thus, between mining new bitcoins and receiving transaction fees, Bitcoin miners are provided with an incentive to maintain the decentralized system.



[31] Eventually this energy intensity may force the adoption of alternative consensus mechanisms by Bitcoin and other blockchains. Ou, E. 7 December, 2017. "No, Bitcoin Won't Boil the Oceans." *Bloomberg*. https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think.

[32] Initially, the reward for successfully sealing a block was 50 bitcoins. Interestingly, the Bitcoin software is set such that the reward decreases by half about every four years. Currently, the reward sits at 12.5 bitcoins (worth, at the time of this writing, over $130,000 CAD). Eventually, the reward will decrease to nothing with the 21 millionth, and final, new bitcoin likely appearing sometime around 2140, depending on what the average time required per block actually ends up being.



At some point you need someone to staple this physical thing and this digital thing together... and the stapler can always corrupt the system.

3 THE FIRST DIGITALLY NATIVE VALUE SYSTEM

With this understanding of how blockchain functions in place, we can shift our focus to the potential implications of this new technology. As was mentioned earlier, applications for blockchain technology are being proposed, developed and launched across an increasingly diverse array of sectors ranging from personal digital identity management, to electricity grids,[33] to digital pet breeding games.[34]

In subsequent sections we highlight a few of these applications. Before diving too deeply into specific applications, however, it is important to first get to grips with the fundamental innovations introduced by blockchain which underpin these new applications. Thus, in this section, we focus on the two key dimensions along which blockchain's impact will likely flow, namely automation and decentralization.

Digital commerce

Before examining these two key dimensions, however, it is useful to quickly review the context into which blockchain is emerging and illuminate the significant changes to this context it may trigger.

Enthusiasts often suggest that blockchain is important because it creates an "Internet of Value" in the same way that the worldwide web created an "Internet of Information."[35] Similarly, others suggest that blockchain is the "distributed trust network that the Internet has always needed but never had."[36] Care should be taken with these catchy turns-of-phrase, however, as it is often unclear what they actually mean or what the implications of an "Internet of Value" might be. After all, we can already transfer value across the Internet fairly easily – as shown in Figure 8, digital commerce is already booming.

[33] Briggs, L. 2 December, 2016. "NEWS: Energy May be Ripe for the Sharing Economy, Thanks to Bitcoin's Blockchain Technology." *Advanced Energy Perspectives*. http://blog.aee.net/news-energy-may-be-ripe-for-the-sharing-economy-thanks-to-bitcoins-blockchain-technology.

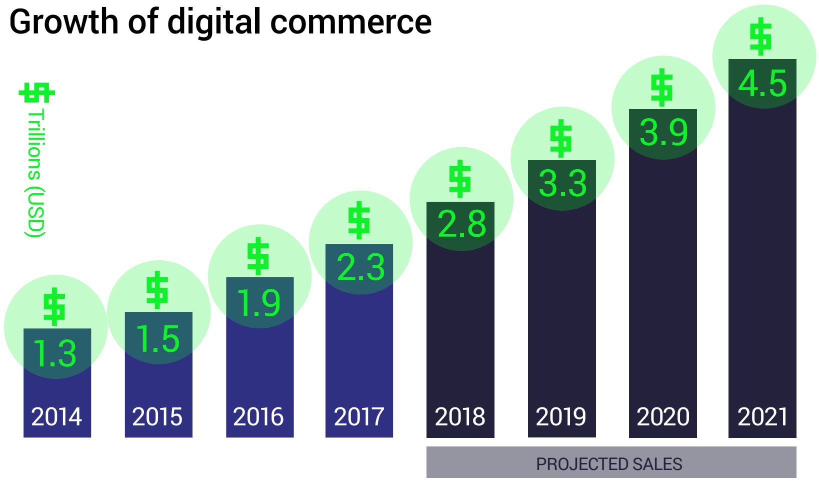
[34] See https://www.cryptokitties.co/.

[35] Hasse, F. von Perfall, A. Hillebrand, T. Smole, E. Lay, L. Charlet, M. 2016. Blockchain – an opportunity for energy producers and consumers? *PwC*. https://www.pwc.com/gx/en/industries/energy-utilities-resources/publications/opportunity-for-energy-producers.html. Page 40.

[36] Marc Andreessen, quoted in Tapscott, D. and Tapscott, A. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World*. London: Portfolio Penguin. Page 5. This is a confusing quotation as the great innovation of blockchain is not that it creates a network of trust, but rather, that it eliminates the need for trust.

FIGURE 8

Growth of digital commerce



Source: Orendorf, A. 1 September, 2017. *Global Ecommerce: Statistics and International Growth Trends [Infographic]*. ShopifyPlus. https://www.shopify.com/enterprise/global-ecommerce-statistics and Statisa. 2018. "Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars)." *E-Commerce*. Statisa. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

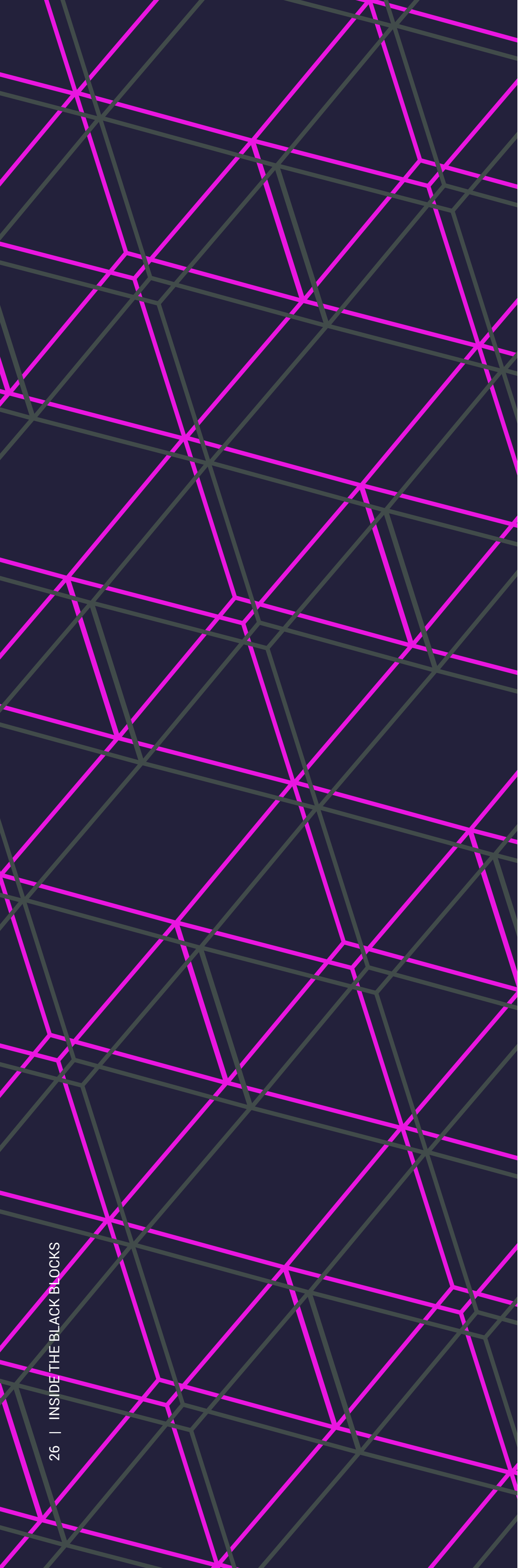
What is special about blockchain is how it has enabled, for the first time, the creation of what we call the first "digitally native value system." More than anything else, it is this innovation that stands to enable blockchain's most revolutionary consequences.

The key difference between existing forms of value that can be transferred digitally and blockchain-enabled forms of digital value is that unlike existing forms – such as "fiat" currencies (see Box 2) like dollars, euros, yen – which are only represented digitally, blockchain allows the creation of forms of value that are *intrinsically digital*. Most existing systems of value are created and controlled through legislation. These currencies derive their value from a system of laws that exists independent of the digital realm. This means that any digital representation of these forms of value is only the *representation* of an original version which is ultimately controlled and defined by that other system. Alternatively, blockchain-enabled assets are *originally* digital and are controlled and defined by software. Their existence is a function of the digital system they are embedded in, impossible outside of this context and independent of any national system of laws.[37]

BOX 2
Fiat Currency

The term "fiat currency" refers to the money, such as Canadian dollars, that we currently use and which have value only because some entity, such as a government or central bank, has declared them to have this value. This value is usually substantiated by an individual's ability to pay the taxes owed by them to said government in currency backed by this government. Fiat money has no independent intrinsic value, as opposed to representative currency (where money represents a claim on a commodity, usually held by a government) or commodity money (where the money has intrinsic value by dint of the usefulness of the commodity, often a precious metal, out of which it is made).

[37] For an in-depth discussion of the legal character of Bitcoin and the difficulties involved in understanding it using traditional legal concepts, see Szilagyi, K. 2018. "A Bundle of Blockchains? Digitally Disrupting Property Law." *Cumberland Law Review*. 48(1) 9-34.



This is new and profoundly important. Digitally native value systems represent a potentially tremendous disruption to the institutions that currently manage the connection between existing digital representations of existing forms of value and their physical and legal anchors. These intermediary institutions, which derive considerable power from their roles as such, are currently necessary because, as one of our key informants put it, "at some point you need someone to staple this physical thing and this digital thing together... [and] [t]he stapler can always corrupt the system."[38] When a form of value is inherently digital, however, this is no longer true because the stapler is no longer necessary. Consequently, those currently holding the stapler stand to lose a great deal of their power.

While much has been made of the disruptive potential that blockchains possess *vis-à-vis* traditional financial institutions, this potential disruption is just one of many possible repercussions of the even more fundamental shift that the advent of digitally native value systems entails. Indeed, the most significant result that is likely to emerge from blockchain's creation of digitally native value systems lies in how the novel characteristics of these systems will enable new areas of economic activity that were not previously possible.

[38] Corruption is perhaps a strong word, but the point is clear. Banks and governments exercise tremendous power over the existing financial system, but this power is often hidden. Only rarely, for instance when the Greek government and the country's banks effectively froze Greeks' bank accounts in 2015 and limited them to a maximum of only €60 worth of withdrawals a day, does this power become obvious. The Associated Press. 29 June, 2015. "Greece in limbo as it shuts banks, puts limits on cash withdrawals to avoid financial collapse." *The National Post*. http://business.financialpost.com/news/economy/greece-in-shock-as-banks-shut-after-creditor-talks-break-down.

BOX 3
Digital Assets

According to *Investing.com* there are now more than 1,900 “cryptocurrencies.”[39] While many of these, such as Bitcoin, are best understood as something akin to a traditional currency, for many of these assets the term “cryptocurrency” is actually misleading as it implies a level of homogeneity among these assets that does not exist. Increasingly, the terms “crypto assets” or “digital assets” are being used as a way of referring to this universe of distinct digital tokens.[40]

In an attempt to organize this expanding universe, Don and Alex Tapscott have developed an initial typology that divides this new class of assets into seven categories.[41] Drawing on their work, we define each of these categories below and provide examples of particular tokens for each category. It is important to note, however, that this list is offered as a helpful guide and is by no means definitive or exhaustive. The divisions between these categories are blurry as many are still emerging and evolving, and any attempt at such categorization will need to be amended in the months and years to come.

CRYPTOCURRENCY

A blockchain-based system of digital cash money that serves as a P2P medium of exchange, store of value and unit of account and which uses cryptographic techniques to generate new units of money and to secure the system against corruption. Cryptocurrency has no physical form and exists only on the network. Units of different cryptocurrencies can be exchanged for each other or exchanged for fiat currency. This money-changing usually occurs at cryptocurrency “exchanges,” institutions that act like digital foreign currency exchanges. Bitcoin is the most well-known cryptocurrency, but other cryptocurrencies that focus on providing specific functionalities such as Zcash (improved privacy) or Litecoin (faster transaction confirmations) also exist.

PLATFORM TOKENS

Similarly to cryptocurrencies, platform tokens are units of value within digitally native value systems. Unlike cryptocurrencies, which are specifically designed to enable secure digital payment systems, platform tokens are designed to serve as value systems for general purpose blockchain-based software platforms capable of supporting additional functions beyond payments. Ether, the token that is native to the Ethereum platform, is the most well-known of these tokens. Ethereum, a blockchain that emerged out of its creators’ frustration with the Bitcoin blockchain’s limited ability to support applications other than digital payments, was designed to provide users with the ability to run “smart contracts” (business logic and agreements encoded in software - see Box 4) – and DApps (decentralized applications, i.e., software programs like Bitcoin that run on a decentralized P2P network) on its network. The role of the ether token, which represents an entitlement to the use of some of the Ethereum network’s decentralized computing power – often called “gas” – is a component of an internal pricing system used to allocate the computing power of the network.

[39] See https://ca.investing.com/crypto/currencies This estimate was made on 26 July, 2018.
[40] Garner, B. 14 February, 2018. “What is Storj? | Beginner’s Guide.” *CoinCentral.* https://coincentral.com/storj-beginners-guide/.
[41] Tapscott, A. 28 March, 2018. “Crypto Summit 2018 | Alex Tapscott: Global State of Crypto.” *YouTube*. https://www.youtube.com/watch?time_continue=1602&v=YM4EwxQ3eFY.

UTILITY TOKENS

Like cryptocurrencies and platform tokens, utility tokens are also units within digitally native value systems. Contrary to platform tokens, which are native to general purpose decentralized computing systems, utility tokens serve as units of value within the digital value systems created by specific DApps. Thus, while a DApp might require a platform token such as ether to pay nodes on the Ethereum network for the computational work they perform to run the DApp, users of the DApp would need to spend or hold that DApp's native utility token to participate in the activities of that DApp. Storj, a decentralized cloud storage DApp that runs on the Ethereum network, is one such example. Storj users who want to store data (called tenants) upload data to the cloud through the Storj DApp. Storj processes this data and deposits it with users who have spare storage capacity (called farmers). Tenants whose data is being stored pay the farmers who are storing their data using Storj's native utility token.

SECURITY TOKENS

Security tokens are best understood as securities – such as stocks or other equities – issued digitally on a blockchain platform. In other words, security tokens are tokens that constitute an "investment contract" and thus meet the legal criteria used to define a security. These criteria are often referred to in the USA as the "Howey Test" or, in Canada, by the name of the court case (Pacific Coast Coin Exchange v. Ontario Securities Commission) that imported a slightly wider version of the Howey Test into Canadian law. Essentially, according to this test, a token is a security if it involves:

» an investment of money

» in a common enterprise

» with the expectation of profit

» to come significantly from the efforts of others[42]

There are many potential advantages to issuing securities on a blockchain, such as faster clearing and settling of transactions, better tracking of ownership, and other features enabled by the fact that these tokens, unlike paper share certificates, are programmable, meaning they can be controlled by software.[43]

NATURAL ASSET TOKENS

While similar to security tokens in that they represent an entitlement to the ownership of an asset, natural asset tokens represent ownership of a physical asset, such as a specific amount of gold or oil, instead of an intangible asset like a share in a company. Alex Tapscott suggests that these tokens might be most useful in creating or advancing what he calls "frontier markets" in physical assets like atmospheric carbon emissions. Indeed, some interviewees told us that some governments are already examining the possibility of using blockchains to implement carbon pricing systems.

[42] Canadian Securities Administrators. 24 August, 2017. "Cryptocurrency Offerings." *CSA Staff Notice 46-307*. http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm.

[43] Currently, however, many existing securities tokens have likely been issued without meeting many of the requirements, such as the issuing of a regulator-approved prospectus, that have been set by securities regulators. Consequently, many of these token are likely illegal offerings.

DIGITAL COLLECTIBLES

In much the same way that the creation of blockchain technology solved the double-spend problem for digital currency, its creation of “digital scarcity” is now enabling the production of unique non-replicable digital collectibles. The most well-known of these are CryptoKitties which exist as tokens in a blockchain-based game in which players are able to collect and breed unique digital “cats.” Other collectibles have started to emerge, such as the ability to buy a share of a musician’s song[44] or digital trading cards. Indeed, impressed by the success of CryptoKitties, Major League Baseball announced that it will soon launch a blockchain-based game involving crypto-collectible avatars from significant moments in baseball history which users will be able to collect and trade with each other.[45] The market for digital collectibles may be larger than one would initially imagine: in computer gaming circles, the sale of fraudulent digital items such as in-game weaponry – which for our purposes count as collectibles – is a major problem in a growing market already worth 15 billion USD.[46]

CRYPTO-FIAT CURRENCIES OR STABLECOINS

Given how the current volatility of cryptocurrencies has undermined their usefulness as a medium of exchange, some have suggested that governments could issue a digital fiat currency on a blockchain as a means of overcoming this problem. The idea would be that such a currency would marry many of the advantages of a fiat currency, such as the stability that can derive from government backing, with many of the advantages of a cryptocurrency, such as faster transaction speeds and the ability to easily transfer money across borders. Stablecoins, such as Tether, seek to achieve much the same result by creating a system whereby the value of a token is pegged to a specific physical asset like gold or oil or even to an existing fiat currency.[47]

[44] Krewen, N. 10 December, 2017. “Want to buy a piece of a Drake song? Track’s rights sold via pioneering digital currency scheme.” *The Toronto Star*. https://www.thestar.com/entertainment/music/2017/12/10/want-to-buy-a-piece-of-a-drake-song-tracks-rights-sold-via-pioneering-digital-currency-scheme.html.

[45] Kelly, M. 13 July, 2018. “MLB will release a crypto baseball game on the blockchain.” *The Verge*. https://www.theverge.com/2018/7/13/17568766/mlb-cryptocurrency-baseball-game-summer.

[46] Casey, M and Vigna, P. 2018. The Truth Machine. Page 96. An important innovation that sets blockchain-based collectibles apart from other digital ones is that they exist on a decentralized network and are thus less vulnerable to the single point of failure problem that exists for other digital items, such as collectibles in online games run by a single company like World of Warcraft. Wong, J. 4 December, 2017. “The ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain.” *Quartz.* https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion/.

[47] Venezuela’s petro, a digital currency that it began issuing in February 2018 and which it claims is backed by Venezuela’s oil reserves, appears to represent some combination of these two ideas, but it may also be a scam designed to circumvent international financial sanctions. Laya, P. “Crypto Rating Sites Are Already Calling Venezuela’s Petro a Scam.” *Bloomberg.* https://www.bloomberg.com/news/. articles/2018-04-03/crypto-rating-sites-are-already-calling-venezuela-s-petro-a-scam and Karsten, J. and West, D. 9 March, 2018. “Venezuela’s “petro” undermines other cryptocurrencies – and international sanctions.” *TechTank*. The Brookings Institute. https://www.brookings.edu/blog/techtank/2018/03/09/venezuelas-petro-undermines-other-cryptocurrencies-and-international-sanctions/.

