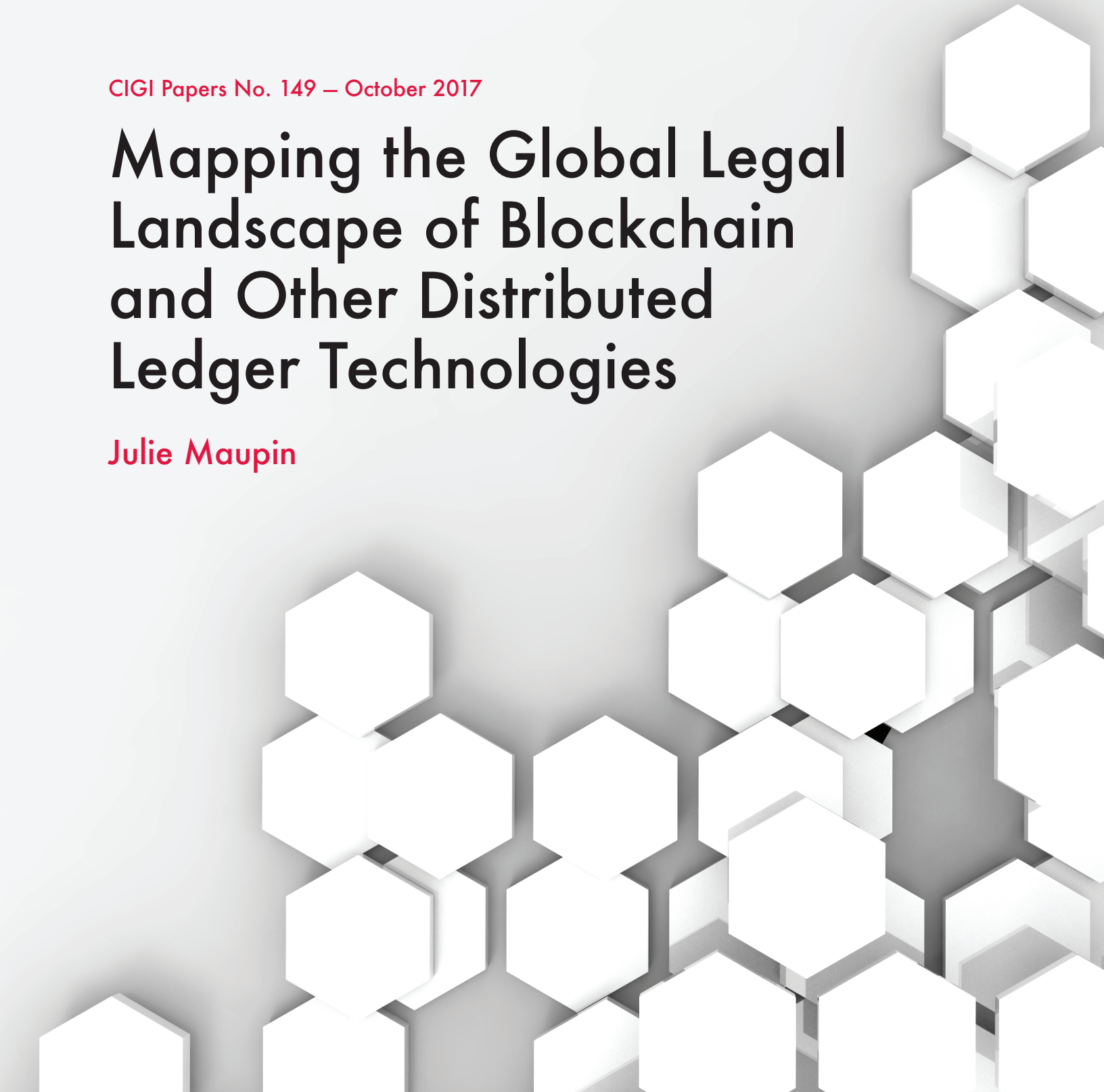
Centre for International
Governance Innovation

CIGI Papers No. 149 — October 2017

Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies

Julie Maupin



Centre for International
Governance Innovation

CIGI Papers No. 149 — October 2017

Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies

Julie Maupin

CIGI Masthead

Executive

President Rohinton P. Medhora

Director of Finance Shelley Boettger

Director of the International Law Research Program Oonagh Fitzgerald

Director of the Global Security & Politics Program Fen Osler Hampson

Director of Human Resources Susan Hirst

Interim Director of the Global Economy Program Paul Jenkins

Chief Operating Officer and General Counsel Aaron Shull

Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett

Senior Publications Editor Jennifer Goyder

Publications Editor Susan Bubak

Publications Editor Patricia Holmes

Publications Editor Nicole Langlois

Publications Editor Lynn Schellenberg

Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

Printed in Canada on paper containing 10% post-consumer fibre and certified by the Forest Stewardship Council® and the Sustainable Forestry Initiative.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Julie Maupin is a senior fellow with CIGI's International Law Research Program (ILRP). She is also a senior research fellow at the Max-Planck Institute for Comparative Public Law and International Law in Heidelberg, Germany.

At CIGI, Julie is contributing to the ILRP's research theme on international economic law. Her research explores the international law dimensions of the use of blockchain (the underlying technology of Bitcoin) in global economic systems. She is also assessing potential regulatory frameworks.