New forms of economic activity

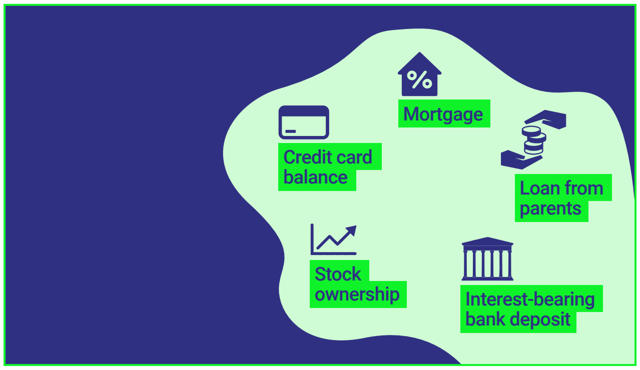
Some commentators compare the invention of blockchain to the invention of double-entry bookkeeping. Often, this comparison is designed to highlight the foundational importance of blockchain but also to caution readers not to expect too much from blockchain too soon. After all, while double-entry bookkeeping may have enabled the development of modern capitalism, it took hundreds of years before the practice became a ubiquitous backbone technology of commerce.[48]

Another analogy that may be better at illustrating how blockchain can enable novel forms of economic activity is to consider how other new developments, such as the invention of joint stock companies, did so when they were launched. The creation of these technologies enabled a new class of enterprises to raise capital in innovative ways and to create business models and businesses that were not previously viable. These new economic entities also opened up previously restricted commercial opportunities to a wider percentage of the population than ever before and helped to spur significant wealth creation and economic growth.

Josh Stark, a lawyer and blockchain entrepreneur, illustrates this idea by using a concept that he calls the "space of possible economic relationships."[49] We have adapted his graphical representation of this concept in Figures 9-12.

FIGURE 9

Space of possible economic relationships, circa 2007



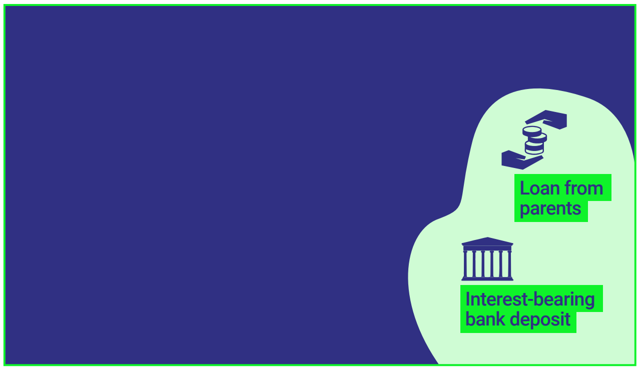
The space illustrated in Figure 9 represents all economic relationships between individuals that could theoretically exist. The portion of the space in the bottom right-hand corner – coloured light green and encompassing the five icons – represents all the economic relationships that were actually available at the level of technology that existed prior to the invention of blockchain technology. The five icons represent illustrative examples of the many potential relationships available within that portion of the space. Because of how technology changes over time, the size of this space of possible economic relations also changes as the level of technological development changes. For example, Figure 10 represents the space of possible economic relationships as well as the actual relationships available to the ancient Romans. Notice how it is smaller and more limited in examples than Figure 9.

[48] The Economist. 15 July, 2017. "Disrupting the trust business." *The Economist*. https://www.economist.com/news/world-if/21724906-trust-business-little-noticed-huge-startups-deploying-blockchain-technology-threaten.

[49] Stark, J. 26 July, 2018. *The Space of Possible Economic Relationships*. Medium. https://medium.com/@jjmstark/the-space-of-possible-economic-relationships-bca4511fa88b.

FIGURE 10

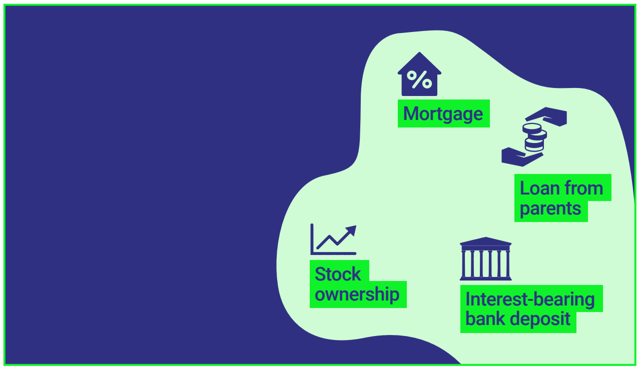
Space of possible economic relationships in ancient Rome, circa 200



Over time, technology developed and new innovations arrived making more of this space available. In Figure 11, we illustrate how the space had evolved and expanded by the mid-1800s.

FIGURE 11

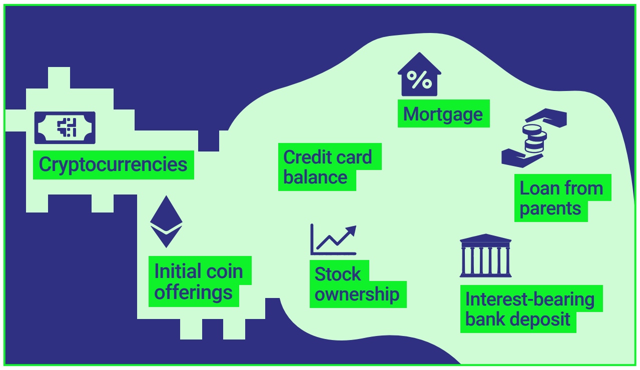
Space of possible economic relationships in Victorian England, circa 1850



As is shown in Figure 12, the advent of blockchain is further increasing the proportion of the space of possible economic relationships that is available as new inventions such as cryptocurrencies and initial coin offerings (ICOs) emerge.

FIGURE 12

Space of possible economic relationships, circa 2018



ICOs provide good examples of how the sort of expansion described in these figures is occurring as well as its potential impacts, both good and bad. ICO proponents argue that they offer an easier way for investors to raise funds than through existing sources like angel investors and venture capitalists. They also argue that ICOs are more democratic and fair because of how they provide retail investors anywhere in the world with the opportunity to invest in exciting new technologies at the ground level, an opportunity previously reserved for well-connected and already wealthy accredited investors.

BOX 4
Initial Coin Offerings (ICOs)

An ICO is an unregulated sale of digital coins or tokens generally used by blockchain start-ups and entrepreneurs to raise funds for their ventures. Sometimes these coins have characteristics, such as voting rights or the right to use a service offered on that blockchain, associated with them. The purchase of the tokens sold in an ICO is usually made using one of the most popular cryptocurrencies such as bitcoin or ether. The term ICO is modelled after the term IPO, or Initial Public Offering, which refers to the raising of investment capital by a private corporation through the regulated sale of stock to the public for the first time. ICOs are controversial because of their unregulated nature and are banned in some countries such as China. In other countries, regulators have warned consumers that many of the tokens sold in ICOs may constitute illegal securities. Other jurisdictions, such as Singapore, Hong Kong and Switzerland are more accepting and accommodating of ICOs.

ICOs have proven both popular and lucrative as it is estimated that in 2017, entrepreneurs raised more funds through ICOs than from traditional early-stage venture capital.[50] This is not necessarily a positive development, however, as ICOs have their shortcomings. Many ICO projects may never deliver any real results, and a few will be outright scams or frauds.[51] Moreover, given the terms of some ICOs, these tokens may in fact constitute securities in a legal sense, meaning that, in order to be legal offerings, they must comply with the same disclosure and other regulatory requirements as traditional securities. Many ICOs are likely illegal given their failure to do so.[52] But just as it was not worth abandoning joint stock companies as a financial tool because of early failures like the catastrophic Darien Scheme[53] or frauds like ones that helped produce the South Seas bubble,[54] the fact that an ICO can be misused or can fund a project that ends up being bungled does not mean that the instrument is itself necessarily flawed or irredeemably compromised.

[50] The Economist. 9 November, 2017. “The meaning in the madness of initial coin offerings.” *The Economist*. https://www.economist.com/news/leaders/21731161-there-ico-bubble-it-holds-out-promise-something-important-meaning.

[51] Higgins, S. 15 February, 2018. “CFTC Joins SEC In Warning Against Crypto Pump-and-Dumps.” *Coindesk*. https://www.coindesk.com/cftc-joins-sec-warning-crypto-pump-dumps/.

[52] Rawle, G. and Rizvi, Z. 7 September, 2017. “Cooling the Blockchain Boom: CSA Staff Narrow the Path for Cryptocurrency Offerings.” *Bulletin*. Davies Ward Phillips & Vineberg LLP. https://www.dwpv.com/en/Insights#/article/Publications/2017/CSA-Staff-Narrow-Path-for-Cryptocurrency-Offerings.

[53] Carroll, R. 11 September, 2007. “The sorry story of how Scotland lost its 17th century empire.” *The Guardian*. https://www.theguardian.com/uk/2007/sep/11/britishidentity.past.

[54] President and Fellows of Harvard College. No date. “South Sea Bubble Short History.” *South Sea Bubble Resources in the Kress Collection at Baker Library*. Harvard Business School. https://www.library.hbs.edu/hc/ssb/history.html.

ICOs are still a very new means of raising capital and thus it is not yet possible to know exactly which of their features will become significant. One example of how this innovation can create new types of economic relationships lies in the ability of platform and utility tokens to create new incentive structures for token holders – as opposed to the incentive structures that exist for holders of traditional securities. Indeed, contrary to a cryptocurrency, proponents argue that many tokens are better understood as similar to a license or a coupon that confers the holder with the right to use a company's service or platform in the future.[55] Because of how these utility tokens essentially represent IOUs for future services, they provide a built-in incentive to participate in the activities and communities that these tokens are associated with.[56]

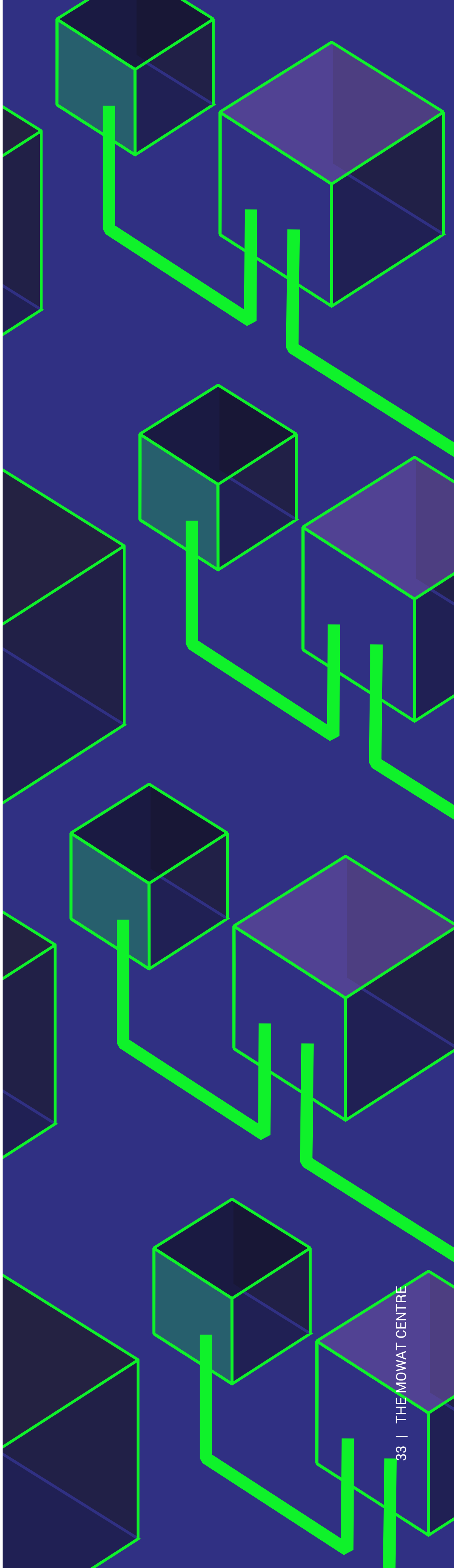
By this logic, ICOs would be similar to "local currencies" – such as Ithaca HOURS – in that they fix value within a particular economic network in a way that helps build community, albeit in a non-geographical digital context.[57] Some have argued these characteristics could help to reduce the sorts of short-term profit seeking that are exhibited by many of those who own traditional securities – a short-term focus that arguably encourages sub-optimal corporate decision-making.[58]

[55] Adlerstein, D. and Tinianow, A. 21 April, 2018. "Why ICOs Could Eat Delaware's Lunch." *Coindesk*. https://www.coindesk.com/icos-eat-delawares-lunch/.

[56] Korjus, K. 19 December, 2017. "We're planning to launch estcoin—and that's only the start." Republic of Estonia E-Residency Blog. *Medium*. https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790; Johnson, S. 16 January, 2018. "Beyond the Bitcoin Bubble." *The New York Times Magazine*. https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html.

[57] Jacob, J. Brinkerhoff, M. Jovic, E. Wheatley, G. 23 May, 2004. "The Social and Cultural Capital of Community Currency, An Ithaca HOURS Case Study Survey." *International Journal of Community Currency Research*. 8. pp.42-56. https://ijccr.files.wordpress.com/2012/05/ijccr-vol-8-2004-4-jacob-et-al-2.pdf. See also Gilbert, K. 22 September, 2014. "Why Local Currencies Could Be On The Rise In The U.S. -- And Why It Matters." *Forbes*. https://www.forbes.com/sites/katiegilbert/2014/09/22/why-local-currencies-could-be-on-the-rise-in-the-u-s-and-why-it-matters/2/#8279c837259a and De, N. 5 June, 2018. "Lawmaker Wants New York State to Pilot Local Cryptocurrencies." *Coindesk*. https://www.coindesk.com/lawmaker-wants-new-york-state-to-pilot-local-cryptocurrencies/.

[58] Mougayar, W. 10 June, 2017. Tokenomics—A Business Guide to Token Usage, Utility and Value. *Medium*. https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416.



BOX 5
Smart Contract

First articulated as a concept by Nick Szabo, a smart contract is a piece of software that encodes the terms of a contractual agreement and automates a part or the whole of its observation, verification and/or performance.[59] Because they are written in computer code, smart contracts have the ability to be self-executing and self-enforcing.[60] All that is needed is for the smart contract to be provided with the means of controlling the property implicated in the agreement, such as programmable digital assets or smart property (that is, physical property that can be controlled by software) and connected to the sources of information – often called "oracles" – required by the terms of the contract.

The dimensions of the blockchain revolution

ICOs are only one of a number of ways that blockchains can expand the space of possible economic relationships. Most of these new possibilities will likely have their impact along two dimensions of change, namely increased automation and decentralization. In both cases, the changes and new capabilities that blockchains enable will likely have impacts that spread beyond the economic sphere.

Automation

As with many other technological advances, some of the most important implications of blockchain will flow from the ways in which it enables automation. The most significant way that blockchain will likely do this derives from how its creation of a digitally native value system will enable the use of "smart contracts."

Before getting too far into a discussion of smart contracts, it is worth stepping back and considering what a traditional contract does. Currently, individuals or firms often create a contract to specify the parameters of an agreement between them. For example, contracts will often describe the services or products being purchased, the prices that have been agreed to, and the schedule for payments to be made. Signing a formal written contract is meant to clarify obligations between parties and to provide proof of an agreement that can be used to enforce compliance if one party fails to meet their obligations.

[59] Szabo, N. 1996. *Smart Contracts: Building Blocks for Digital Markets*. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[60] Investopedia. No date. "Smart Contracts." *Investopedia*. https://www.investopedia.com/terms/s/smart-contracts.asp.

Significantly, the signing of a contract does not itself ensure compliance. Often services and products are delivered that do not meet the agreed criteria, payments can be late and other conditions can be breached. It is true that the existence of a contract entitles the parties to apply to courts and the state for enforcement of the terms of the agreement, but doing so often involves lengthy and time-consuming litigation or negotiations.[61] Moreover, in countries where the rule of law is poorly observed, these problems often multiply and satisfaction can be difficult to obtain. Ultimately, contracting is always an imperfect exercise that, while it helps to coordinate activities between counterparties and reduce risk, serves only to reduce, not eliminate, economic friction, risk and inefficiency.

Smart contracts offer the possibility of further reducing this inefficiency and risk by increasing predictability, thereby creating additional value.[62] The creation of a digital value system enables smart contracts to accomplish this by expanding the boundaries of what can be automated by increasing the ability of a contract to directly exercise control over value.[63] In other words, by writing the terms of a contract into software that can directly perform these terms, smart contracting can reduce the risks of non-compliance, while also increasing the speed and efficiency of the execution of the agreements they implement.[64] Essentially, a digital contract written in computer code has the ability to remove much of the need for human intervention in enforcement from the practice of contracting.

Consider the following example. Bob purchases a car from Acme Motor Corp and agrees to make payments of one ether every month for 36 months. Bob and Acme Motor Corp can formalize this agreement in a smart contract that runs on the Ethereum blockchain and links their digital wallets (the accounts that hold ether) and the car itself to the smart contract over the Internet. This smart contract will monitor Bob's payments and, should he miss one beyond the limit specified in the smart contract, it could send a signal to the car locking its doors and disabling its engine until payments resume. Indeed, once autonomous vehicles arrive, the smart contract could even include a clause that commanded the car to return itself to the dealership if the purchaser missed a sufficient number of payments.[65]

Setting aside the non-blockchain technological innovations needed for this to occur (such as the development of autonomous vehicles) what this scenario shows is how, by enabling smart contracts, many systems could be rendered much more efficient through the removal of intermediaries. For instance, in this case, the purchaser sets up a direct payment from their digital wallet to the car company – thereby removing banks and credit card companies from this transaction. Moreover, the combination of smart contracts and smart property linked to this arrangement could remove the need for intermediaries like collections agencies to hound the purchaser and repossess the car if the purchaser was ultimately unable to pay.

[61] Wright, A. and de Filippi, P. 12 March, 2015. *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*. SSRN. Page 25-26.

[62] Szabo, N. 1996. *Smart Contracts: Building Blocks for Digital Markets*. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[63] Nick Szabo refers to this as an "embedding" of the contract in the world. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[64] Wright, A. and de Filippi, P. 12 March, 2015. *Decentralized Blockchain Technology*. Page 25.