Previously a lecturer at Duke Law School, Julie has taught international investment law, international commercial arbitration, comparative competition law and many other areas of international law at leading law faculties in North America, Europe and Africa. In addition to her scholarly work, Julie regularly advises international organizations, governments, businesses and non-governmental organizations on matters of economic law and policy, with a special emphasis on developing markets.

Julie holds a Ph.D. in international studies, with magna and summa cum laude honours, from the Graduate Institute for International and Development Studies in Geneva; a J.D. and an M.A. in economics from Yale University; and a B.Sc. in economics from the University of Washington. She is an admitted member of the Oregon State Bar.

About the International Law Research Program

The International Law Research Program (ILRP) at CIGI is an integrated multidisciplinary research program that provides leading academics, government and private sector legal experts, as well as students from Canada and abroad, with the opportunity to contribute to advancements in international law.

The ILRP strives to be the world's leading international law research program, with recognized impact on how international law is brought to bear on significant global issues. The program's mission is to connect knowledge, policy and practice to build the international law framework — the globalized rule of law — to support international governance of the future. Its founding belief is that better international governance, including a strengthened international law framework, can improve the lives of people everywhere, increase prosperity, ensure global sustainability, address inequality, safeguard human rights and promote a more secure world.

The ILRP focuses on the areas of international law that are most important to global innovation, prosperity and sustainability: international economic law, international intellectual property law and international environmental law. In its research, the ILRP is attentive to the emerging interactions among international and transnational law, Indigenous law and constitutional law.

Executive Summary

Blockchain, tangle and other distributed ledger technologies (DLTs) are pushing a broad array of previously centralized global economic activities toward decentralized market structures. Governments should tackle the new regulatory conundrums of an increasingly disintermediated global economy by focusing on DLTs' individual use cases rather than its underlying enabling technologies. Grouping the known use cases by common characteristics reveals three broad categories of blockchain-law interfaces. For ease of reference, this paper labels these the recycle box, the dark box and the sandbox. Each raises distinct legal, regulatory and policy challenges deserving of separate analysis.

"Recycle box" use cases adopt blockchain/DLT solutions to accomplish indisputably permissible objectives in "better, faster, cheaper" ways. They necessitate only minor adaptations to existing national and international regulatory frameworks. In this sense, the existing legal frameworks can be "recycled" for many blockchain use cases, although these may still raise difficult policy questions — for example, labour market disruptions — due to structural transitions.

"Dark box" use cases employ blockchains or other DLTs to accomplish per se illegal objectives. They call on regulators to develop more effective global cooperation regimes for detecting, tracking and prosecuting blockchain-based illicit activities. This requires the development of clear policies on cross-border data collection, analysis and sharing that are robust enough to create and sustain public trust.

Finally, "sandbox" use cases utilize blockchains or DLTs to pursue permissible objectives but in ways that entail regulatory risks that — for reasons having to do with the technical properties of blockchains — cannot be addressed within existing regulatory regimes without destroying their core value proposition. Realizing the social benefit of these use cases requires national and international regulators to work with blockchain and DLT entrepreneurs to create innovative ways of satisfying important regulatory prerogatives across multiple industries on a global scale. While piecemeal cross-border regulatory cooperation is always possible and is already occurring to a limited extent, a more efficient way forward would be to set up a global regulatory sandbox for DLTs that is transnational, cross-sectoral, start-up friendly and use-case adaptable.

Introduction: Why Do Blockchains and DLTs Matter?

Blockchain and other DLTs are quietly revolutionizing the way people connect and transact. The world's first blockchain — Bitcoin — was launched in January 2009. With Bitcoin, individuals became empowered to send and receive money on a peer-to-peer basis, within minutes, across borders and for virtually no fees — all without ever touching a bank account.[1] This was quite an achievement.[2] It opened up the amazing possibility of connecting the world's two billion unbanked people to the global economy for the first time in history. But money transmission was just the tip of the iceberg. In the years since Bitcoin launched, developers have realized that while Bitcoin itself has inherent limitations,[3] the technological innovation behind it, the blockchain, enables a great deal more than the creation of borderless "digital gold."[4] Next-generation distributed ledger innovations, such as the tangle, now promise to extend the

1 For a technical description, see Satoshi Nakamoto (pseudonym), "Bitcoin: A Peer-to-Peer Electronic Cash System" (October 2008), online: <https://bitcoin.org/bitcoin.pdf>. For non-technical readers, the Bitcoin Wiki page provides an accessible introduction: "Bitcoin", online: <https://en.wikipedia.org/wiki/Bitcoin>.

2 As attested by the fact that one Bitcoin is worth more than US$770 as of this writing. For updated figures on major cryptocurrency prices and market caps, see "CryptoCurrency Market Capitalizations", online: <https://coinmarketcap.com/all/views/all/>.

3 Most significantly, technical challenges to its scalability; see Kyle Croman et al, "On Scaling Decentralized Blockchains" (Position paper delivered at the Financial Cryptography & Data Security 20th International Conference, Barbados, 22–26 February 2016), online: <fc16.ifca.ai/bitcoin/papers/CDE+16.pdf>. At the time of writing, the Bitcoin community was about to enter a major contestation period over competing scaling solutions. See "Bitcoin Scaling Watch: News and Guides to Navigate the Coming Clash of Code" *CoinDesk* (13 July 2017), online: <www.coindesk.com/bitcoin-scaling-watch-news-guides-navigate-coming-clash-code/>.