[65] In principle, these smart contracts need not benefit only large corporations. Smart contracts could also be created to enforce a car's warrantee, thereby saving customers the need to badger an unresponsive manufacturer in order to have their rights enforced.

By extension, this could also enable the firms financing car purchases to lower the cost of financing because the costs associated with defaults would be reduced. This reduction in the onerousness of financing might in turn lower the number of defaults thereby creating a virtuous circle. By removing financial institutions from the equation, however, these smart contracts would also result in lost jobs.

The implications of smart contracting are even more striking because of how, by enabling this sort of automation, digitally native value systems could enable robots to begin contracting with each other autonomously. In so doing, blockchains may provide one of the critical technological advances that enables the mainstreaming of the IoT.

Currently, despite significant hype, the IoT has not yet noticeably impacted most people's daily lives. There are a variety of reasons for this but some of the most important obstacles could be dissolved by the capabilities that blockchains offer. For example, IBM has suggested that blockchains will be essential to the deployment of the IoT because centralized command and control systems will be too complex, and by extension expensive and insecure, to maintain effectively when hundreds of billions, perhaps trillions, of devices will need to be connected remotely to these systems. Control will need to be decentralized and that likely means that the devices in question will need to be autonomous – at least to a certain degree.[66]

Blockchains offer critical functionality in this regard. Recall that one of the key problems that blockchains were created to solve was to enable transactions – and, by extension, collaboration – between anonymous entities in a trustless environment. This is exactly the situation that will likely confront many autonomous devices as they seek to interact with other anonymous autonomous devices – and humans – in the real world. Currently, we use economic value, and exchanges thereof, as a means of coordinating the allocation of scarce resources. Because of how blockchains enable the creation of smart contracts capable of controlling digitally native forms of value, one can imagine the establishment of dedicated blockchains supporting self-contained digital markets in a host of different contexts within which autonomous devices would be able to interact and efficiently allocate scarce resources. In so doing, these automated markets could play the role of hyper-efficient coordination mechanisms that would likely generate significant new value.

Why not just use a credit card?

One might ask why some of the examples, such as Bob's car payments, require a blockchain to function. Could not such a contract be programmed on existing technology? Perhaps it could: things that look a bit like smart contracting, such as algorithmic trading on the stock market, do already exist. Nonetheless, a number of important obstacles stand in the way of existing technologies supporting the mass proliferation of such systems.

The most obvious of these obstacles is cost, something that is often a function of the presence of intermediaries. Currently, there are limited ways of transferring value electronically and they tend to feature relatively high costs – especially when one considers the fees that intermediaries like

[66] Pureswaran, V. and Brody, P. with Cohn, J. Finn, P. Nair, S. Panikkar, S. 2015. *Device democracy: Saving the future of the Internet of Things*. IBM Institute for Business Value. Slides 3-5 and 7.

banks and credit card networks charge both the customer and the merchant. One estimate made in 2016 suggested that the fees incurred carrying out a Bitcoin transaction were 5.5 times lower than the same fees that would have been incurred using a credit card.[67]

The question of fees charged by intermediaries is an especially important one because some of the more innovative implementations of blockchain that have been theorized would depend heavily on micropayments, often being made extremely frequently. In order for such implementations to be viable, high transaction throughputs at very low cost would be necessary. For instance, some have suggested that blockchains could help to enable the implementation of smart electricity grids in which independently-owned but autonomous home solar panel electricity generating systems negotiate with each other and the larger grid, trading power between them in real time.[68] For these grids to function efficiently, a secure system capable of processing payments valued at the level of micro-cents multiple times a second would be necessary. Similarly, many have suggested that blockchains might enable revolutionary new forms of digital rights management for digital assets such as music based on the concept of 'metered' access to content that would involve users making micropayments directly to artists every time they access their content instead of to intermediaries like record labels, iTunes or Spotify.[69]

It is difficult to imagine how existing credit card-based payment systems would be able to handle the volume of payments required to make these sorts of implementations possible. While it is true that the most important blockchains currently have lower throughput capacity than credit card networks,[70] upgrades – such as the use of state channels or ensuring interoperability between multiple blockchains – are already well into development and testing.[71] More important, however, is the idea that blockchain technology could enable local or implementation-specific blockchains to be created and optimized – relatively cheaply and flexibly on a per-project basis – in ways that simply would not be possible for the systems utilized by legacy payment systems.[72]

[67] Hayes, A. 13 September, 2016. "How Much Cheaper are Bitcoin Fees than Credit Card Fees?" *Investopedia*. https://www.investopedia.com/news/how-much-cheaper-are-bitcoin-fees-credit-card-fees/. Even at the height of the cryptocurrency frenzy in December 2017 and January 2018, fees on the bitcoin blockchain remained comparatively low. For example, on 22 December, 2017, the median fee paid to have a transaction processed was $31.71 (USD) and the median value transacted was $3,814 (USD) suggesting that the median rate being paid to transact on the network was about 0.8 per cent – still significantly lower than the standard fees charged by the major credit card networks. See https://bitinfocharts.com/comparison/bitcoin-median_transaction_fee.html.

[68] Kishewitsch, S. June 2017. "The promise of blockchain in distributed energy." News. *Association of Power Producers of Ontario*. https://magazine.appro.org/news/ontario-news/5166-1498093738-the-promise-of-blockchain-in-distributed-energy.html.

[69] Tapscott, D. and Tapscott, A. 22 March, 2017. "Blockchain Could Help Artists Profit More from Their Creative Works." *Harvard Business Review.* https://hbr.org/2017/03/blockchain-could-help-artists-profit-more-from-their-creative-works.

[70] Overcoming the hurdle posed by "scalability" remains an important challenge for public blockchains like Bitcoin and Ethereum. For example, Bitcoin can currently only process somewhere between 3.3 and 7 transactions per second, while Visa claimed in 2016 that its VisaNet system could process up to 65,000 transactions per second. See https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-fact-sheet.pdf.

[71] State channels are a mechanism whereby transactions can be carried out directly between parties without the need for the transactions to be conducted on the blockchain, thereby reducing the burden they impose on the network. Integrity of the transactions is guaranteed by a sort of "emergency break" which enables any of the parties involved to unilaterally move the transaction onto the blockchain at any time in a way that ensures that cheaters will not be rewarded. For a more in-depth explanation, please see Stark, J. 28 August, 2017. "Making Sense of Cryptoeconomics." L4 Media. *Medium*. https://medium.com/l4-media/making-sense-of-cryptoeconomics-c6455776669.

[72] Kishewitsch, S. June 2017. "The promise of blockchain in distributed energy."

Decentralization

The second main dimension along which blockchain enables innovation and change is decentralization. As discussed earlier, decentralization is one of the key characteristics of blockchain technology. But, unlike automation, the opportunities offered by decentralization can take more time to appreciate. Indeed, beyond the fact that decentralization makes blockchains possible and that it increases their resilience and security, the most obvious implication of blockchain's decentralization is that it creates redundancy and inefficiency in systems that use blockchain. This inefficiency is often cited as a problem for the expansion or scalability of blockchain-based systems like Bitcoin. In fact, Adam Ludwin, an entrepreneur working in the blockchain industry argues that "on almost every dimension, decentralized services are worse than their centralized counterparts:

» They are slower

» They are more expensive

» They are less scalable

» They have worse user experiences

» They have volatile and uncertain governance."[73]

Nonetheless, Ludwin still sees significant value in blockchains because of how decentralization creates what is referred to in the blockchain community as "censorship resistance." Censorship resistance is a term that refers to a system's imperviousness to unilateral alteration or control by a third party. In the case of Bitcoin, this means that no third party can unilaterally intervene to stop a transaction from being completed on the network. In the case of Ethereum, it means that no entity can unilaterally halt the performance of a smart contract running on the platform.[74]

Censorship resistance is not important for everyone or at all times. To understand how it can become important, it is worth examining a recent case where a centralized intermediated system engaged in censorship of its users. In 2010, all major credit card companies, as well as Paypal, refused to allow payments to Wikileaks over their networks, a move likely taken under pressure from the US government after Wikileaks released thousands of classified and secret US military and diplomatic documents.[75] While many might applaud these firms for taking these actions on the grounds that Wikileaks was irresponsibly releasing government secrets, many early Bitcoin adopters would likely see this as exactly the kind of authoritarian government action that Bitcoin was created to frustrate.

[73] Ludwin, A. 16 October, 2017. "A Letter to Jamie Dimon." Chain. *Medium*. https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80.

[74] This statement is true but obscures a slightly more complicated reality. See the discussion of "The DAO" in Section 6.

[75] Poulson, K. 12 April, 2010. "PayPal Freezes WikiLeaks Account." *Wired*. https://www.wired.com/2010/12/paypal-wikileaks/; Greenberg, A. 7 December, 2010. "Visa, MasterCard Move To Choke WikiLeaks." *Forbes*. https://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/#522954382cad.

Another example of the importance of censorship resistance can be found in the current enthusiasm for ICOs. As was discussed earlier, ICOs have exploded in popularity and, in 2017, attracted over $3.2 billion (USD) in investment.[76] In fact, in 2017, ICOs provided more funding for Internet firms than did traditional early-stage venture capital.[77] The funding for many of these projects would not have been available but for blockchains because the alternative platforms, such as stock markets, would decline to list them and traditional investors would decline to fund them.[78] Setting aside the question of whether this is positive or not, the fact that blockchains like Ethereum are enabling ICOs, and that there is little regulators can do to stop them, demonstrates the extent to which blockchains are censorship resistant.[79]

A more fundamental form of censorship resistance can be illustrated with a comparison between cryptocurrencies and fiat currencies. Blockchain was first proposed in the "cypherpunk" community where resentment of central bank control of fiat currency was strong.[80] Many believe that the key motivation behind Bitcoin's creation was to create a currency that no entity could manipulate and debase in the ways that governments and central banks have often done throughout history.[81] In fact, it is often said that Bitcoin first became popular in the places that needed it least because ensuring that a currency is censorship resistant is not a priority for many in a country like Canada where citizens have benefited from a competent, professional and independent central bank.[82]

But cypherpunks' concerns resonate powerfully with those who have seen their life savings wiped out by hyperinflation, have had them forcibly converted into a new currency, or had access to their savings restricted by capital controls imposed by the government in places such

[76] The Economist. 9 November, 2017. "The meaning in the madness of initial coin offerings."

[77] Kharpal, A. 9 August, 2017. "Initial coin offerings have raised $1.2 billion and now surpass early stage VC funding." *CNBC*. https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html.

[78] Ludwin, A. 16 October, 2017. "A Letter to Jamie Dimon."

[79] The case of Plexcoin, one of the few ICOs where regulators have taken action, is instructive in this regard. Despite ordering Dominic Lacroix, its creator, to not go ahead with his planned ICO, Lacroix was still able to launch his ICO and collect more than $15 million dollars from investors before he was arrested and sentenced to jail time. Had Lacroix attempted to conduct a traditional IPO, the regulator would have been able to ensure that PlexCoin never hit the market. Pearson, J. 8 December, 2017. "PlexCoin Scam Founder Sentenced to Jail and Fined $10K." *Motherboard*. Vice. https://motherboard.vice.com/en_us/article/qvzkx7/plexcoin-scam-founder-sentenced-to-jail-and-fined-10k and Bergeron, Y. 8 December, 2017. "Le créateur d'une monnaie virtuelle condamné à la prison." *ICI * Quebec*. http://ici.radio-canada.ca/nouvelle/1071971/peine-prison-createur-monnaie-virtuelle-dominic-lacroix It is also interesting to note that the only reason that Lacroix was caught and stopped was because he was charged by a Canadian authority while he was physically in Canada. More concerning are fraudulent ICOs launched from foreign jurisdictions where enforcement of Canadian laws may be impossible.

[80] Indeed, sometimes these ideas can get a little strange: Pearson, J. 29 September 2017. "Inside the World of the 'Bitcoin Carnivores'." *Motherboard*. Vice. https://motherboard.vice.com/en_us/article/ne74nw/inside-the-world-of-the-bitcoin-carnivores.

[81] See for instance, Spiralus. 23 March, 2017. Satoshi's Incomplete Economic Vision. *Medium*. https://medium.com/@Spiralus/satoshis-incomplete-economic-vision-eb833a33bcb5 and Liu, A. 16 January, 2014. "What Satoshi Said: Understanding Bitcoin Through the Lens of Its Enigmatic Creator." *Motherboard Blog*. Vice. https://motherboard.vice.com/en_us/article/vvbm43/quotes-from-satoshi-understanding-bitcoin-through-the-lens-of-its-enigmatic-creator.

[82] Popper, N. 29 April, 2015. "Can Bitcoin Conquer Argentina?" *The New York Times Magazine*. https://www.nytimes.com/2015/05/03/magazine/how-bitcoin-is-disrupting-argentinas-economy.html Similarly, The creation of basic banking services for the world's 5 billion unbanked individuals, something that has proven difficult or unattractive to traditional providers because of its low margins and limited profitability, is often touted as a potentially transformative application of blockchain that could make a material contribution to improving the lot of the world's poor. Vigna, P. and Casey, M. 2016. *The Age of Cryptocurrency*. Page 186. Another example would be to provide reliable access to secure property rights for the two-thirds of the world's population that currently live without them. See Vigna, P. and Casey, M. 2016. *The Age of Cryptocurrency*. Page 216-217. and Arsenault, C. 1 August, 2016. "Property rights for world's poor could unlock trillions in 'dead capital': economist." *Reuters*. https://www.reuters.com/article/us-global-landrights-desoto/property-rights-for-worlds-poor-could-unlock-trillions-in-dead-capital-economist-idUSKCN10C1C1.

as Zimbabwe,[83] Argentina,[84] Venezuela[85] and Greece.[86] While Bitcoin is known for its own price volatility, this volatility is arguably the result of its immaturity as an asset and will likely decrease as it matures and grows more widespread.[87] Conversely, inflation in a country like Zimbabwe is the direct and predictable result of the government's reckless decision to print money to pay its debts. Inflation of this type would be impossible in an economy that used only Bitcoin because the number of bitcoins is transparently controlled by the Bitcoin software and resistant to unilateral change (i.e. censorship) by a self-interested party – like a profligate government looking to print its way out of its debts.

Decentralization also helps make blockchains reliable and secure. We have already discussed how blockchains enable greater reliability because of how they eliminate single points of failure. Similarly, by avoiding the creation of "honeypots," the use of a blockchain can increase security. Chris Dixon, a venture capitalist active in the blockchain industry, illustrates this point by comparing the value hosted on the biggest blockchains to a "bug bounty" – that is, the reward software firms will pay to hackers who inform them of vulnerabilities in their software. He notes that if someone were able to hack any of the big blockchains, the monetary reward would be immense – potentially worth billions of dollars. But, "Bitcoin is now a nine-year-old multibillion-dollar bug bounty, and no one's hacked it. It feels like pretty good proof [that it is secure]."[88]

Finally, some are arguing that the importance of decentralization is actually much more abstract and fundamental. Those who make this argument hold that the decentralization enabled by blockchain is an essential corrective to a flaw in the current evolutionary path of the Internet. According to this argument, the lack of a protocol for personal identification on the Internet has enabled the centralization of control over the Internet into the hands of a small group of mega-companies with negative results for competition, users' health and democracy.[89] In combination with several other technologies, blockchain could enable society to disintermediate these firms, help to return the Internet to its decentralized origins and re-empower individuals by enabling them to own and better protect the data and value they create.[90]

[83] Titcomb, J. 20 November, 2017. How bitcoin has become Zimbabwe's crisis currency. *The Telegraph*. http://www.telegraph.co.uk/technology/2017/11/20/bitcoin-has-become-zimbabwes-crisis-currency/.
[84] Popper, N. 29 April, 2015. "Can Bitcoin Conquer Argentina?"
[85] The Associated Press. 13 December, 2017. "Bitcoin boom seen as survival, not speculation, in Venezuela." *News.* CBC. http://www.cbc.ca/news/world/venezuela-bitcoin-1.4447568.
[86] The Associated Press. 29 June, 2015. "Greece in limbo as it shuts banks, puts limits on cash withdrawals to avoid financial collapse."
[87] Murphy, H. 27 November, 2017. "Bitcoin stirs volatility fears as it heads for $10,000." *The Financial Times*. https://www.ft.com/content/23392588-d398-11e7-8c9a-d9c0a5c8d5c9.
[88] Johnson, S. 16 January, 2018. "Beyond the Bitcoin Bubble."
[89] The Economist. 18 January, 2018. "How to tame the tech titans." *The Economist*. https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame.
[90] Mainelli, M. 5 October, 2017. "Blockchain Could Help Us Reclaim Control of Our Personal Data." *Harvard Business Review*. https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data.

One critical question that governments must constantly ask themselves is whether a blockchain is necessary or whether a simpler DLT – or even a traditional database – will suffice.

4 POTENTIAL USES BY THE BROADER PUBLIC SECTOR

Some of the most interesting potential use cases for blockchain lie within the broader public sector. These use cases – which range from enabling greater effectiveness, patient control and privacy of medical records, to creating a reliable and accessible public record of individuals' academic credentials to improving the efficiency of government business permit issuing and licensing regimes – all offer governments the possibility of improved transparency, efficiency and effectiveness.

Nevertheless, all of these applications are still in the early stages and significant work remains to be done to ensure that any new solutions offer worthwhile improvements on existing systems. Blockchain is not a solution to all problems – or even most problems for that matter. One critical question that governments must constantly ask themselves is whether a blockchain is necessary or whether a simpler DLT – or even a traditional database – will suffice. In many cases, DLT and traditional databases will serve the government's purpose more efficiently and effectively.

Nevertheless, even with this healthy scepticism, blockchain offers governments numerous functionalities that could help them improve their operations. Consequently, they should seize opportunities to experiment with potential uses of blockchain technology when they can. This section highlights three areas that hold significant promise or in which some governments are already active.

Electronic health records

In the past few years a number of proposals for using blockchain to improve electronic health records (EHRs) have emerged. While initially pursued out of a desire to simply improve efficiency, EHRs are now also being seen as a means of giving patients greater control over their own health and medical treatments, something that is attractive from a privacy perspective but also because doing so seems to improve patients' health outcomes.[91] Existing EHR systems aim to further these objectives, but for a variety of reasons including rigorous privacy requirements, poor interoperability, incompatible workflow designs and poor audit trails they have failed to deliver many of the sought-after improvements.[92]

[91] The Economist. 1 February, 2018. "A revolution in health care is coming." *The Economist*. https://www.economist.com/news/leaders/21736138-welcome-doctor-you-revolution-health-care-coming.

[92] Halamka, J. Lippman, A. Ekblaw, A. 3 March, 2017. "The Potential for Blockchain to Transform Electronic Health Records." *Harvard Business Review*. https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

The solution offered by blockchain would be to use a blockchain to create an overarching mechanism that would provide patients with a means of linking all their records, regardless of where they are stored, controlling who gets to see them, and tracking their use. Critically, the EHRs themselves would probably not be put on the blockchain as is sometimes confusingly suggested. Rather, the records would remain at the institution, be it a clinic or hospital, where they currently reside, but access to these robustly encrypted records would only be possible through a portal created by a blockchain. Access to the records would be controlled by the patient via the blockchain, and any access to the records would be tracked by the blockchain as would any additions made to it.

The creation of a common, public, likely open-sourced, EHR blockchain platform would provide a single simplified focus for efforts to build compatibility into a system riddled with poor interoperability. It could also conceivably enable massive new medical breakthroughs by providing machine learning algorithms with a means of using transparent, open source smart contracts to query millions of EHRs for specific pieces of information without compromising the privacy of these records. In so doing, this could unlock enormous new datasets for these algorithms to mine for new discoveries and identify candidates for medical trials, potentially saving thousands of lives and billions of dollars.[93]

Professional and post-secondary credentials

Another area that offers a potentially important use case for blockchain is in professional and post-secondary accreditation. Currently, it can be frustrating, time-consuming and costly for individuals to prove that they hold the credentials that they claim to hold. Conversely, it can be just as difficult for individuals to reliably confirm that other individuals hold the credentials they claim to hold. Many institutions that require individuals to prove that they hold a credential still require them to do so by providing an original or validated physical copy of the credential.

The process of proving one's credentials can be inefficient and costly, especially for refugees and skilled immigrants who otherwise need to go through extensive testing to have their credentials recognized or to establish new credentials.[94] It can also be frustrating for students – especially international students – who may be required to purchase multiple copies of their transcripts or degree certificates from universities when they need them to apply for additional schooling, scholarships or jobs. Moreover, it is difficult to reliably demonstrate the authenticity of many of these physical documents, making them vulnerable to fraud.

[93] See, for example, the proposal contained in Shrier, A. Chang, A. Diakun-Thibault, N. Forni, L. Landa, F. Mayo, J. van Riezen, R. Hardjono,T. *Blockchain and Health IT: Algorithms, Privacy, and Data*. White Paper prepared for Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services.

[94] The use of blockchain to overcome this problem is already being piloted: World Education Services. 30 May, 2018. "World Education Services Pilots Blockchain-Based Digital Badges for Internationally Educated Students and Professionals." *Globenewswire*. https://globenewswire.com/news-release/2018/05/30/1513818/0/en/World-Education-Services-Pilots-Blockchain-Based-Digital-Badges-for-Internationally-Educated-Students-and-Professionals.html.

The solution offered by blockchain or DLT would be for the credential granting institutions – such as universities, colleges or professional associations – to jointly operate a permissioned blockchain on which they issued the credential granted to an individual in the form of a digital token. Individuals who received these credentials would be able to add the token to their digital wallet. If another institution or potential employer wanted to check an individual's credentials, the individual could simply provide the institution or employer with their wallet address for them to query at any time.

Not only would such a system increase efficiency, it would also make degree fraud much more difficult. This may seem like a small benefit, but some experts claim that as many as half of all PhDs issued in the USA each year come from fraudulent degree mills.[95] Considering that credential requirements often play important roles in ensuring public safety and accountability for credential holders, such a system could reduce some of the significant, but often unnoticed, harmful impacts of credential fraud.[96]

Government permits, licensing and "verifiable claims"

Finally, blockchain may prove extremely useful in improving the efficiency of government permit granting, licensing and the provision of what are referred to as "verifiable claims" such as an individual's date of birth.

One of the most fundamental problems this could solve would be to reduce the burden of interacting with government or complying with regulations currently faced by individuals and businesses. Indeed, individuals and businesses often complain that they are forced to waste a significant amount of time by repeatedly providing different parts or levels of government with the same information that they have already provided to other parts or levels of government.[97] Not only is this inefficient, it creates a greater likelihood that this information will be hacked or corrupted through human error or technological failure because it is being transmitted and physically entered into multiple systems multiple times.

Blockchain offers a real opportunity to reduce some of these burdens for individuals and business. The Government of British Columbia's Verified Organization Network (VON) represents a good example of how governments could use blockchain in this way. The provincial government's plan for VON is for government permits and other "verifiable claims" to be pre-loaded onto the system so that other government services can query the VON's digital wallet, called TheOrgBook, to verify information about

[95] Szeto, E. Vellani, N. "'All of us can be harmed': Investigation reveals hundreds of Canadians have phoney degrees." *Marketplace.* CBC. http://www.cbc.ca/news/business/diploma-mills-marketplace-fake-degrees-1.4279513.

[96] Johnson, E. 11 September, 2017. "'I am devastated': Toronto lawyer out $100K after hiring fraudster with fake law degree." *Go Public*. CBC. http://www.cbc.ca/news/business/fake-toronto-lawyer-defrauds-clients-1.4276157.

[97] Johal, S. and Urban, M. 11, May, 2017. *Regulating Disruption: Governing in an era of rapid technological change.* The Mowat Centre. https://mowatcentre.ca/regulating-disruption/.

organizations on the network. Eventually, the ambition is for organizations like businesses to have their own wallets to hold their verifiable claims so that they will be able to prove their credentials to others themselves.[98]

In another similar example, the Government of Canada, the Government of Ontario and the City of Toronto recently concluded a proof of concept in which they explored how blockchain might be used to improve the way governments interact with someone seeking to open a restaurant. In this proof of concept, they created a test database that was shared between a variety of departments and agencies at the municipal and provincial level with each of these entities operating one of the network's nodes. This private test database never contained real individuals' or businesses' information, but the database was used to simulate the movement of information needed to acquire a restaurant permit between the following portals and systems of record:

» the Government of Ontario online portal used to provide information and request incorporation of a new business

» the Government of Ontario ONBIS registration system

» the Canada Revenue Agency Business Number Registry System

» the City of Toronto Licensing Office's Progress Software Licensing System

» the Alcohol and Gaming Commission of Ontario Computronix Regulatory Assurance System

Additionally, the project also included using an Ethereum test network to simulate how an external entity – e.g., a bank evaluating a loan request from a potential restaurateur – might access a public blockchain linked to a private government one to confirm that the applicant had acquired the permits needed to open their restaurant. The manner in which the blockchain was used, and the changes in the processes that it enabled are illustrated in Figures 13 and 14.

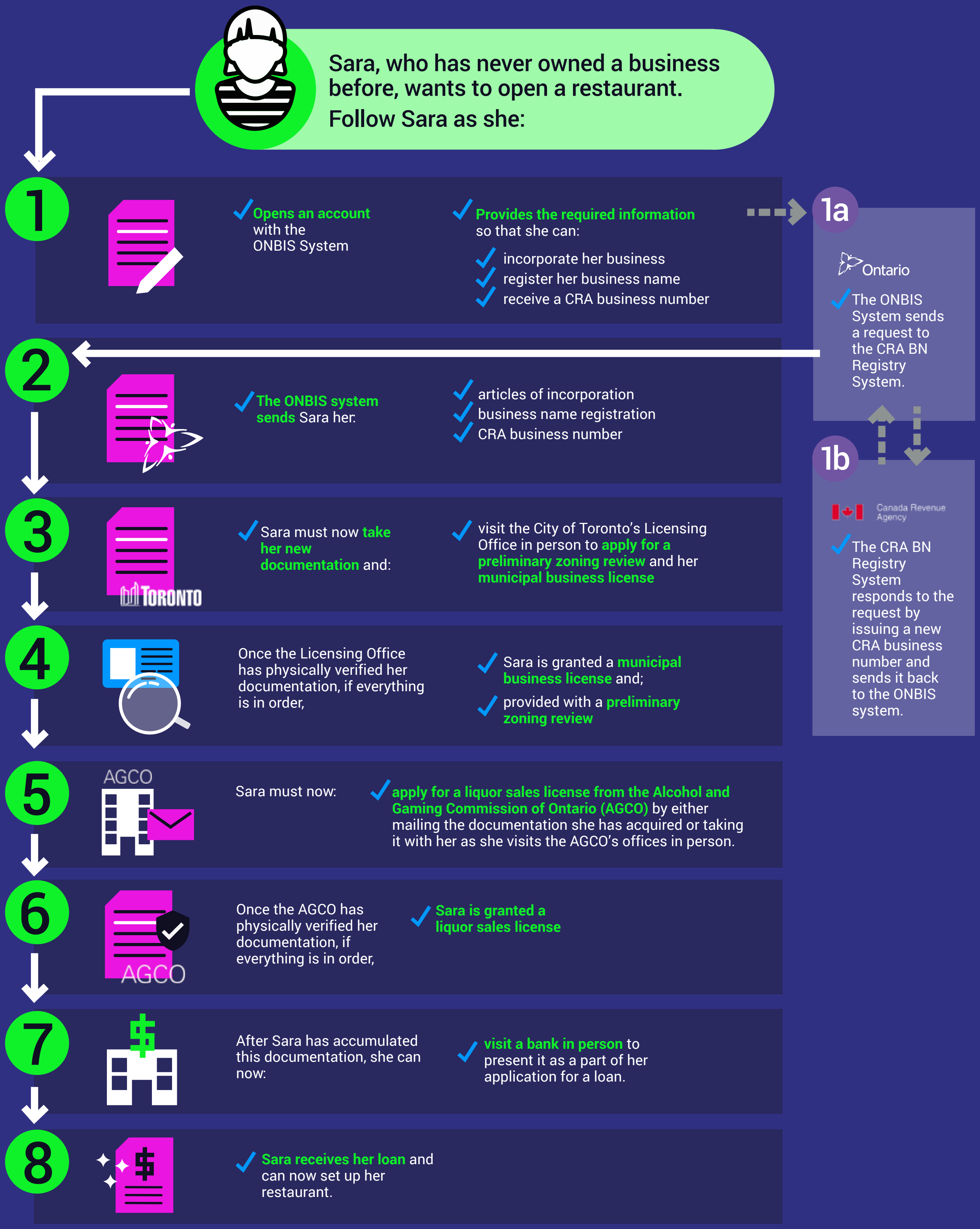
The proof of concept demonstrated that there was significant scope for the use of blockchain to improve the efficiency of the current customer journey from both the perspective of the applicant and the various levels of government. For the customer, the use of blockchain or DLT in this way could reduce the burden of travelling to many different government offices to acquire the necessary permits and cut the time required to do so from weeks to days. Note, for example, how the number of steps a citizen is required to take was cut from eight under the current system to four in the proof of concept. For governments, this sort of system could also help realize the ambition to create a more "client focused" approach to government services and also increase the integrity and security of the data involved while also reducing costs.

Moreover, the proof of concept also demonstrated that it would be possible to introduce a blockchain or distributed ledger as just one piece that could help to connect the larger ecosystem of legacy systems. This is an important point to note as it means that blockchain or DLT could be implemented incrementally across the system as appropriate and in line with the lifecycles of existing legacy systems. In other words, a "Big Bang," in which the entire system is replaced with a single blockchain at enormous cost and with significant risk, would not be necessary.

[98] O'Donnell, D. 18 April, 2018. "BCGov Verifiable Organization Network – Impressive Client Demo." *Blog.* Continuum Loop Inc. https://www.continuumloop.com/bcgov-verifiable-organization-network/.

FIGURE 13

Current restaurant permit acquisition journey



Sara, who has never owned a business before, wants to open a restaurant. Follow Sara as she:

1

✓ **Opens an account** with the ONBIS System

✓ **Provides the required information** so that she can:

- ✓ incorporate her business
- ✓ register her business name
- ✓ receive a CRA business number

1a

Ontario

✓ The ONBIS System sends a request to the CRA BN Registry System.

1b

Canada Revenue Agency

✓ The CRA BN Registry System responds to the request by issuing a new CRA business number and sends it back to the ONBIS system.

2

✓ **The ONBIS system sends** Sara her:

- ✓ articles of incorporation
- ✓ business name registration
- ✓ CRA business number

3

✓ Sara must now **take her new documentation** and:

✓ visit the City of Toronto's Licensing Office in person to **apply for a preliminary zoning review** and her **municipal business license**

4

Once the Licensing Office has physically verified her documentation, if everything is in order,

✓ Sara is granted a **municipal business license** and;

✓ provided with a **preliminary zoning review**

5

Sara must now:

✓ **apply for a liquor sales license from the Alcohol and Gaming Commission of Ontario (AGCO)** by either mailing the documentation she has acquired or taking it with her as she visits the AGCO's offices in person.

6

Once the AGCO has physically verified her documentation, if everything is in order,

✓ **Sara is granted a liquor sales license**

7

After Sara has accumulated this documentation, she can now:

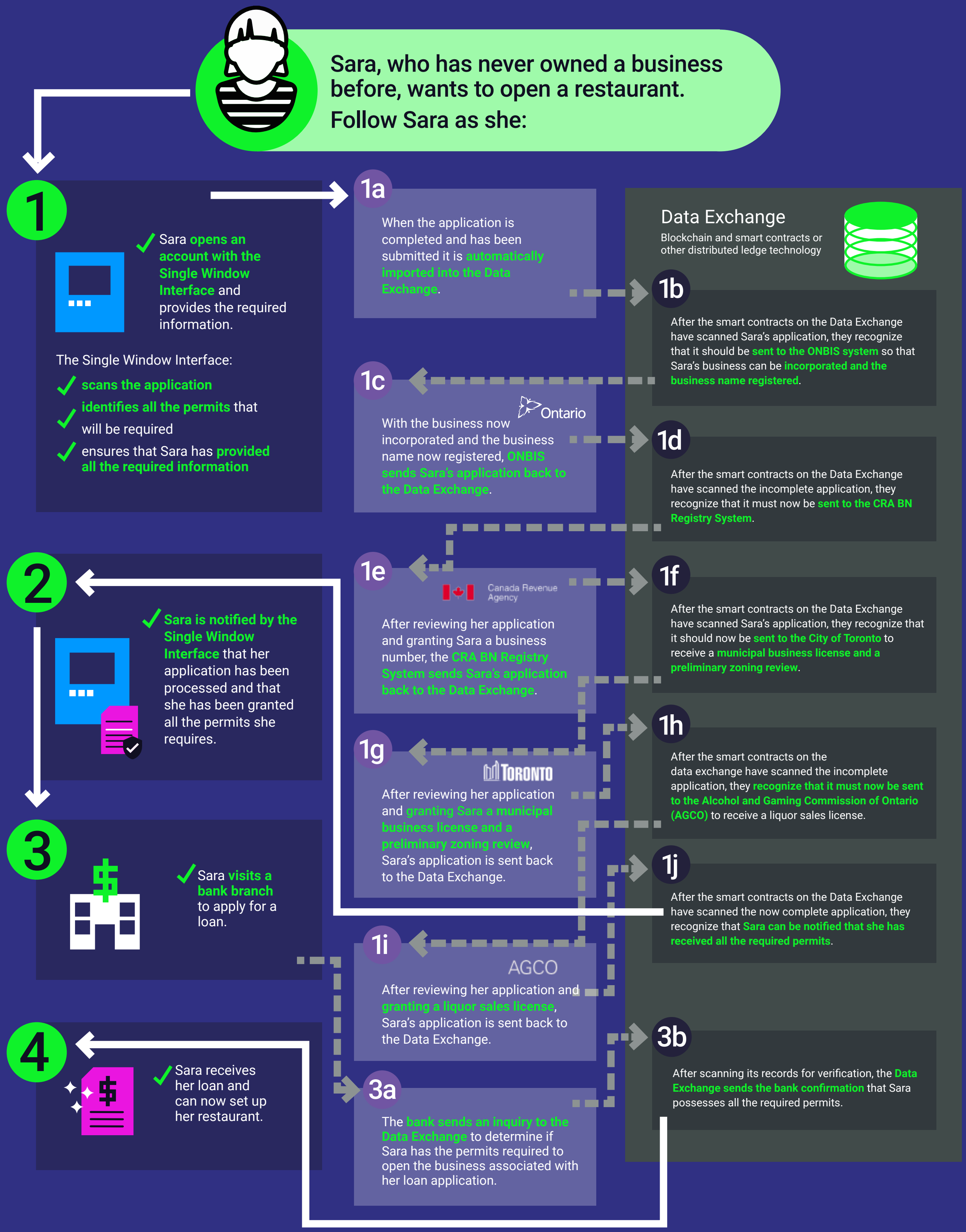
✓ **visit a bank in person** to present it as a part of her application for a loan.

8

✓ **Sara receives her loan** and can now set up her restaurant.

FIGURE 14

Potential restaurant permit acquisition journey



Sara, who has never owned a business before, wants to open a restaurant.
Follow Sara as she:

1

✓ Sara **opens an account with the Single Window Interface** and provides the required information.

The Single Window Interface:

- ✓ **scans the application**
- ✓ **identifies all the permits** that will be required
- ✓ ensures that Sara has **provided all the required information**

1a When the application is completed and has been submitted it is **automatically imported into the Data Exchange**.

Data Exchange
Blockchain and smart contracts or other distributed ledge technology

1b After the smart contracts on the Data Exchange have scanned Sara's application, they recognize that it should be **sent to the ONBIS system** so that Sara's business can be **incorporated and the business name registered**.

1c Ontario
With the business now incorporated and the business name now registered, **ONBIS sends Sara's application back to the Data Exchange**.

1d After the smart contracts on the Data Exchange have scanned the incomplete application, they recognize that it must now be **sent to the CRA BN Registry System**.

1e Canada Revenue Agency
After reviewing her application and granting Sara a business number, the **CRA BN Registry System sends Sara's application back to the Data Exchange**.

1f After the smart contracts on the Data Exchange have scanned Sara's application, they recognize that it should now be **sent to the City of Toronto** to receive a **municipal business license and a preliminary zoning review**.

1g TORONTO
After reviewing her application and **granting Sara a municipal business license and a preliminary zoning review**, Sara's application is sent back to the Data Exchange.

1h After the smart contracts on the data exchange have scanned the incomplete application, they **recognize that it must now be sent to the Alcohol and Gaming Commission of Ontario (AGCO)** to receive a liquor sales license.