4 Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (New York: Harper Collins, 2015).

ongoing decentralization revolution beyond peer-to-peer computer networks to potentially every Internet of Things connected device.[5]

Before considering the legal implications of these fast-evolving new technologies, it is useful to begin with an overview of what they are and how they can be used. A preliminary caveat on terminology is necessary. This paper uses the terms "blockchain" and "DLTs" interchangeably. This is solely to facilitate ease of reading, in concession to the fact that "blockchain" is now the popular term outside of technical circles.[6] From a technical standpoint, however, blockchains are only one subset of DLTs. The latter term encompasses additional technologies — including networked databases, directed acyclic graph tangles and more — whose technical properties differ in important ways from blockchains "properly so-called." These design differences matter a great deal in the real world, as they render different DLTs more or less scalable, more or less secure, and more or less useful for specific purposes. Nevertheless, since the goal of this paper is to map out the international legal landscape of DLTs, the present anlysis lumps them together as a class and focuses on their potential use cases rather than on the technical differences between their underlying protocols. The appendix at the end of the paper provides a basic overview of some of the key differences between popular DLT designs. Readers in search of greater precision are encouraged to consult the technical references cited therein.

Briefly, blockchains are shared digital ledgers that employ cryptographic algorithms to verify the creation and/or transfer of digital assets or content over a peer-to-peer network.[7] While digital money (Bitcoin) was the first and is still the most widely known application of DLT, some of the most promising use cases may actually lie in the realm of accounting and accountability. Corporate actors are developing distributed ledgers to track the movement of goods and payments through their supply chains, reducing fraud and waste.[8] Public–private partnerships are deploying blockchains to certify non-conflict diamonds under the Kimberly Process.[9] Governments are looking to blockchains to replace opaque and outdated official registries with transparent and real-time-updated ones for everything from real property[10] to internet domain names[11] to complex financial assets.[12] Charities are investigating blockchains to improve their financial accountability to donors.[13] Many of these experimental projects make use of "private" or "permissioned" blockchains — distributed digital ledgers controlled by a closed set of known actors such as governments or registered companies.

5 Sergui Popov, "The Tangle" (2016) White Paper, online: <https://iota.org/IOTA_Whitepaper.pdf>.

6 The terms "blockchain" and "DLTs" are used interchangeably in this paper solely for purposes of brevity. This does not in any way suggest that the technical differences between, for example, public blockchains, private permissioned ledgers, tangles and other forms of DLTs are either trivial or unimportant. Different types of DLTs have very different design features that make them more or less useful for specific purposes, and these design differences matter greatly in the real world. However, since the goal of this paper is to map out the international legal landscape for DLTs, the author lumps them together and focuses on their potential use cases rather than on the technical differences between the underlying DLTs themselves. Readers in search of greater technical precision are encouraged to consult the technical references cited herein.

7 For a more detailed non-technical description, see e.g. "Bitcoin", *supra* note 1; Gian Volpicelli, "Beyond Bitcoin. Your Life is Destined for the Blockchain", *Wired* (7 June 2016), online: <www.wired.co.uk/article/future-of-the-blockchain>; "Blockchains: The Great Chain of Being Sure About Things", *The Economist* (31 October 2015), online: <www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable>.

8 Stan Higgens, "IBM Tests Blockchain for Supply Chain With India's Mahindra Group", *CoinDesk* (30 November 2016), online: <www.coindesk.com/ibm-blockchain-mahindra-supply-chain/>; Luke Parker, "Cubichain Tackles 3D Printing Counterfeiting Issues with Blockchain Technology", *Brave New Coin* (10 December 2016), online: <bravenewcoin.com/news/cubichain-tackles-3d-printing-counterfeiting-issues-with-blockchain-technology/>.

9 Luke Parker, "Kimberley Process Pilots a Blockchain for Tracking the World's Diamonds", *Brave New Coin* (28 August 2016), online: <bravenewcoin.com/news/kimberly-process-pilots-a-blockchain-for-tracking-the-worlds-diamonds/>.

10 Laura Shin, "Republic of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury", *Forbes* (21 April 2016), online: <www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#2421bdfe6550>.

11 Mike Ward, "Change Is Coming: How the Blockchain Will Transform the Domain Name Business", *CoinTelegraph* (23 April 2015), online: <https://cointelegraph.com/news/change-is-coming-how-the-blockchain-will-transform-the-domain-name-business>.

12 Depository Trust and Clearing Corporation (DTCC), "Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape" (January 2016) White Paper [DTCC White Paper], online: <www.dtcc.com/news/2016/january/25/blockchain>.

13 Luke Parker, "GiveTrack Offers Confidence in Charities", *Brave New Coin* (13 December 2016), online: <bravenewcoin.com/news/givetrack-offers-confidence-in-charites/>.

But a host of start-ups is also busy building visionary "smart contract" applications on top of prominent "public" or "permissionless" (open source and open access) distributed ledgers.[14] These innovations aspire to allow ordinary people all over the world to do useful things, including:

- buy and sell goods, services and assets without going through any broker, marketplace or exchange;[15]
- invest in grassroots crowdfunding schemes that allow investors — not fund managers or oversight boards — to allocate capital to projects and benefit directly from returns;[16]
- execute legal wills that automatically transfer control over assets to designated heirs upon death;[17]
- settle contract disputes digitally without having to go through any country's courts;[18]
- create sustainable circular economies[19] and sharing economies[20] to power the green revolution; or
- securely store, exchange and control access to data, communications and other content, including personal data and data from internet infrastructure.[21]

In short, the list of transformative possibilities is long. DLTs are on track to bring major disruption to long-standing industries and market structures in the near to medium term. In doing so, they will interface with and often challenge the logic behind a broad spectrum of existing legal regimes. They will force law makers, policy makers and regulators at all levels of government — from the subnational to the international — to rethink how best to advance public policy objectives in an increasingly blockchain-powered world.

The Need for Governance Innovation to Support Blockchain Innovation

Unfortunately, not all the news in the blockchain innovation space has been good. Criminals have used Bitcoin and other cryptocurrencies to facilitate payment on illegal online drug bazaars such as Silk Road. Thanks to the inherent transparency of data within the Bitcoin network, Silk Road and its early successors were shut down and their operators

14 For an accessible overview of what smart contracts are and how they can be used, see Alan Morrison, "Blockchain and Smart Contract Automation: How Smart Contracts Automate Digital Business", PwC Technology Forecast Series, online: <www.pwc.com/us/en/technology-forecast/blockchain/digital-business.html>.

15 See e.g. OpenBazaar website, online: <https://openbazaar.org/>.

16 See e.g. Waves website, online: <https://wavesplatform.com/>; AI Coin website, online: <www.ai-coin.org/>.

17 Scott Fargo, "Blockchain Apparatus Launches a New Trusted Will System", *InsideBitcoins* (9 April 2015), online: <insidebitcoins.com/news/blockchain-apparatus-launches-a-new-trusted-will-system/31516>. Blockchain-based legal disruption is also being supported by the open-source project Legalese, see online: <https://legalese.com/>.

18 For examples of proposals that have been considered or are currently under development, see e.g. Andreas Antonopoulos & Pamela Morgan, "Decentralised Arbitration and Mediation Network", Research and Project Proposal, submitted to The DAO, online: https://github.com/thirdkey-solutions/damn/blob/master/proposal.asciidoc>; Isabella Kaminska, "Decentralised Courts and Blockchains", *Financial Times* (29 April 2016), online: <https://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/>; more recently, Wulf Kaal & Craig Calcuterra, "Smart Contract Dispute Resolution—The Need for an Open Source Blockchain Platform Ecosystem", *Medium.com* (26 June 2017), online: <https://medium.com/@wulfkaal/smart-contract-dispute-resolution-the-need-for-an-open-source-blockchain-platform-ecosystem-e6318610fdef>; and Washington Sanchez, "Dispute Resolution in OpenBazaar", online: <https://gist.github.com/drwasho/405d51bd1b1a32e38145>.

19 See e.g. the Brooklyn Microgrid project, online: <brooklynmicrogrid.com/>.

20 See e.g. ZF, Press Release, "ZF, UBS and innogy Innovation Hub Announce the Jointly Developed Blockchain Car eWallet" (1 May 2017), online: <www.zf.com/corporate/en_de/press/list/release/release_29152.html>.

21 See e.g. the following blockchain-based content management firms: Decent, online: <https://decent.ch/>; LBRY, online: <https://lbry.io/>; Namecoin, online: <https://namecoin.org/>; Bitmessage, online: <https://bitmessage.org/>. See also the ambitious next-generation distributed internet initiative Inter-Planetary File System [IPFS], online: <https://ipfs.io/>.

prosecuted by authorities.[22] But next-generation drug bazaars quickly appeared using blockchain technologies to decentralize the exchanges themselves, not just the payments, rendering it much more difficult for legal authorities to intervene.[23] Meanwhile, rapid cryptographic innovations on the payments side are also keeping regulators on their toes. Revenue authorities worry that newer-generation blockchains with much stronger privacy properties, for example Zcash,[24] could be used for widespread tax evasion — leaving governments with inadequate revenue streams with which to build schools and roads.[25] Even well-intentioned blockchain projects can sometimes subject consumers to inordinate and poorly understood financial risks. This was well demonstrated by the spectacular failure of The DAO,[26] a blockchain-based venture capital fund that raised — then partly lost to a hacking incident — more than US$150 million over a few weeks in May and June 2016.[27]

These unwelcome scenarios arise because the very feature that makes blockchains so useful — their ability to enable ordinary people to transact with one another in a peer-to-peer fashion without the need for a trusted central party — also makes them vulnerable to exploitation for illicit purposes. Historically, governments have cooperated to avoid such unwanted outcomes by regulating the intermediaries or "choke points"[28] within our global economy. For example, governments rely on banks to combat money laundering by subjecting them to Know Your Customer rules[29] and suspicious activity reporting requirements.[30] They fight securities fraud by forcing companies to file elaborate disclosures with securities commissioners as a condition of being listed on exchanges.[31] In the brave new blockchain world, however, many existing intermediaries — banks, exchanges, etc. — stand to be fully or partially disintermediated.

How, then, should regulatory imperatives be carried out once the choke points are removed? This is the central governance dilemma presented by blockchain technologies, and it is not an easy problem to solve. It takes years to develop effective regulatory schemes that adequately protect public values and advance important public policy goals, and because of this regulators are risk-averse toward new technologies by default. Meanwhile, Blockchain technologies continue to splinter off in unpredictable directions at a stupefying pace. This makes adopting a purely

22 See Joshua Bearman & Tomer Hanuka, "The Rise and Fall of Silk Road", *Wired* (January 2015), online: <www.wired.com/2015/04/silk-road-1/>. Silk Road 2.0 was also successfully seized by authorities (see US Attorney's Office (Southern District of New York), Press Release, "Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court" (6 November 2014), FBI Takedown Notice, online: <www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court>).