1i AGCO
After reviewing her application and **granting a liquor sales license**, Sara's application is sent back to the Data Exchange.

1j After the smart contracts on the Data Exchange have scanned the now complete application, they recognize that **Sara can be notified that she has received all the required permits**.

2

✓ **Sara is notified by the Single Window Interface** that her application has been processed and that she has been granted all the permits she requires.

3

✓ Sara **visits a bank branch** to apply for a loan.

3a The **bank sends an inquiry to the Data Exchange** to determine if Sara has the permits required to open the business associated with her loan application.

3b After scanning its records for verification, the **Data Exchange sends the bank confirmation** that Sara possesses all the required permits.

4

✓ Sara receives her loan and can now set up her restaurant.

The proof of concept also demonstrated that while there would be some technical issues to overcome, the largest challenges in implementing a blockchain solution would likely lie elsewhere. Specifically, while the blockchain itself would be tamper-proof and easily audited, it would only be as good as the information added to it by the participating departments and agencies and the security of the processes by which these additions were made. The type of data structures used on the blockchain, the organizations allowed to operate a node, the question of how new organizations would be on-boarded – all of these questions would need to be resolved prior to implementation. Additionally, certain regulatory and legislative requirements that are not technologically neutral may have to be changed before a blockchain or DLT-based solution could be implemented.

On the human side, an external consultant was contracted to provide much of the technical know-how for the proof of concept. While some government employees were able to take advantage of the project and use it as a learning opportunity, getting to a point where government has sufficient in-house blockchain capacity to tackle more ambitious projects will take time, both on the technical and policy sides.

In this respect, proofs of concept and small scale pilot projects represent excellent opportunities to advance multiple objectives. As just mentioned, they can be leveraged to help build internal government capacity without raising the stakes too high. Significantly, these benefits are also applicable for small and medium-sized enterprises as well. These opportunities can provide small and medium-sized blockchain enterprises – of which there are many based locally in Ontario and elsewhere in Canada – with experience working with governments at a scale which is comfortable for them. This procurement experience can be especially valuable for firms who often complain of an inability to attract critical institutional reference customers, even as they help to set up the government organizations involved for future projects of greater scope and ambition.

Overall, the proof of concept demonstrated that there are real use cases for blockchain in government operations, especially as a means of encouraging and enabling cooperation between different departments, agencies and levels of government that need to exchange information or verify claims with each other regularly. The proof of concept also demonstrated that there could be significant benefits for the public should this technology be implemented by government in areas where there was a need for the public to be able to access data or prove a verifiable claim, such as their possession of a restaurant permit. But it also demonstrated that there are significant obstacles on the path towards the implementation of an actual operational blockchain solution in government in Canada.

5 IMPLICATIONS FOR PUBLIC POLICY

Blockchain is still a young technology and its implications for public policy are still unclear. Nevertheless, understanding how blockchain works, how it will enable more automation and decentralization and how it might impact government operations can help to reduce this uncertainty. Building on this analysis, the following section identifies four broad “Issues to Watch” which are likely to have important impacts in the context of public policy.

Competition in “governance services”

Many services that governments provide could conceivably be better delivered using blockchain or DLT. In some places this is already occurring. The most obvious instance are in countries that lack stability or effective rule of law. For example, in countries where the government has failed to provide a stable currency (such as Venezuela[99] and, previously, Argentina[100]), many citizens are turning to, or have previously turned to, cryptocurrencies.

Blockchains are also being used in other less extreme circumstances to provide governance services – often with governments playing a leading role. In 2017 the Eastern European country of Georgia began shifting its national land registry system onto a blockchain.[101] Sweden recently completed a pilot project along similar lines.[102] The government of Dubai has said that it wants all visa applications, bill payments and license renewals – processes which account for over 100 million documents per year – to be transacted on blockchains by 2020.[103] Each of these projects have unique motivations and contexts, but overall, the idea is that the combination of transparency and immutability

[99] Chun, R. September, 2017. “Big in Venezuela: Bitcoin Mining.” *The Atlantic*. https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/.

[100] Popper, N. 29 April, 2015. “Can Bitcoin Conquer Argentina?”

[101] Shin, L. 7 February, 2017. “The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project.” *Forbes*. https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#1f4ecc134dcd; The Economist. 1 June, 2017. Governments may be big backers of the blockchain. *The Economist*. https://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers.

[102] Haaramo, E. 5 July, 2017. “Sweden trials blockchain for land registry management.” *ComputerWeekly.com*. https://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management.

[103] D’Cunha, S. 18 December, 2017. Dubai Sets Its Sights On Becoming The World’s First Blockchain-Powered Government. *Forbes*. https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#4a56a414454b.

offered by blockchains could help to improve the efficiency of government operations, the ease of citizens' interactions with their governments, and reduce opportunities for corruption.

The Baltic country of Estonia is arguably the country that is the furthest along this path. Its X-road information system enables residents to do everything from viewing their medical records, to paying their taxes, to voting online.[104] Since the X-road only links a number of separate centralized databases it is not itself a blockchain according to our definition.[105] Nevertheless, it uses similar cryptographic techniques and DLT to track changes to shared databases by multiple collaborators, enable high levels of transparency and provide differentiated access to information depending on permission levels. In fact, given the nature of government operations, Estonia's X-road may provide a better indication of what many of the potential implementations of blockchain and DLT by government will look like than do public blockchains like Bitcoin.[106] Thus, the Estonian experience offers a number of lessons and insights into how government services can be delivered more conveniently and efficiently using these sorts of technologies. It also offers some important warnings.

The most noticeable results of the X-road-led digitization of government in Estonia have been the significant increases in administrative convenience and efficiency it has enabled. The Estonian government claims to have saved the equivalent of 2 per cent of GDP a year in government spending.

But other more complex benefits also appear to be emerging.[107] For example, in 2014, Estonia launched something called e-residency, a program whereby non-Estonians can become "digital residents" of the country. E-residency, which does not confer any special ability to actually immigrate to Estonia, enables e-residents to access many of the services that Estonia's increasingly digital government offers such as "remote management, lower cost of business services, access to the EU market, and access to a wider choice of e-services."[108]

As of December 2017, almost 27,000 applications for e-residency had been received from 143 countries. At that time, e-residents had already set up 4,272 companies in Estonia. Furthermore, a 2017 report by Deloitte estimated that, in its first three years of operation, Estonia's e-residency program had generated €1.4 million in government revenues and €13 million in indirect socio-economic benefits. The same report suggested that these revenues and indirect benefits would likely rise to over €31 million and €194 million respectively by 2021.[109]

[104] Jaffe, E. 20 April, 2016. "How Estonia became a global model for e-government." *Side|Walk|Talk.* Sidewalk Labs. https://medium.com/sidewalk-talk/how-estonia-became-a-global-model-for-e-government-c12e5002d818.

[105] Birch, D. 29 March, 2017. "The mystery of the non-existent Estonian digital identity blockchain: solved!" *disruptive.asia*. https://disruptive.asia/estonian-digital-identity-blockchain/.

[106] Note, for instance, the similarity of the X-road to the Government of Ontario and City of Toronto proof of concept outlined in Section 5.

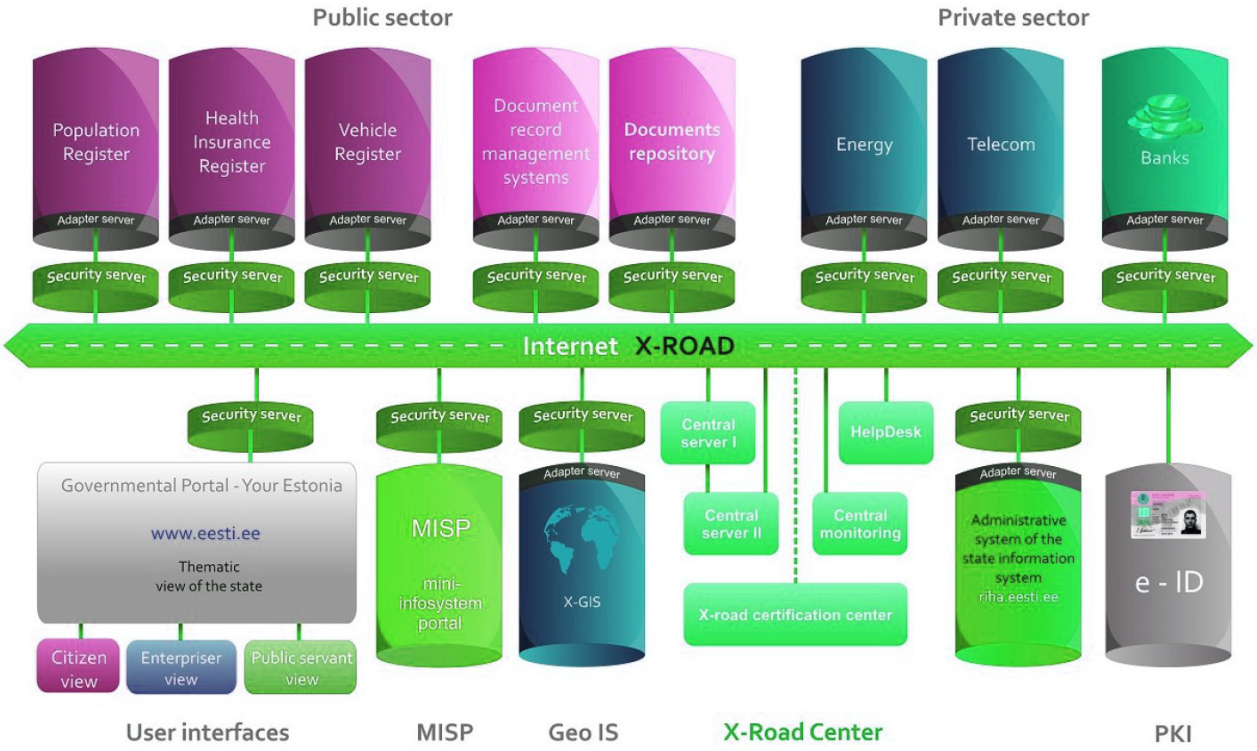
[107] Heller, N. 18 & 25 December, 2017. "Estonia, the Digital Republic." *The New Yorker.* https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

[108] https://medium.com/e-residency-blog/heres-why-tax-evaders-are-disappointed-in-estonian-e-residency-2322644f5f59.

[109] Cavegn, D. (ed) 2 December, 2017. "Deloitte: E-residency brought €14.4 million to Estonia in first three years." *News.* eer.ee. https://news.err.ee/646254/deloitte-e-residency-brought-14-4-million-to-estonia-in-first-three-years.

FIGURE 15

Estonia's X-Road data exchange



Source: Vassil, K. June 2015. "Estonian e-Government Ecosystem: Foundation, Applications, Outcomes." World Development Report Background Paper. http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf. Page 12.

At the moment, the advantages of e-residency that are often touted – such as the ability to use digital signatures for all business interactions, the ability to set up a company in hours instead of days or weeks, the speed and ease of filing pre-populated smart tax forms and access to the EU market – may not seem overwhelming from a Canadian perspective.[110] But for residents of some developing countries where regulations can make it difficult to start and run businesses – especially for marginalized groups like women and especially when that business works across borders – the program has been very attractive. Indeed, the e-residency program has partnered with the United Nations (UN) to develop a project called "e-Trade for All" aimed at helping individuals in developing countries to start an online business using the e-residency program.[111]

[110] The benefits are a bit more obvious for Briton's who want to operate a business in the EU in a post-Brexit world. Hardy, A. Robinson, N. and Haggman, A. 18 November, 2016. "VISIT | How to stay in.eu: A post-Brexit gift from Estonia and an evening inside its Embassy." *Geopolitics & Security*. Royal Holloway; University of London. https://rhulgeopolitics.wordpress.com/2016/11/18/visit-how-to-stay-in-eu-a-post-brexit-gift-from-estonia-and-an-evening-inside-its-embassy/.

[111] Godoy, D. 25 April, 2017. "UN and e-Residency join forces to empower entrepreneurs in the developing world." Republic of Estonia E-Residency Blog. *Medium*. https://medium.com/e-residency-blog/un-and-e-residency-join-forces-to-empower-entrepreneurs-in-the-developing-world-ea834005f85e.

More fundamentally, e-residency shows how the digitization of Estonia's governance services has created the infrastructure needed to enable "government-as-a-platform."[112] E-residency is just one example of how the creation of platforms like this can enable the most unexpected innovations. (Indeed, the next big step for the e-residency program looks likely to be the launch its own blockchain-based digital asset, the Estcoin.[113]) Critically, however, innovation like this is not just the result of Estonia having built a technological infrastructure. Rather, the construction of a corresponding "smart policy framework"[114] – the policy culture and infrastructure needed to get an optimal return from the technology and enable innovations like e-residency – has also been essential. Overall, this smart policy framework has provided Estonia with a competitive head start in the race to attract businesses and investment, as well as "residents," to its outsized corner of the growing digital world.[115]

It is not difficult to imagine how a welcoming regulatory framework in a country like Estonia, combined with the ability to remotely administer a company through a program like e-residency, might appeal to entrepreneurs.[116] Indeed, one can see important parallels between this approach and the strategy used by the US state of Delaware to attract businesses to incorporate there in the twentieth century. By passing business friendly laws, by ensuring its Court of Chancery – a law court focused on business transactions – was staffed with the best judges available and by building up a robust business case law, Delaware managed, despite its small population (still less than a million), to become the legal US domicile of about two-thirds of all Fortune 500 companies (see Figure 15).[117]

Why is this important in the context of blockchain? By creating a digitally native value system, blockchain is enabling the digitization and automation of a vast new category of activities. In so doing, it is empowering individuals, firms and networks *vis-à-vis* the state in new ways and reducing the extent to which geography and borders can blunt the competition that governments face. In other words, individuals, networks, firms and governments in other jurisdictions now have the ability to compete with Canadian governments in the provision of governance services in ways that were simply not possible previously. With Bitcoin, a small network of individuals have shown that they are capable of disrupting an area – currency issuance – that has basically been a state monopoly for at least a century. How might

[112] Government-as-a-platform is a concept patterned after the concept of Web 2.0. At its core, it refers to the idea that government's function is as a convenor or enabler of beneficial forms of collective action. Thus, it refers to the idea that one of government's core functions is to enable private individuals and groups to engage in beneficial activities that it would be difficult or impossible to undertake without government support – and which government itself is unlikely or poorly suited to do. For example, this often involves the creation of value through the leveraging of government data, as with citizen science initiatives or in building real-time transit tracking apps. See O'Reilly, T. "Chapter 2. Government as a platform." *Open Government*. http://chimera.labs.oreilly.com/books/1234000000774/ch02.html.

[113] Korjus, K. 19 December, 2017. "We're planning to launch estcoin."

[114] Korjus, K. 7 July, 2017. "Welcome to the blockchain nation." *Republic of Estonia E-Residency Blog*. https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4.

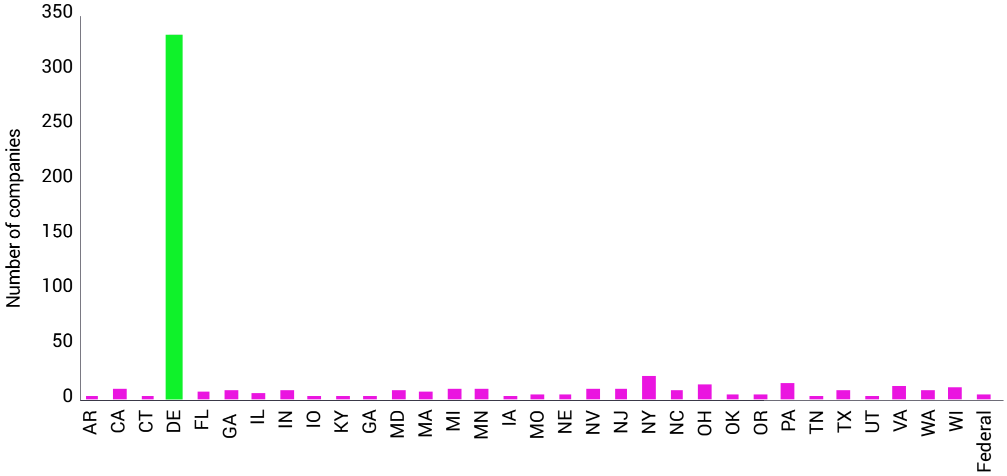
[115] In another example, Estonians are also taking a leading role in grappling with the many legal issues that the development of artificial intelligence will raise – they even have a hashtag for it: #krattlaw. Heller, N. 18 & 25 December, 2017. "Estonia, the Digital Republic."

[116] "Competition [between governments] is good. If you don't offer good services, through e-residency, citizens will have options and can choose a better digital government". See https://twitter.com/AlexBenay/status/963166899314962432.

[117] Semuels, A. October 3, 2016. "The Tiny State Whose Laws Affect Workers Everywhere." *The Atlantic*. https://www.theatlantic.com/business/archive/2016/10/corporate-governance/502487/.

FIGURE 16

Corporate domiciles of Fortune 500 companies in the USA



Source: Semuels, A. October 3, 2016. "The Tiny State Whose Laws Affect Workers Everywhere." *The Atlantic*. https://www.theatlantic.com/business/archive/2016/10/corporate-governance/502487/.

governments respond if, for example, significant portions of the economic activity occurring under their jurisdiction came to be conducted in a currency over which their monetary policy has essentially no effect?[118]

While unlikely to occur in the short term, challenges like these are not amenable to quick solutions – governments need to begin considering responses to contingencies of this nature well in advance.[119] While fractional reserve banking will not be disrupted tomorrow,[120] the significance alone of such a possibility is so great that prudence demands that governments build expertise in these new technologies and consider how they might respond. Estonia and its e-governance infrastructure are providing an early and innocuous warning of how a government that embraces digitization can out-compete less innovative governments. (Estonia has committed to share all necessary tax information with the countries in which e-residents are physically active.[121]) While the details of the challenges presented by this increasingly competitive environment are not yet clear, the trend in this direction is.[122]

[118] For a more substantive discussion of the tax-specific implications of the transfer of value into digitally native value systems – one that has already started to occur with the advent of the "data economy" – see Johal, S. Thirgood, J. and Urban, M. with Alwani, K. and Dubrovinsky, M. 30 July, 2017. *Robots, Revenues & Responses: Ontario and the Future of Work*. The Mowat Centre. https://mowatcentre.ca/robots-revenues-responses/. Pages 35-36 and 38-41.