23 But Silk Road 3 and other successors went live even before the takedown notice for Silk Road 2.0 was published. See Kate Knibbs, "Silk Road 3 is already Up, But It's Not the Future of DarkNet Drugs", *Gizmodo* (14 November 2014), online: <gizmodo.com/silk-road-3-is-already-up-but-its-not-the-future-of-da-1655512490>.

24 Zcash is a cryptocurrency using cutting-edge cryptography to make peer-to-peer money transactions secure without being publicly viewable. Technical specifications may be found on the Zcash website, online: <https://z.cash/about.html?page=0>.

25 For an academic discussion of this problem in relation to Bitcoin, see Omri Marian, "Are Cryptocurrencies Super Tax Havens?" (2013) 112 Mich L Rev First Impressions 38. Of course, the problem becomes much more difficult with the increasing adoption of more privacy-centric cryptocurrencies.

26 DAO stands for distributed autonomous organization. It is basically a collection of smart contracts designed to interact with one another in prescribed ways, given certain conditions. In principal, many different types of DAOs are conceivable. "The DAO" under discussion here (a rather unfortunate name choice, given the applicability of the abbreviation to many possible organizations) is merely one instantiation of the broader idea. For one tech observer's overview of this particular DAO's ("The DAO's") evolution and hack, see *supra* note 21. The DAO's wiki entry is also informative: "The DAO (organization)", online: <https://en.wikipedia.org/wiki/The_DAO_(organization)>. For a more technical explanation of The DAO as a concept, see Christoph Jentzsch, "Decentralized Autonomous Organization to Automate Governance" (2016) White Paper, online: <https://download.slock.it/public/DAO/WhitePaper.pdf>.

27 This incident is discussed in greater depth in the below section of this paper entitled "The Sandbox." For background on The DAO and its hack, see David Siegel, "Understanding The DAO Hack for Journalists", *Medium* (19 June 2016), online: <https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993#.5dc9cchhx>.

28 Natasha Tusukov, *Chokepoints: Global Private Regulation on the Internet* (Oakland: University of California Press, 2016).

29 See e.g. "Customer Due Diligence Requirements for Financial Institutions: A Rule by the Financial Crimes Enforcement Network (FinCEN)", US Department of the Treasury (11 May 2015), online: <www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions>.

30 These regimes are highly onerous, as evidenced by FinCEN's self-analysis of the US government's suspicious activity reporting regime: FinCEN, "Index to Topics for The SAR Activity Review Volumes 1-23", online: <www.fincen.gov/index-topics-sar-activity-review-volumes-1-23>.

31 See e.g. London Stock Exchange Admission and Disclosure Standards (effective 3 July 2016), online: <www.londonstockexchange.com/companies-and-advisors/main-market/rules/regulations.htm>.

"wait and see" regulatory stance less viable (and arguably more risky) as time passes.

Yet it would be counterproductive to stifle the tremendous social gains these technologies promise to deliver by taking an ill-considered or heavy-handed approach to regulating them. Forbidding their use, for example, would cause more harm than good and would likely prove ineffective. Short of shutting down the internet, there's no way to stop DLT from proliferating. Attempts by governments to intervene at the protocol level are likewise inadvisable, as this could interfere with active private sector experimentation, which is generating rapid security and functionality improvements in the source code of many blockchains and other DLTs.

Instead, governments should tackle the new regulatory challenges of a disintermediated global economy by focusing on individual DLT use cases rather than their underlying enabling technologies. Such an approach aligns well with one of the core values of internet design: the end-to-end principle. As articulated in the seminal 1981 paper of Salzer, Reed and Clark, the principle states that the payoff from placing features (in the present case, regulatory intervention) "at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level."[32] For this reason, most discussions about global internet governance have also centred on higher-layer use cases and their prominent actors, leaving technical decisions on underlying protocol specification to specialized standards-making bodies.[33] While a discussion of the evolution of global internet governance is beyond the scope of this paper, a similar approach could work well for DLT, both those that build on top of existing internet protocols and those that aim to replace them.[34]

Another, more practical, reason to focus on use cases rather than underlying technologies is that this approach helps break down the regulatory task into discrete and manageable subtasks whose contours can be better identified. Stepping back to survey the use cases that have emerged in the DLT world to date reveals that they largely can be sorted into three broad boxes, each of which should be treated differently from a legal and policy perspective: the recycle box, the dark box and the sandbox. The path forward lies in understanding the basic characteristics of these three use cases and developing sensible regulatory approaches for each.

The Recycle Box

The term recycle box evokes the image of the everyday recycling bin. Blockchain use cases falling into the recycle box category are essentially variations on themes governments have seen before. As such, they are use cases to which existing regulatory regimes can be applied with only minor adaptation.

A prime example is the launch of blockchain-based interbank settlement systems such as the Ripple network.[35] Ripple uses blockchain technology to put large global financial institutions onto a single distributed ledger with which they can settle their global interbank trades (cash transfers, asset swaps, etc.) in real time. This promises to save the institutions, and hopefully their customers, considerable time and money as compared to the multi-day batching and settlement processes being carried out through the global correspondent banking system.[36]

In other words, Ripple's blockchain technology gives banks a "better, faster, cheaper" way to do something they already do. Banks are known entities and highly regulated ones. One can almost take for granted that even after replacing their legacy settlement systems with blockchain technologies, banks must still

32 JH Saltzer, DP Reed & DD Clark, "End-to-End Arguments in System Design" (1981) 2:4 ACM Transactions on Computer Systems 277.

33 For a more thorough analysis, see Global Commission on Internet Governance, "One Internet" GIGI, Final Report, 21 June 2016, online: <www.ourinternet.org/report>.

34 For an interesting example of the latter, see the IPFS project, *supra* note 21.

35 Ripple is a company focused on building solutions for "instant, low-cost international payments," as described on the company's website, online: <https://ripple.com/>.

36 Ripple estimates the efficiency gains to be on the order of 60 percent, but this depends upon a number of assumptions, such as network effects and the price stability of Ripple's native digital asset, XRP. See "The Cost-Cutting Case for Banks, the ROI of Using Ripple and XRP for Global Interbank Settlements" (February 2016) Ripple Promotional Paper, at 11, online: <https://ripple.com/files/xrp_cost_model_paper.pdf>.

satisfy all relevant legal requirements.[37] These factors are typical of blockchain use cases that are unlikely to pose massive challenges to existing regulatory regimes. Indeed, a simple way to identify potential recycle box blockchain innovations is to ask the following questions:

- → Is this blockchain use case essentially replacing a back-office function?
- → Is this blockchain solution being deployed by one or more regulated actors within their traditionally regulated line(s) of business?

If the answer to either question is yes, it's highly likely that governments and intergovernmental regulatory bodies can accommodate the new blockchain use case within their existing regulatory regimes.

Of course, this does not mean that no regulatory modifications will be necessary for recycle box use cases. In the case of Ripple and interbank settlements, for example, regulators must put careful thought into how to ensure that participating banks cannot use the shared ledger to collude in illegal ways, as was the case with the Libor scandal. But this is more of a technical challenge than a legal one. Provided the blockchain solution is properly designed, tested, and regularly and transparently audited for its performance, there is no reason to expect it will not pass regulatory muster.

That said, at least some recycle box use cases will likely entail socio-economic consequences that could prove politically sensitive even if not legally difficult. The displacement of back-office workers in functions like accounting and auditing, financial services, supply chain management or notarial services does not sit well with the heightening pressure on many governments to adopt policies that help to create and/or maintain high-paying jobs.

While it is difficult to predict how many jobs might be eliminated by the widespread adoption of distributed ledger solutions in the coming decades,[38] there is reason to believe the potential scale of job losses could be non-negligible.[39] A recent report by the World Economic Forum estimates that 5.1 million jobs will be lost overall to so-called fourth industrial revolution technologies between 2015 and 2020.[40]

On the other hand, blockchain technologies will also create new jobs for certain highly skilled workers, including developers, IT consultants, cyber security specialists, etc. Only time will tell to what extent *net* job losses may materialize because of blockchain innovation. Policy makers should look for guidance to the broader relationship between technological innovation and employment as evidenced in their countries over the past 20 to 30 years. This information can help shape possible policy responses, such as displaced-worker assistance and skills retraining programs, in anticipation of possible blockchain-based employment disruptions. Meanwhile, increased investment in STEM (science, technology, engineering and mathematics) education and training — in particular in the fields of programming, cryptography, big data analysis, quantum computing and cyber security — should be prioritized.

37 As evidenced by the fact that FinCEN assessed a US$700,000 civil penalty against Ripple in 2015 for "willfully violat[ing] several requirements of the Bank Secrecy Act (BSA) by acting as a money services business (MSB) and selling its virtual currency, known as XRP, without registering with FinCEN, and by failing to implement and maintain an adequate anti-money laundering (AML) program designed to protect its products from use by money launderers or terrorist financiers." See FinCEN, Press Release, "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger" (5 May 2015), online: <www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>.

38 For many industries and countries, there are no reliable estimates of how many workers are employed in such functions to begin with, much less what percentage might be made redundant by specific blockchain deployments.

39 For example, in 2014 a controversial independent study of the US Department of Defense found that the Pentagon was employing over 1,014,000 back-office personnel (most of them civilians and contractors) in support of only 1,300,000 troops on active duty. Of these, nearly half a million were employed in supply chain management and logistics – a major disruption target for blockchain start-ups and corporate innovation labs. Craig Whitlock and Bob Woodward, "Pentagon Buries Evidence of $125 billion in Bureaucratic Waste", *Washington Post* (5 December 2016), online: <www.washingtonpost.com/investigations/pentagon-buries-evidence-of-125-billion-in-bureaucratic-waste/2016/12/05/e0668c76-9af6-11e6-a0ed-ab0774c1eaa5_story.html?pushid=breaking-news_1480983605&tid=notifi_push_breaking-news&utm_term=.77ae33c30e64>.

40 World Economic Forum, *The Future of Jobs Report* (January 2016), online: http://reports.weforum.org/future-of-jobs-2016/. The report does not single out blockchains, but its Executive Summary describes the fourth industrial revolution as follows: "We are today at the beginning of a Fourth Industrial Revolution. Developments in previously disjointed fields such as artificial intelligence and machine learning, robotics, nanotechnology, 3D printing and genetics and biotechnology are all building on and amplifying one another. Smart systems—homes, factories, farms, grids or entire cities—will help tackle problems ranging from supply chain management to climate change."