[119] The Federal Reserve Bank of St Louis is already examining the potential problems such a situation could cause. Bullard, J. 14 May, 2018. *Non-Uniform Currencies and Exchange Rate Chaos*. Federal Reserve Bank of St Louis. Presentation made to Coindesk Consensus 2018. New York City. https://www.stlouisfed.org/~/media/Files/PDFs/Bullard/remarks/2018/Bullard_Consensus_New_York_14_May_2018.pdf?la=en.

[120] Lagarde, C. 29 September, 2017. *Central Banking and Fintech—A Brave New World. International Monetary Fund*. Presentation made to the Bank of England Conference. London. https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world.

[121] Anderson, J. 19 July, 2016. "One way to get around Brexit: Become an e-resident of Estonia." *Quartz*. https://qz.com/736004/one-way-to-get-around-brexit-become-an-e-resident-of-estonia/.

[122] Hammersley, B. 27 March, 2017. "Concerned about Brexit? Why not become an e-resident of Estonia." *Wired*. http://www.wired.co.uk/article/estonia-e-resident. For an example of an effort to effectively challenge government's monopolies on a number of governance services, visit https://bitnation.co.

Decreasing effectiveness of “negative” regulatory frameworks

Another aspect of blockchain’s ability to empower individuals *vis-à-vis* the state that is worth watching concerns the declining effectiveness of existing regulatory frameworks which have traditionally relied on “negative” approaches. In our usage, negative approaches are ones that achieve their goals by removing or restricting the freedom of individuals within the system. Positive approaches, conversely, seek to advance an objective without restricting the freedom of individuals.

The undermining of the federal government’s Canadian content regime for broadcast media by the Internet provides an example of this sort of challenge. Previously, the Government of Canada was able to foster the production of Canadian cultural content by mandating that a percentage of broadcast content met certain criteria for Canadian-ness, such as the MAPL system for defining a Canadian song.[123] The Canadian government was able to enforce this requirement because the Canadian Radio-television and telecommunications Commission (CRTC), the industry’s regulator, was able to monitor broadcasts and, if a broadcaster did not adhere to the policy, take corrective action such as fines or the revocation of licenses. The logic of this policy was that by guaranteeing a market for Canadian content, the government was guaranteeing that Canadian content would be produced.

The arrival of the Internet and streaming audio and video services has dramatically undermined the viability of this approach. Services like Netflix and Spotify, which an already significant and increasing proportion of Canadians use to access content, have no obligation to include Canadian content in their offerings and the CRTC and the Government of Canada have to date found no way of forcing these services to create a guaranteed market for Canadian content. This is largely because these services are based in other jurisdictions and are able to connect with their users directly via the Internet. Without restricting access to the Internet, something likely unacceptable to the public, it is not clear how the Canadian government could force these foreign firms to abide by its current Canadian content regime.

The key point to draw from this is that, as individuals are given more powerful tools and more options, regulatory frameworks designed to govern behaviours by coercively erecting barriers to block individuals and enterprises from doing certain things will tend to be weakened. By enabling streaming services, for instance, the Internet has enabled many Canadians to opt out of the highly regulated Canadian broadcasting industry, thereby undermining the ability of the negative Canadian content regulatory framework that governs it to achieve its goal of ensuring the production of Canadian content.

A parallel situation is playing out in the rush of investors keen to participate in unregulated ICOs based in foreign countries. Canadian securities regulators are now facing a similar challenge as the CRTC. Previously, these regulators relied to a large extent on their ability to control what offerings were allowed to trade on stock exchanges to achieve their regulatory objectives. Now, this negative approach is being undermined.

[123] Canadian Radio-television and Telecommunications Commission. 10 August, 2009. “The MAPL system - defining a Canadian song.” *Content Made by Canadians*. Government of Canada. https://crtc.gc.ca/eng/info_sht/r1.htm.

In such situations, governments are faced with two options. First, they can double down on the negative approach and seek to improve its functioning by extending its rules, making punishments more serious and increasing the resources devoted to enforcement. In many cases, such an approach is unlikely to work well in a society like Canada that cherishes its liberties. Limiting access to the Internet, for example, would likely be decried as an authoritarian outrage.

The other option is to use a proactive "positive" approach where, instead of seeking to block unwanted activities, governments take steps to encourage desired ones. In the case of Canadian content, such an approach would achieve the policy's objective – namely, the creation of Canadian content – by proactively supporting the creation of Canadian content by, for example, providing funding directly to creators.

In a blockchain context, such an approach might see the Bank of Canada responding to the popularity of cryptocurrencies by creating its own cryptocurrency. Similarly, the Government of Canada might respond to concerns about corporate (mis)uses of individuals' data by creating its own blockchain-based digital identity as a foundation for a better digital rights management framework.[124] While these options are presented here as illustrations and not recommendations the key underlying point is critical, namely that by acting proactively, governments and regulators can potentially achieve their goals more effectively. By offering or enabling the thing for which there is demand, but doing so in a way that also allows the government to integrate safeguards or steer the activity in its preferred direction, it may be better able to achieve its ultimate objective through inducement rather than enforcement.

Novel legal questions

As novel as many of these challenges are, they are at least recognizable to most policymakers. With Canadian content, for instance, governments have long pursued a dual-track approach that mixes both negative and positive tools. Using more positive tools in response to the arrival of streaming services represents a shift in emphasis, not a new departure.

Conversely, some of the most important challenges posed by blockchains will be the novel legal questions for which there are no real precedents. Or, as one author put it: "You think it's hard to figure out what Bitcoin is from a regulatory standpoint, well, now we're talking about figuring out what an autonomous corporation is... [that's] like something from The Matrix."[125]

Because of how they would remove the need for employees, officers and directors – and even potentially owners – DAOs and DACs (see Box 7; hereafter, we use DAO to include both) essentially reduce corporations to their legal skeleton, namely a set objectives, some business logic and agreements designed to achieve these objectives. When this is all encoded in software, it can become difficult to distinguish DAOs from computer programs like video games. But, unlike

[124] The United Kingdom (UK), for example, has taken steps in this direction. This program, called GOV.UK Verify, enables citizens to prove their identity online through the use of one of a few trusted private firms' identity verification systems. Having done this, citizens can then use this verified digital identity to access government services, such as tax filing or checking the information on their driver's license. Government Digital Service. 12 July, 2018. *Guidance GOV.UK Verify*. Government of the United Kingdom. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

[125] Quoted in Vigna, P. and Casey, M. 2016. The Age of Cryptocurrency. pg. 241.

current video games, DAOs could be completely decentralized, exist entirely on a blockchain, have no national domicile but still be able to act in the physical world. This is because control over digitally native assets could enable them to purchase services or exercise control over Internet-connected devices like autonomous vehicles.[127] Should such creations be allowed? If yes, how should they be regulated? How could such regulations be enforced? If not, how could one country stop them from acting within their borders?

DAOs are only one of the more extreme potential applications of the much wider concept of smart contracts. Smart contracts are an innovation separate from blockchain but, because of how blockchain enables their more widespread and powerful deployment, they helpfully highlight the importance of approaching these interconnected technological innovations holistically. In fact, blockchain-based smart contracts are already beginning to appear. French insurer AXA recently tested an automated Ethereum-enabled smart-contract-powered

BOX 7

Distributed Autonomous Organization (DAO) or Corporation (DAC)

Traditional organizations or corporations consist of a Board of Directors that employs managers and other employees to pursue a specific mission according to a set of by-laws and within a business environment structured by laws, regulations and jurisprudence. The Board is accountable to members or shareholders for how well the corporation meets its goals which are usually set out in a mission statement – supplemented by legal and regulatory frameworks which further define its duties.

A distributed autonomous organization (DAO) or corporation (DAC) is an entity that would replace the functions performed by the corporation's by-laws, mission statement and employees – and potentially the Board – with a set of smart contracts that could control capital in a digitally native value system, collect information from pre-specified sources via the Internet, analyze this information using machine learning algorithms. On the basis of this analysis the DAO/DAC would take actions, such as making investments, designed to advance its objectives within the applicable legal and regulatory frameworks. While functionally equivalent to a traditional corporation, the current legal status of such, still largely theoretical, entities is unclear.[126]

[126] Malta has recently adopted a legal framework recognizing DAOs/DACs (which it refers to as "technological arrangements") as similar to a traditional limited company with many of the same rights and duties. See Ronstedt, M. and Eggert, A. 4 July, 2018. "Among Blockchain-Friendly Jurisdictions, Malta Stands Out." Coindesk. https://www.coindesk.com/among-blockchain-friendly-jurisdictions-malta-stands-out/.

[127] Some thinkers have already suggested that such vehicles, legally owned by not-for-profit DAOs and directed by powerful machine learning algorithms, could be created and mandated to provide inexpensive mobility to marginalized communities. Kelion, L. 16 February, 2015. "Could driverless cars own themselves?" News. *BBC*. http://www.bbc.com/news/technology-30998361.

flight insurance policy that paid customers automatically if their flight was more than two hours late.[128]

Smart contracts raise a number of important questions. Currently, the control of courts and quasi-judicial agencies by humans like judges enables human discretion and common sense to intervene in the performance of a contract if necessary, such as when extenuating or mitigating circumstances arise. If a contract is self-executing and hosted on a blockchain, however, it may be the case that nothing can be done to stop automatic performance of the contract – even if the results end up being monstrous, unintended or in conflict with other laws.[129] For example, any contract agreed to under duress would be a candidate for nullification by a court of law. But, if uploaded as a smart contract for performance on a domicile-less global blockchain, such nullification may not be possible even if backed by a court order.

Similarly, sometimes monetary compensation for breach of contract may be a preferable alternative to performance by one of the parties. While it may be possible to ensure options like this are written into smart contracts, it may be necessary to legally require inclusion of "escape clauses" of this type for them to actually be included given that increasing automaticity would likely represents one of the key motivations for using a smart contract.

Other emerging challenges that blockchains could sharpen – especially when they intersect with issues like automatic performance – include questions of transparency and equity in the use of algorithms to determine everything from who gets a job interview or a car loan to the length of a convict's sentence.[130] We raise these questions not out of alarmism: the posing of novel legal puzzles is a necessary corollary of the emergence of any new area or form of human activity. But it will take some time for courts, regulators and legislators to figure out the optimal governance frameworks for these areas. In order to minimize the harm that is caused during this period of transition, governments and regulators need to be thinking ahead, aggressively developing their own capacity, consulting with stakeholders, educating the public and actively piloting potential responses.

Governance

We described earlier how blockchains may create competition for states in the market for governance services. While this certainly raises the question of how governments might compete with these new providers, it also raises the question of how these providers and services ought to be governed.

The infamous hack of "The DAO" in 2016 provides a helpful example of some of the issues that governments will need to think about in respect of blockchain governance.[131] In this case, hackers exploited a flaw in the smart contracts that comprised "The DAO" – an autonomous corporation that had been built on top of the Ethereum blockchain – and "tricked" it into transferring around $55 million (USD) worth of

[128] Higgins, S. 13 September, 2017. "AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product." *Coindesk*. https://www.coindesk.com/axa-using-ethereums-blockchain-new-flight-insurance-product/.

[129] The authors thank Katie Szilagyi for bringing this issue to our attention.

[130] See O'Neil, C. 2017. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* New York: Broadway Books.

[131] Note, in this case "The DAO" refers to a specific decentralized autonomous corporation that was generically, and confusingly, named "The DAO".

ether to an account they controlled.[132] It's likely that no laws were broken by the hackers because the creators of "The DAO" had specifically stated that the software that comprised "The DAO" was itself the authoritative version of the contracts between the corporation and the investors and that any other information about the corporation, its purposes and its operations were superseded by the logic encoded in this software. According to this interpretation, anything the software was capable of doing would be, by definition, in line with the contracts that governed "The DAO" and thus legal.

Nevertheless, investors in "The DAO" who lost money were understandably upset. Moreover, the Ethereum community was very concerned that, despite the fact that the Ethereum platform itself had not been compromised and was not at fault, this incident would cause irreparable harm to the larger Ethereum project simply by association. The Ethereum community eventually decided to "hard fork" the underlying Ethereum blockchain at a point prior to the hackers' transfer of the contested funds to allow the former owners of the ether in question to recover it.[133]

This decision created a major controversy and resulted in a split of the Ethereum blockchain into two distinct blockchains. Most miners and users agreed to move forward with the hard fork and the new version of Ethereum. A small minority of miners and users balked, however, and suggested that the hard fork was essentially analogous to a mob-mandated retroactive changing of the law that constituted a theft of $55 million from the hackers who had done nothing wrong beyond reading "The DAO's" fine print more carefully than everyone else.[134] This small minority argued that doing so betrayed the entire idea of censorship resistance and decided to continue using the old version of the Ethereum blockchain, which came to be called Ethereum Classic, on which the hackers were still in possession of the "stolen" funds.

This controversy largely turns on the idea that the entire point of an autonomous organization like "The DAO" is to remove arbitrary human decision-making and recognize that "code is law."[135] Indeed, because code was meant to be law, the need to hard fork the Ethereum blockchain was unexpected and the entire procedure by which the decision was made was created on the fly without any pre-existing agreed-upon governance or decision-making processes.

Ethereum is not alone in having faced such problems. Bitcoin has also experienced a number disagreements – largely concerning whether block size should be increased – which have led to hard forks that have created alternate versions of the currency such as Bitcoin Cash and Bitcoin Gold. While less acute than "The DAO" incident, these conflicts also exposed a lack of governance infrastructure in the Bitcoin community – at least as governance is traditionally understood.[136]

[132] The Economist. 25 June, 2016. "Theft is property." *The Economist*. https://www.economist.com/news/finance-and-economics/21701136-cyber-attacker-outsmarts-smart-contract-theft-property.

[133] The "hard fork" described here is similar to the fork described in Section 3 except that in addition to going back in time on the blockchain and forking it at an earlier point in the record of transactions, this fork also involved simultaneously changing the underlying software that operated the blockchain. These sorts of changes to the blockchain's operating software are called either "soft forks" – which refer to changes that maintain backwards compatibility with previous versions of the software – and "hard forks" which do not.

[134] Schumpeter. 28 June, 2016. "Not-so-clever contracts." *The Economist*. https://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted.

[135] Lessig, L. 1 January, 2000. "Code Is Law: On Liberty in Cyberspace." *Harvard Magazine*. https://harvardmagazine.com/2000/01/code-is-law-html.

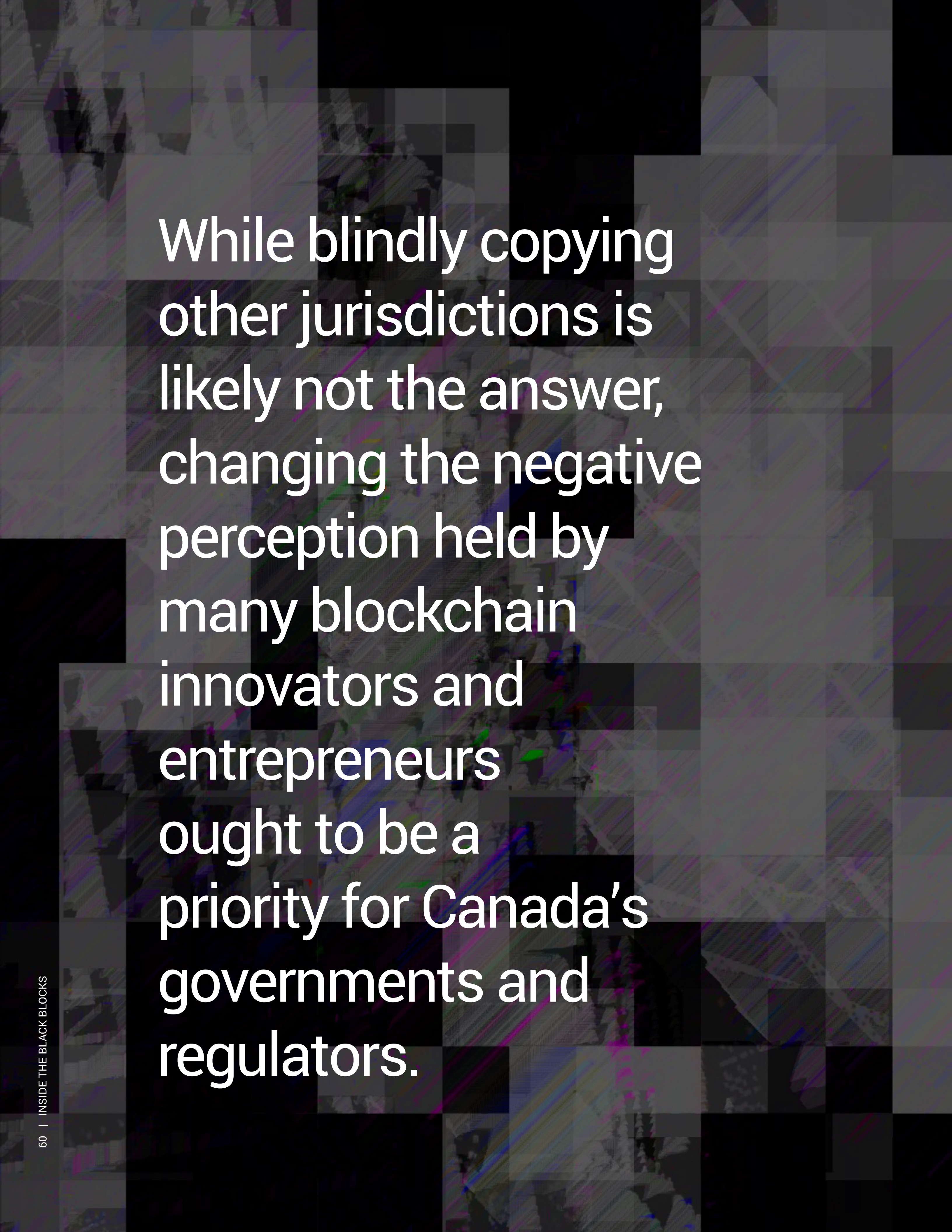
[136] An account of Bitcoin's "Civil War" can be found in Casey, M. and Vigna, P. 2018. *The Truth Machine*. Pages 71-79.

Ultimately, all these controversies were resolved by having the users and miners decide for themselves which versions of these blockchains they wanted to continue using. At one level this is actually quite democratic – no one is forcing anyone to use any of these blockchains. But this emerging "vote with your feet" approach to governance – which one can also discern in e-residency's limited empowering of individuals to shop around for the government they like best – is a novel way to govern a community, at least in a context where digital tools make it much easier to implement than previously. While this might be exciting to some, especially libertarians, it's pretty clear that governments are only just beginning to think through the potential implications of the spread of this approach.

In fact, as blockchains continue to grow in size, importance, and ubiquity, governments may find that the use of a "vote with your feet" approach is not desirable in all cases of conflict with the results of their own decision-making procedures and political processes. Situations may arise where they find they have a much stronger desire or need to become involved in blockchain governance. For instance, how large a proportion of a country's economic activity will need to be conducted using Bitcoin before that country decides it needs to find some way to exercise some control over the currency? If code is law, then those who are impacted by the code will eventually – and reasonably – want there to be a fair, predictable, transparent and democratic procedure for how that code can be changed short of walking away from it.

Moreover, even if they end up ceding the market for some "governance services" to new competitors, governments will not be able to wash their hands of the need to ensure that these services are delivered to their citizens in ways that adhere to constitutional requirements or obligations under international treaties. For a variety of reasons, not everyone has the same ability to walk away and governments have a responsibility to ensure that these individuals are not inequitably disadvantaged, regardless of what others do.

The questions raised by this incipient "vote with your feet" approach to governance represent only a sub-set of a host of questions that could be raised by the emergence of blockchain and to which governments will need to respond. How for instance might the "right to erasure" guaranteed by the EU's General Data Protection Regulation (GDPR) be given effect on an immutable public blockchain? How should governments reach accommodations with the private networks that operate blockchains – or conceivably with non-human DAOs? Alternatively, how might governments stop DAOs offering illegal services via blockchain if these decentralized, distributed entities have no national domicile? While the answers to these questions remain to be determined, one thing that is clear is that governments need to not only begin thinking about them, but to also start actively working to shape the decisions that will need to be taken. This will involve working to influence when these questions make it onto the agenda and the fora in which decisions about them are taken.



While blindly copying other jurisdictions is likely not the answer, changing the negative perception held by many blockchain innovators and entrepreneurs ought to be a priority for Canada's governments and regulators.

6 RECOMMENDATIONS

Developments in the blockchain community are moving very quickly. When we approached one blockchain entrepreneur for an interview, his response was to ask: “Why are you doing research so late in the game when there are lots of others that have done extensive research?” It was almost as if he was saying that if you are not already up to speed on blockchain, you might as well not even try to catch up.

If this report represents your first thorough engagement with blockchain, this type of response can be deflating and concerning. But, while it is true that government has some catching up to do, we suggest taking this quotation as we took it: as a reminder that events are moving fast and a spur to get a move on, certainly, but also as a reminder of the need to be wary of some of the exuberance, skewed perspectives and self-promotion that pervade the industry.

In this final substantive section, we offer the following five recommendations to policymakers:

» Build internal capacity

» Create an attractive environment for blockchain innovation

» Support internal and allied experimentation

» Make use of standards and other flexible tools

» Foster national and global governance cooperation

Implementing these recommendations will help governments capture the potential benefits offered by blockchain and avoid its pitfalls.

Build internal capacity

Given that blockchain is such a new development, it should not be surprising that the level of blockchain expertise and capacity within Canadian governments and regulators is currently limited.[137] One of the first steps that governments need to take in preparing for the impacts of blockchain is to increase their own internal capacity. In the first instance, this means building up groups of technologists and policymakers within government who understand the technology, its implications and the potential opportunities and challenges that flow from it.

It is encouraging that Canadian governments are alive to this challenge and the need to increase their internal capacity. Indeed, many have already taken some important initial steps:

» Innovation, Science and Economic Development Canada has been involved as a partner in blockchain proofs of concept and pilot projects with a number of provincial and municipal government partners.

[137] Stein, S. 14 February, 2018. “Blockchain engineers are in demand.” *TechCrunch*. https://techcrunch.com/2018/02/14/blockchain-engineers-are-in-demand/.

» Treasury Board Secretariat recently hosted a Government of Canada Blockchain Codefest and a Blockchain Day conference to advance the federal government's understanding of the technology.

» The National Research Council of Canada has experimented with using the Ethereum blockchain as a way of executing and posting grant and contribution agreements which it already discloses publicly.

» As discussed in section 5, the Government of Ontario and the City of Toronto ran a proof of concept designed to investigate potential uses of blockchain technology in increasing the ease of use and efficiency for the restaurant permitting process. The Government of Ontario also recently ran a blockchain hackathon that generated a number of ideas for other blockchain applications in government.

» As noted in section 5, the Government of British Columbia will soon be launching its Verified Organization Network (VON) with the aim of putting government permits and other "verifiable claims" on a blockchain and, eventually, enabling individuals and businesses to use their own digital wallets to prove their credentials to third parties.

» Project Jasper is a joint initiative between the Bank of Canada and a variety of other financial institutions and actors. Jasper's first and second stages involved the building and testing of a "CADcoin," a DLT-based interbank payments settlement instrument.[138] Jasper's third stage, on which the Bank of Canada is partnering with Payments Canada and Toronto Stock Exchange operator TMX Group Ltd, is focused on testing the use of DLT for improving the security settlements process.[139]

These are all positive steps but they will need to continue and multiply. As we have previously recommended in the context of the relationship between government and disruptive technologies, proofs of concept and pilot projects[140] – really any initiative that provides hands-on experience – are critically important to building capacity. Additionally, governments should pursue:

» Greater encouragement of secondments and interchanges with external blockchain and DLT firms and organizations by government staff.

» Fellowships and other programs designed to attract academics with blockchain expertise to work in the government for a set period of time.

» Specific, carefully designed and well-supported programs for private sector technologists to do a "tour of duty" in government for a set period of time or for a specific blockchain or DLT project.

» Greater encouragement of, and support for, existing government employees to pursue educational leaves to upgrade their blockchain and DLT knowledge and skills.

» Better integration of new learning opportunities like micro-credentials and nano-degrees targeted at enhancing government employees' capacity in blockchain and DLT.

Critically, these recommendations need to go beyond simply building internal technical capacity. While some technical capacity will be essential for governments to be able to identify, procure, implement and manage blockchain

[138] Wilkins, C. 19 May, 2017. "Project Jasper: Lessons From Bank of Canada's First Blockchain Project." *Coindesk*. https://www.coindesk.com/project-jasper-lessons-bank-of-canada-blockchain-project/.

[139] Reuters Staff. 17 October, 2017. "Bank of Canada, TMX to test blockchain for securities settlement." Reuters. https://www.reuters.com/article/us-boc-tmx-grp-blockchain/bank-of-canada-tmx-to-test-blockchain-for-securities-settlement-idUSKBN1CM30X.

[140] Johal, S. and Urban, M. 11, May, 2017. *Regulating Disruption*. Pages 28-29.

and DLT use cases in the public sector, many of the most important challenges this technology creates lie in its implications for policy, regulation and the law. Not only does government need to upgrade its technical capacity, it needs to build familiarity and upgrade its understanding of the technology's non-technical implications throughout government and society.

Given that governments exist in an environment of fiscal restraint, building up the capacity of those parts of government that will grapple with the challenges and opportunities associated with blockchain's emergence should be prioritized. This list ought to include regulators that are already confronting these new developments such as securities commissions, as well as those entities that have the most obvious immediate uses for the technology such as shared and government services agencies.

Given their central role supporting other departments, central agencies should also be a focus for capacity building, especially on the policy side. Existing policy innovation organs, such as Ontario's Policy Innovation Hub, could even be directed to develop an internal government consultancy function to support other parts of government. Finally, ensuring that senior executives understand blockchain at a sufficient level so that they are able to effectively integrate blockchain and DLT-related policy advice into their decision-making will also be critical.

Building a strong understanding of the non-technical aspects of the technology will, ultimately, be even more important for managing not just how government itself uses blockchain, but also how it modifies its policy, regulatory and legal frameworks to address the challenges and seize the opportunities that the technology presents for society at large. Moreover, it is precisely these sorts of individuals who will be critical to the successful implementation of many of our additional recommendations.

Finally, one of this report's reviewers suggested that even before an organization starts to build capacity, it is critical to ask "do we actually have a use case' for blockchain? Is blockchain relevant to our work in a way that offers substantially superior results compared to existing approaches?" These are critical questions to ask and it is true that not every government department or agency will require in-house blockchain capacity. Awkwardly, being able to answer these questions itself requires a significant level of blockchain expertise. This underlines the importance of government as a whole, and central agencies in particular, developing nimble and re-deployable capacity able to facilitate the sorts of analyses which individual departments and agencies that cannot (yet?) justify their own build-up of capacity will need.

Create an attractive environment for blockchain innovation

Even with a commitment to increasing internal capacity, it is unrealistic to expect that government will be able to compete with the private sector for the best and brightest blockchain innovators.[141] But, given the relative strength of Canada's homegrown blockchain talent,[142] Canadian governments have a good opportunity to build and support an innovative blockchain ecosystem in Canada. By doing so, and by building strong relationships with this sector, governments should be able to leverage this sector and its expertise in many of the ways described above. Successfully building and maintaining this sector, however, will depend on governments' abilities to create an environment capable of attracting blockchain entrepreneurs and innovators and retaining them. [143]

Some other jurisdictions have already taken significant steps in this direction.[144] The town of Zug in Switzerland has, for example, been dubbed "Crypto Valley" for its government's enthusiasm for encouraging blockchain and related firms to locate there. Not only do many local stores accept payment in bitcoin, but so too does the local government for many taxes and fees. Given this approach, it is not surprising that four out of 2017's ten biggest ICOs were based in Zug – a town of just under 30,000 people.[145]

Other jurisdictions are also staking claims to being one of the world's blockchain hubs. For example, the US state of Delaware, seeking to build on its existing dominance in corporate formation and the expertise of its business courts, was the first jurisdiction in the world to explicitly allow corporations to maintain their corporate shares using a blockchain-based ledger.[146] It is also looking at enabling the creation and maintenance of certain legal documents that often interact with shares on this blockchain and to enable shareholder voting through blockchain technology.[147]

Encouragingly, Canadian governments and regulators are trying to move in this direction. For instance, the Canadian Securities Administrators (CSA) – an umbrella organization for Canada's provincial and territorial securities regulators – has produced a number of staff notices to provide entrepreneurs and firms with insight into the evolution of regulators' views. In its most recent notice, it even recognized the possibility of there being a difference between a utility token and a security token – a significant regulatory step.[148]

[141] Indeed, demand "is off the charts" with "14 job openings for every one blockchain developer." See Stein, S. 14 February, 2018. "Blockchain engineers are in demand."

[142] Canada was ranked third in terms of the number of blockchain start-ups behind the USA and the UK with the Toronto area accounting for much of this activity. Blatchford, A. 28 February, 2017. "Ottawa explores potential of 'blockchain,' billed as next-generation Internet tech." *The Toronto Star*. https://www.thestar.com/business/2017/02/28/ottawa-explores-potential-of-blockchain-billed-as-next-generation-internet-tech.html.

[143] In this light, the failure of the proposed blockchain supercluster application to even make the shortlist in the federal government's supercluster selection process represents a missed opportunity. See https://www.canada.ca/en/innovation-science-economic-development/news/2017/10/innovation_superclustersinitiativeshortlistofapplicants.html.

[144] Popper, N. 29 July, 2018. "Have a Cryptocurrency Company? Bermuda, Malta or Gibraltar Wants You." *The New York Times*. https://www.nytimes.com/2018/07/29/technology/cryptocurrency-bermuda-malta-gibraltar.html.

[145] The Economist. 24 February, 2018. "A banking centre seeks to reinvent itself." *The Economist*. https://www.economist.com/finance-and-economics/2018/02/24/a-banking-centre-seeks-to-reinvent-itself.

[146] Adlerstein, D. and Tinianow, A. 21 April, 2018. "Why ICOs Could Eat Delaware's Lunch."

[147] Stromberg, T. Negre, J. Reinhardt, M. Peleg, M. 23 March, 2018. "Are Headwinds Hampering Delaware's Blockchain Initiative?" *Law360*. https://jenner.com/system/assets/publications/17844/original/stromberg%20Law360%20March%2023%202018.pdf?1521837416.

[148] Canadian Securities Administrators. 11 June, 2018. "Securities Law Implications for Offerings of Tokens." *CSA Staff Notice* 46-308. http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm.

The CSA's regulatory sandbox (see Box 8),[149] is another good example of regulators seeking to be flexible and meet the needs of blockchain innovators.

Despite these laudable efforts, Canada is not currently seen as a leader in the regulation of digital assets. Many of our interviewees who are active in the blockchain sector suggested that their interactions with Canadian governments and regulators had not been particularly encouraging. Some complained of delays and unresponsiveness from regulators as well as unclear guidance. One even suggested that by the time that this report was published, there was a good possibility that they would have moved to another, more supportive, jurisdiction.[150] Another declared bluntly that "the brain drain is real" and that Canada has lost many of the advantages that it enjoyed in blockchain even just a few years ago.

Unfortunately, even though the regulatory challenges posed by blockchain are not unique to Canada, the regulatory uncertainty that has persisted here has eroded some of Canada's attractiveness among entrepreneurs. While blindly copying other jurisdictions is likely not the answer, changing the negative perception held by many blockchain innovators and entrepreneurs ought to be a priority for Canada's governments and regulators.[151]

BOX 8
Regulatory Sandbox

A program operated by a regulator which provides enrolled firms temporary exemptive relief from certain regulatory or legal requirements. The relief offered to firms is usually delimited in scope – up to a certain number of transactions or customers – or in duration. The purpose of a regulatory sandbox is to enable successful applicants to test new and potentially innovative and beneficial products and services whose development might otherwise be discouraged by existing regulatory or legal frameworks. Ideally, this relaxed regulatory environment will be coupled with tailored and ongoing engagement by the regulator with successful applicants as a means of facilitating innovation, protecting consumers and enabling regulators to learn about new innovations and potential regulatory changes they should consider.

[149] See https://www.securities-administrators.ca/industry_resources.aspx?id=1588.
[150] See also The Economist. 24 February, 2018. "A banking centre seeks to reinvent itself."
[151] To be fair, Canadian regulators' responses to blockchain innovations are in line with Canada's generally prudential approach to financial regulation, an approach that was much lauded during the most recent global financial crises. It may also be the case that some jurisdictions with more lax approaches are actually engaging in a "race to the bottom" and reducing their regulations imprudently. Thus, Canadian regulation of digital assets also likely represents, at least partially, a conscious decision to proceed with caution, even if it means losing out on some homegrown blockchain innovation.

One way to build a more attractive environment for innovation is to get more creative. One interviewee suggested that one particularly useful way of doing this would be to try and find ways of aligning regulatory requirements for innovators with the way that the "crypto community" itself thinks about blockchain while still ensuring that the principles behind these regulatory regimes were being applied. To see how this might be accomplished, consider the following example.

Many financial institutions have a set of regulatory responsibilities collectively called "know your customer" (KYC). Depending on the product or service being offered, one part of KYC is a requirement for the institution to take steps to understand an investor's strategies, expectations and level of sophistication and to then tailor their offerings to this customer accordingly. Currently, such "client-onboarding" can take significant time and involve questionnaires, the submission of documentation and numerous other due diligence activities. Our interviewee suggested that a creative way for blockchain firms to fulfil some of their KYC requirements around investor sophistication might be to allow firms to use technical indicators to provide this information, an approach that aligns with a lot of current thinking in the crypto community.

For instance, if a buyer wanted to use a cryptocurrency to purchase another crypto-asset, as opposed to a fiat currency-denominated credit card, this would be taken to indicate a higher than average level of investor sophistication. The use by a buyer of a personal crypto-wallet in this transaction instead of an account at a crypto-exchange would be taken to indicate an even higher level of sophistication. The motivation for using such an approach as a part of KYC due diligence would be that it could reduce the regulatory burden on firms and customers, while still achieving the underlying objectives of the regulatory framework, namely to determine the level of the investor's sophistication.

This idea is not offered as a specific recommendation, but as an illustration of the sort of creative thinking being advocated. One way to identify creative ideas like this would be to increase efforts to build a strong network of relationships between policymakers, regulators and entrepreneurs and technologists. Some of the capacity building tools identified earlier, specifically those that encourage exchanges of personnel like the successful Presidential Innovation Fellows program in the US,[152] could go a long way to building these relationships and a culture of innovation within government. While governments and regulators will often have different priorities and responsibilities than entrepreneurs and should thus be wary of regulatory capture, it is exactly these sorts of exchanges which could boost Canada's regulatory innovation and attractiveness.[153] Such insight will be especially important in the case of blockchain, given the many novel regulatory challenges the technology will create.

Another positive step that could be taken would be to create standing advisory committees designed to bring industry, consumer, and community members with a stake in specific potential blockchain implementations into contact with policymakers working in the space. These committees could offer technical advice, sector intelligence and serve as conduits to additional expertise, as well as offering an important challenge function for proposed

[152] Ehlinger, S. 9 January, 2017. "Effort to codify Presidential Innovation Fellows program is back in House." *Statescoop.* https://statescoop.com/effort-to-codify-presidential-innovation-fellows-program-is-back-in-house.
[153] Johal, S. and Urban, M. 11, May, 2017. *Regulating Disruption.* Pages 18-19.

government blockchain applications or policies. Increased self-organization within the blockchain industry could also help to provide government with a more robust interlocutor.

Support internal and allied experimentation

As was highlighted earlier, one effective way for governments and regulators to build improved internal capacity and better relationships with stakeholders is to actively support the piloting of potential use cases of blockchain and DLT in the broader public sector.

Supporting pilots might be especially productive at a local level or in partnership with a small set of connected institutions such as a hospital and a network of medical clinics. By starting small, governments limit risk and enable themselves to develop internal expertise before the stakes become very high. Moreover, by starting local but working collaboratively, these projects can help spread risk between the partners. This is important as some of the best candidates for the sorts of low-risk implementations ideal for piloting lie with municipal governments that might otherwise lack the funds or expertise needed. Federal and provincial governments would benefit from providing funds and expertise by gaining the opportunity to learn with only low levels of risk.

These sorts of projects would also enable multiple levels of government to connect with and gain experience collaborating with private sector firms and entrepreneurs. One of the complaints most often heard from technology entrepreneurs in Canada is that they lack large institutional reference customers like government – something they argue disadvantages them as they work to scale up their businesses.

By piloting, governments could respond to complaints like this and begin to build the expertise and trust they need to move on to larger partnerships in the future. Such an approach would also help to advance Canadian governments' oft-stated desires to nurture homegrown technology start-ups and help these companies scale up their operations while remaining in Canada.