One possible criticism of the recycle box category is that the concept might favour incumbents or large existing actors over start-ups or newer entrants to a given industry. This criticism is not compelling, because it is true of all existing laws and regulations. Incumbents are by definition privileged by existing regulatory regimes whose strictures they have already satisfied as a precondition to becoming incumbents. But provided the existing regulatory regime is flexible enough to also allow start-ups to satisfy regulators' prerogatives in some not-too-burdensome manner — a challenge taken up in the sandbox discussion below — this is not an insurmountable hurdle to effective competition. When incumbents' business models come under threat from savvy DLT start-ups (or savvier co-incumbent competitors), incumbents themselves become forced to attempt to "innovate or die," as the Ripple case illustrates.[41]

The Dark Box

The second major category into which blockchain use cases may fall is also easy to grasp at first glance. The dark box draws its name from the "dark net." It encapsulates all use cases whose fundamental objective is per se illegal from the outset under existing local, national or international law. The simplicity of this classification exercise again confirms that focusing on use cases rather than technologies is a helpful way to approach DLTs. Sorting a blockchain use case into the dark box is as simple as answering one of the following questions in the affirmative:

- Is the basic objective the innovator is trying to achieve here universally illegal (for example, terrorism), irrespective of which technologies might be used?
- Does the balance of indicators suggest that the innovator is only utilizing a DLT to get around the fact that the basic objective is illegal in at least one jurisdiction where the innovator operates or hopes to operate (for example, gambling)?

Examples of dark box use cases would include blockchains that are deployed to enable: online drug bazaars, weapons bazaars or other marketplaces for illegal items; human trafficking networks; terrorist financing and communications networks; tax evasion schemes; and so on. These illegal services and many others have existed on the dark web for years, and some of them have recently found new life on blockchains. Yet as Ross Ulbricht (founder of the first Silk Road drug bazaar) discovered, they become no less illegal simply by putting them on a blockchain.[42]

Dark box use cases do sometimes pose special challenges — not to law makers and rule makers, but to regulatory enforcement officials. They are easy to identify, but difficult to stop. To see why, consider the possibility of an online drug bazaar that relies on one of the new privacy-focused cryptocurrencies such as Zcash or Monero[43] as its method of payment. Payments made in these cryptocurrencies are much more difficult to trace than Bitcoin payments, because unlike with Bitcoin, their blockchains do not keep publicly viewable (i.e., unencrypted) records of basic information like digital wallet addresses and transaction amounts.

This means a consumer wishing to purchase illegal narcotics could proceed by obtaining a cryptocurrency (for example, Bitcoin) in exchange for a fiat currency (for example, dollars) on a regulated fiat-crypto exchange.[44] After sending the Bitcoin from the user's exchange account to his or her Bitcoin digital wallet, the user could then utilize an unregulated crypto-to-crypto currency "mixer" service to convert the Bitcoin into a portfolio of various other less trackable cryptocurrencies,[45] then distribute them among several other digital wallets. Finally, after logging

41 It is an open question whether an incumbent trying to stamp out competition from a DLT start-up by adopting a back-office DLT solution itself will ultimately succeed. If there is a true business case for disintermediation — i.e., if the intermediary does not add much real value to the business ecosystem in which it operates once decentralized alternatives become available to that ecosystem — then it is doubtful whether retaining regulatory approvals under a recycle box scheme will in any event save the incumbent from being disrupted in the end.

42 Laurie Segall, "Silk Road's Ross Ulbricht sentenced to life", *CNN* (29 May 2015), online: <money.cnn.com/2015/05/29/technology/silk-road-ross-ulbricht-prison-sentence/>.

43 Like Zcash (see *supra* note 24), Monero is a next-generation cryptocurrency, which functions similarly to Bitcoin, but employs more sophisticated cryptography to offer a higher degree of anonymity to its users. Zcash achieves its privacy properties through the use of zero-knowledge proofs, while Monero relies on the slightly less anonymous but more thoroughly battle-tested method of ring signatures.

44 There are many such exchanges, Coinbase, Kraken and Poloniex being among the largest at present.

45 Shapeshift's website describes its service as "The Safest, Fastest Asset Exchange on Earth. Trade any leading blockchain asset for any other. Protection by Design. No Account Needed", see online: <https://shapeshift.io/#/coins>.

onto the Tor network[46] to hide IP addresses and other identifying information like search histories, the user could purchase the illegal narcotics using one of the anonymous cryptocurrencies on a decentralized, blockchain-powered drug bazaar.

Note that in this chain of events the user might make use of multiple blockchains — all of which are perfectly legal except for the drug bazaar itself — while passing through only a single regulatory choke point (the fiat-to-crypto exchange) at the very beginning of the process. But the combined effect of the user's multiple blockchain interfaces, when conducted serially or in tandem, makes it exceedingly difficult for a government to ever discover, much less prosecute, the user's ultimate illegal activities.[47] Similarly, on the service provider side it is not clear how easily a government might "take down" a decentralized drug bazaar operating across thousands of independent nodes in potentially dozens of different countries.[48]

Dark box activities thus call for close cross-jurisdictional regulatory cooperation among the authorities responsible for collecting and analyzing the data points used to ferret out illicit digital activities. Such cooperation is already taking place through fora such as the Financial Action Task Force (FATF).[49] But as blockchain-embedded privacy features continue to become more advanced, and as they continue to gain in popularity, governments will be challenged to continuously develop better detection methods if they are to remain effective.