Finally, it is important that governments do not attempt to develop large blockchain solutions aimed at replacing numerous legacy systems in a single "Big Bang." As demonstrated by repeated failures, delivering massive information technology systems of this type rarely works well or stays on budget. Nimble approaches that start with small scale tests and are designed to grow iteratively in ways that gradually integrate with procurement schedules and lifecycles of existing systems are more likely to succeed. One of the characteristics of blockchain and DLT that make them particularly suitable to such an approach is how they can be designed to connect to and coordinate other systems and expand organically over time, thereby avoiding the need for risky and highly complicated system-wide overhauls.

Make greater use of standards and other flexible tools

As was discussed in Section 4, blockchain will likely entail a reduction in the effectiveness of negative regulatory approaches and the emergence of several novel legal questions. For governments and regulators looking to protect the public interest in this changing environment, this will likely mean some shifts in emphasis and the adoption of some new tools.

One good example of a context in which new tools are needed is ICOs. While many ICOs are helping innovators get their ideas off the ground, some are clearly frauds.[154] Ostensibly, there are regulatory bodies such as the Ontario Securities Commission (OSC) that are mandated to protect investors from these sorts of scams. But, given that many ICOs are both accessible via the Internet and based in other jurisdictions to which the OSC's authority does not extend, it is essentially impossible for the OSC to use its traditional negative tools, such as fines or blocking the listing of a security on an exchange, to protect investors.

The development of standards represents an alternative, positive approach worth exploring in this regard. The idea would be to create and publicize a standard that included a set of requirements around disclosure and reporting that firms undertaking ICOs would need to meet in order to have their offering receive accreditation.[155] A list of ICOs achieving this level of accreditation could even be hosted on a public blockchain maintained by regulators.

Standards might not be as effective as negative regulatory tools were in earlier times, but they would likely be much better than the current situation in which securities regulators' ability to respond effectively to ICOs has been greatly impaired. Ideally standards could be developed in cooperation with organizations like the CSA and OSC. This is important because the reality is that there is a growing appetite for ICOs and there is little that regulators will be able to do to stop motivated individuals from participating in this market. By reconsidering their approach instead of sitting on the sidelines, regulators would be able to offer some form of protection where otherwise there would be none. While this may not be an ideal solution, it could at least help to rein in some of the excesses of the sector.

In addition to providing a helpful regulatory tool, standards will also be essential in ensuring that blockchain is able to reach its full potential in terms of impact. For instance, given some of the challenges around the scalability of public, permissionless blockchains, it is likely that there will be many, many blockchains operating in the future. In this context, blockchains will need to be compatible and interoperable in order to maximize their usefulness. One need look no further than the example of how common protocols like TCP/IP were critical to unlocking the Internet's potential in order to see the importance of interoperability. By allowing different blockchains to integrate easily with each other and enabling crypto assets to move between blockchains, the development of widely accepted crypto-standards could play a significant role in unlocking blockchain's full potential.

[154] Matsakis, L. 30 January, 2018. "Cryptocurrency Scams Are Just Straight-up Trolling at this Point." *Wired*. https://www.wired.com/story/cryptocurrency-scams-ico-trolling/.
[155] In the UK, the TrustSeal standard has been developed along similar lines for accrediting firms offering sharing economy services. See https://sharingeconomytrustseal.com/about/.

One example of how this is already occurring can be found in the creation of the ERC-20 token standard developed by the Ethereum Foundation – the body that more-or-less administers the Ethereum blockchain. The ERC-20 standard is the most popular standard for start-ups conducting an ICO. Given that the Ethereum Foundation is a not-for-profit foundation that is generally perceived as playing a fairly benevolent role, there has not been too much concern about it playing a standard setting role so far. Regardless, as blockchains like Ethereum grow in importance, governments will be forced to decide if they are willing to allow very new organizations, with unclear accountability structures and essentially no democratic legitimacy, to make very consequential decisions with little-to-no opportunities for national governments to influence how these decisions are made.

Farther along the line, governments will need to confront some of the more novel legal questions that the development of a digitally native value system and the emergence of smart contracts entails. The creation of standards for smart contracts, or even open source model contracts, could be useful. Indeed, there are already examples to draw on. In the USA, the Mortgage Industry Standards Maintenance Organization (MISMO) has created a set of standards that show how a specific form of legal contract can be standardized under the supervision of an independent organization that is scrutinized by government or regulators to ensure respect for the public good.[156] In this approach, there could be a requirement that any deviations from the model contract would need to be explicitly signalled to the user and justified before the contract could be signed.

Whatever standards are adopted, enforcement might require inventiveness. For instance, regulators could consider working with academics to create open source algorithms capable of scanning smart contracts for adherence to specific standards. Blockchains that run smart contracts could also be explicitly programmed to block the performance of certain types of contractual terms.[157] Whatever the specific form it took, the key feature of this approach would be to move away from unenforceable prohibitions and towards proactive measures to provide individuals and firms with tools they could use to protect themselves.

Foster national and global governance cooperation

Blockchain is a global phenomenon and, consequently, a significant proportion of any successful attempt at governing it will necessarily take place at the global level. Unfortunately, the critical importance of improved national and international cooperation by governments and regulators is an area currently receiving insufficient attention. More governmental cooperation will be essential to overcoming some of the most important challenges that blockchain will create.

With regard to blockchain Canada currently faces three main challenges with international dimensions. The first one is familiar: jurisdictional arbitrage. Jurisdictional arbitrage refers to how individuals, networks and firms can leverage differences in jurisdictions' regulations in ways that advantage them, often at the expense of at

[156] See http://www.mismo.org/.

[157] This is arguably what occurred in "The DAO" debacle with Ethereum, though the decision not to enforce the terms of the contract was ad hoc and applied retroactively.

least one jurisdiction.[158] A common example is for a firm to declare profits in one jurisdiction that were actually generated in a second jurisdiction where a higher corporate tax rate was in effect. This is already encouraging a sub-optimal race to the bottom among jurisdictions as they attempt to attract firms by enacting lower and lower tax rates and increasingly lax regulatory environments that end up sacrificing the wider public interest.[159] There may already be a race to the bottom taking place to attract blockchain firms, which is a problem in its own right. But, by making it easier to move value around digitally, blockchains may also make it more difficult to combat jurisdictional arbitrage by firms in other sectors as well, worsening an already serious problem.[160]

Second, the decentralized and distributed nature of blockchain makes it difficult for governments to combat undesirable forms of activity that use it, such as tax evasion or money laundering.[161] It also makes it difficult to impose requirements on blockchains that operate in other jurisdictions – such as the idea mentioned earlier about disabling certain contractual terms. These challenges will grow in importance as an increasing amount of financial activity moves out of national currencies and onto blockchain networks.[162] While even perfect international cooperation is unlikely to stop blockchains from being used for undesirable activities, individual countries will find it extremely difficult to take meaningful action against these activities because of their distributed, even ephemeral, character.[163]

The best hope governments have in this regard is working together and presenting as united a front as possible. Thus, in addition to developing methods for regulating activities "on-chain" as discussed in earlier subsections, governments will also need to improve their ability to cooperate effectively "off-chain."

Third, just as the non-territorial nature of blockchains makes it difficult to negatively enforce national laws, it also offers opportunities for powerful governments to try and impose their preferred solutions extraterritorially across the entire network by leveraging their "off-chain" power. In other words, these governments may seek to develop standards that advantage them and use their power in the physical world to impose or induce their acceptance globally. While having uniform standards might be desirable in abstract, Canadian citizens are unlikely to want to simply accept standards developed and unilaterally imposed on them by others without their input. To ensure that Canadian perspectives and interests are integrated into

[158] For a more in-depth discussion see Johal, S. et al. 30 July, 2017. *Robots, Revenues & Responses*. Pages 33-35.

[159] The Organisation for Economic Cooperation and Development's (OECD) Base Erosion and Profit Shifting (BEPS) task force estimates that these sorts of practices "cost countries 100-240 billion USD in lost revenue annually, which is the equivalent to 4-10% of the global corporate income tax revenue." G20 and OECD. July 2018. *Inclusive Framework on BEPS: A global answer to a global issue*. OECD. http://www.oecd.org/tax/flyer-inclusive-framework-on-beps.pdf.

[160] A recent study found that "The average corporate tax rate globally has fallen by more than half over the past three decades, from 49 percent in 1985 to 24 percent in 2018." Stein, J. 24 July, 2018. "Across the globe, taxes on corporations plummet." *The Washington Post*. https://www.washingtonpost.com/business/2018/07/24/across-globe-taxes-corporations-plummet/?noredirect=on&utm_term=.1e9489353c71.

[161] The Economist. 26 April, 2018. "Crypto money-laundering." *The Economist*. https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering. The head of Europol estimates that already 3-4% of criminal revenues in Europe is laundered through cryptocurrencies.

[162] Johal, S. et al. 30 July, 2017. *Robots, Revenues & Responses*. Pages 40-41.

[163] A good example was the Spanish government's inability to disrupt the online aspects of the referendum in Catalonia because of how the Catalan government used a decentralized protocol, the InterPlanetary File System (IPFS) to disseminate information about where and when to vote. Dedi, D. 23 October, 2017. "IPFS's first win: the Catalan referendum." *CryptoInsider*. https://cryptoinsider.com/content/ipfs-first-win-the-catalan-referendum/index.html.

the processes that produce these standards, Canadian governments, firms and non-governmental organizations need to be proactive in engaging other interested parties and working constructively to fill the existing regulatory vacuum.

While concrete international action on blockchain is probably not yet warranted, countries like Canada should already be engaging like-minded states in multilateral discussions on how to collaboratively solve the problems that blockchain will create. International organizations such as the UN, the G20 and others could play a larger role in helping to create a consistent international framework that can help limit a regulatory race to the bottom, keep these new technologies from contributing to problems like tax-base erosion, and ensure they contribute to the greater good.[164] For example, the UN Commission on International Trade Law (UNCITRAL) could potentially serve as a good forum for the development and dissemination of "model laws" that address these problems or for preparing and building support for an international convention on blockchain governance.[165]

Additionally, Canada should ensure that its interests and perspectives are represented in any international exercises in standard setting. An ISO technical committee (ISC/TC-307), led by Standards Australia, is already working on ten standards for blockchain and DLT.[166] From our interviews, we understand, albeit from second-hand sources, that Canada is participating in this exercise but that the Canadians involved are not receiving as much support as they ought to be. Moreover, other interviewees suggested the ISO process may, ultimately, be of only marginal importance. They suggest that governments really need to get over their unwillingness to get involved in the standards development work being done in "consortia" contexts – where small groups of private firms develop standards – and also begin to explore how they might interface with the governance discussions occurring around the most important public blockchains like Ethereum and Bitcoin.

[164] See, for instance, Maupin, J. March 2017. "Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy." *Policy Brief* No. 101. CIGI. https://www.cigionline.org/sites/default/files/documents/PB%20no.101.pdf. At the moment, the G20 has not yet taken any concrete steps: Suberg, W. 23 July, 2018. "G20 Forum Shelves Deadline for 'Very Specific Recommendations' on Crypto." *CoinTelegraph*. https://cointelegraph.com/news/g20-forum-shelves-deadline-for-very-specific-recommendations-on-crypto.

[165] Models laws are legislative drafts developed by legal experts working for UNCITRAL and on the basis of the organization's consultations with UN member states. States are invited to use these expertly-drafted model laws as the basis for national laws. See http://www.uncitral.org/uncitral/en/about_us.html.

[166] These include standards on privacy, security, terminology, identify management, and smart contracting. See https://www.iso.org/committee/6266604.html.

Over the time that this paper was researched and written, the price of a single bitcoin has gone from about $1,200 to over $25,000 and is now back to about $10,500 (CAD).

7 CONCLUSION

As stated in the Introduction, this report is not designed to be a comprehensive discussion of blockchain or its applications. What it does aim to do is to provide policymakers with a fundamental understanding of the key concepts and the basic intellectual tools they will need to continue their exploration of this new technology with greater confidence. Thus, we close this report by summarizing the three key thematic takeaways from our research and by offering a gentle warning regarding the role that is being played by hype in the blockchain sector.

Key Takeaways

Blockchain can be a complicated topic and with so much going on in terms of new ICOs launching, companies and governments announcing new proofs of concept, and enthusiasts offering fantastical speculations, identifying what is important can be difficult. Our research has led us to believe that there are three fundamental conclusions that policymakers need to be aware of and need to integrate into their thinking:

1] **Blockchain marks the arrival of the first digitally native value system.** Blockchains enable the creation of a digitally native value system which in turn lays the foundation for potentially revolutionary automation in new areas. By enabling software to more easily manipulate value and by helping to make smart contracting much easier, blockchains will enable software to do many new and important things that it cannot do today.

2] **Blockchains and distributed ledgers also offer other less revolutionary, but still significant, ways of organizing and coordinating information systems and tracking a variety of assets.** These implementations will enable greater efficiency and decentralization which could help secure greater privacy and a more even distribution of power in the digital era.

3] **The most significant implications of blockchain will arise from its interactions with other emerging technologies.** For many of the most revolutionary impacts that commentators often predict for blockchain, blockchain will only be one of many contributing inputs. For example, when commentators get excited by the possibility of blockchain-enhanced EHRs enabling massive medical breakthroughs through vastly improved access to anonymized patient medical data,[167] the key development

[167] Swan, M. 2015. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly. Page 62.

that will enable this probably lies with the machine learning algorithms that will make the discoveries just as much as with the blockchain technology which will organize the information and facilitate access to it. This pattern will likely be the same across many of the possibilities described as being offered by blockchain. Thus, any effective government response will need to be holistic.

Naturally, there are many other issues related to blockchain that will grow in importance in the future but which are not covered by this report. We hope that this report's analysis of the fundamental concepts and questions raised by this new technology will leave readers better prepared to ask the right questions and to separate what is real from what is hype.

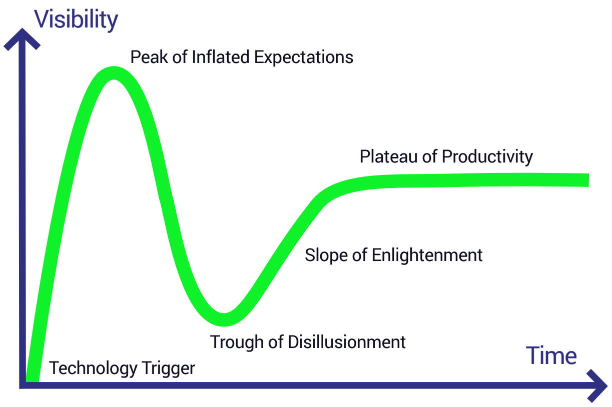
Blinded by the hype?

The question of hype is an important one to consider as we close this paper. When we began our research project in early 2017, many had already begun to see blockchain as something of yesterday's news. At that time, AI and machine learning were the new hot topics that everyone was talking about. Blockchain was seen as increasingly *passé* and "so 2015." But then, in the final third of 2017, the price of a variety of cryptocurrencies started to explode and it seemed like everyone was talking about blockchain again. Over the time that this paper was researched and written, the price of a single bitcoin has gone from about $1,200 to over $25,000 and is now back to about $10,500 (CAD). The fluctuation in the price of ether was even more significant with it starting 2017 at about $12.00 rising to more than $1,800 in the crypto-mania of December 2017-January 2018. It has since fallen back to about $600.[168] Other less well-known tokens have had even wilder rides and overall, the fall back to less inflated prices from the heights of speculation reached in early January 2018 wiped out an astounding $500 billion (USD) in value worldwide in about one month.[169]

It is very important for policymakers not to get distracted by this speculative rollercoaster. Blockchain and DLT offer many benefits, as well as some real dangers, that are completely unconnected to the rise and fall of the price of a bitcoin. At a deeper level, new technologies are often buffeted by inflated expectations based on imperfect understandings, speculation and the simple inability to predict the future that even the most visionary innovators cannot avoid. This pattern has even been recognized and formalized as the "Hype Cycle" illustrated in Figure 17.

FIGURE 17

The Gartner hype cycle



Source: Kemp, J. 27 December, 2007. File: Gartner Hype Cycle.svg. *Wikimedia Commons*. CC BY-SA 3.0. https://commons.wikimedia.org/w/index.php?curid=10547051.

[168] All values as of 25 July, 2018. See https://ca.investing.com/crypto/currencies.

[169] Nishizawa, K. 6 February, 2018. "Get Ready for Most Cryptocurrencies to Hit Zero, Goldman Says." *Bloomberg*. https://www.bloomberg.com/news/articles/2018-02-07/get-ready-for-most-cryptocurrencies-to-hit-zero-goldman-says.

Given that blockchain seems to have gyrated up to multiple "Peaks of Inflated Expectations" – largely on the back of cryptocurrency- and ICO-related financial speculation which has muddied public understanding of the underlying technology – it is hard to say where on this graph we currently find ourselves. The most likely point, however, is somewhere between the "Peak of Inflated Expectations" and the "Trough of Disillusionment."[170] This means that the next few years will likely be when we move onto the "Slope of Enlightenment" and start to find out how useful and impactful blockchain will actually be.

As this report has indicated, there are two main categories of blockchain-related questions that policymakers face. The first concerns the impacts that this technology will have on the wider economy and society. The second concerns the potential uses that this new technology might serve for government in its own operations. To help policymakers answer both categories of questions, we have outlined a series of steps that governments ought to take, including building internal capacity, fostering an attractive environment for innovation, supporting experimentation with the technology, helping to fashion standards and flexible new tools to govern it, and working with other governments to develop the capacity to minimize its threats to their citizens and maximize its benefits.

In closing, we emphasize again just how essential it is to think of both the benefits and the challenges associated with blockchain as being inextricably linked with other emerging technological developments such as AI, big data and IoT. Because of this, it is essential that policymakers be able to think of how they are going to respond to these technologies in these terms. The usual siloed government thinking, whereby one department or regulator assumes responsibility for one thing while another focuses on another without communicating very well with each other, will end badly. Fortuitously, however, blockchain itself – and the transparency and cooperation it can enable – might just help governments find a way to overcome this all-too-persistent bad habit.

[170] Gartner, the firm that developed the hype cycle concept, agrees with our assessment in terms of blockchain's current positioning in the cycle. Panetta, K. 15 August, 2017. "Top Trends in the Gartner Hype Cycle for Emerging Technologies." *Gartner.* https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/.