Ultimately, however, governments may well win some dark box battles but lose the war if they continue along the present course without deeper reflection. Dark innovators have always been among us, and even the savviest governments have almost always been one step behind them. But today the situation is changing. Blockchains are making it easier for increasingly more individuals to "go dark" at precisely the same moment when the trustworthiness of many governments' digital privacy commitments is being questioned. There is a growing concern among citizens that governments themselves — through their secret data collection and analysis programs — may pose a bigger threat to society than dark actors. It is a question of public trust. If governments wish to gain and maintain the public's support for developing new regulatory methods to track and prosecute dark actors using blockchains, they must show a much greater willingness to be held accountable for their own data collection and analysis policies.

The dark box category highlights the importance of two key types of policy innovation that must be pursued simultaneously:

- the further strengthening of international regulatory cooperation mechanisms to combat social ills such as drug trafficking, money laundering, etc.; and
- the need to put far more resources into public consultations to develop a broad citizen consensus around — and suitable accountability mechanisms to protect — the social good of digital privacy.

The Sandbox

The third and final box into which most blockchain use cases can be sorted is the sandbox. This is the most exciting of the three, because it is where the most truly disruptive and hence socially

46 Originally developed by the US Naval Research Laboratory to protect US intelligence communications online, Tor later morphed into a group of volunteer-operated servers. The Tor project today describes itself as "free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security" (see the Tor website, online: <www.torproject.org/>).

47 For an interesting consideration of dark box use cases involving smart contracts and some possible technical strategies for addressing them, see Ari Juels, Ahmed Kosba & Elaine Shi, "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts" (Paper delivered at the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, 24–28 October), Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security at 283–95.

48 Wright and De Filippi point out that there are indeed "draconian" measures that states could take to control such unwanted activities within their own jurisdictions without having to engage in transnational regulatory cooperation efforts, such as "filtering internet service providers, blacklisting malicious decentralized autonomous organizations and criminalizing software developers, introducing back doors on everyone's computer to monitor citizen behavior, or adopting more extreme coercive measures." However, they are quick to add that such measures would be antithetical to the fundamental principles of an open internet and would destroy the many promises of permissionless innovation, and they conclude that "[n]ew regulatory approaches therefore need to be taken." Aaron Wright & Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of the Lex Cryptographia" (10 March 2015), available at SSRN: online: <https://ssrn.com/abstract=2580664>.

49 The FATF is an intergovernmental body established in 1989 to "set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system." See the FATF website, online: <www.fatf-gafi.org/about/>.

beneficial use cases are likely to land. It is also the category raising some of the most difficult legal and policy conundrums. The term sandbox here takes its cue from the Financial Conduct Authority's (FCA's) recent initiative to set up a UK regulatory sandbox: a safe space in which fintech companies targeting UK markets can test out new technologies within a "light touch" regulatory environment under close government supervision and for a defined period.[50] The UK initiative no doubt drew inspiration from similar initiatives by other government officials in other sectors, notably US Federal Communications Commissioner Jessica Rosenworcel's 2014 piece on "Sandbox Thinking."[51]

As applied to the DLT space for purposes of the present analysis, sandbox-type innovations utilize blockchains to pursue worthy goals. The difficulty is that they do so in a way that cannot satisfy existing regulatory requirements because of the technical properties of blockchains. Their end is not to evade the spirit of the law; however, their means is ill-suited to comply with the letter of it. More precisely, blockchain use cases falling within the sandbox category share these basic characteristics:

1. the fundamental objective underlying the use case is:
    a. not illegal on its face, but
    b. does entail real risks that governments are not willing to leave entirely unregulated;
2. the blockchain is being used to accomplish the objective in a way that bypasses traditionally regulated entities;
3. forcing the innovation to comply with the existing regulatory scheme would destroy the business case for deploying the blockchain in the first place (i.e., eliminate the social gains it could bring); and
4. there is conceivably scope for addressing legitimate regulatory concerns through alternate means.

A case in point is the use of blockchain technologies to facilitate novel types of peer-to-peer funding. Here it is instructive to return to the example of The DAO mentioned earlier. The idea behind The DAO was to democratize early-stage investing in the blockchain start-up space. Its creators wanted to make it possible for ordinary individuals — rather than just the usual crowd of wealthy, accredited investors — to get in on the ground floor of exciting new start-ups that might be the next Google, Facebook or Amazon. They did this by launching a set of "smart contracts" (bits of self-executing computer code designed to interact with other bits of self-executing computer code in prescribed ways) on top of the Ethereum blockchain.[52] These smart contracts allowed users to contribute funds in the form of the popular cryptocurrency Ether to a common investment pool. Contributors received "DAO tokens" in exchange for their funds, which gave them the right to vote, in proportion to their token holdings, on which start-up projects the pool should fund. The code also provided instructions for automatically funnelling any returns made on these investments back to the pool's contributors.

At first glance, this sounds a lot like an ordinary venture capital fund. Its objective was to carry out the ordinarily legal activity of investing in early stage start-ups (sandbox characteristic 1.a.). Yet The DAO's method of operation was anything but ordinary, and this placed it structurally at odds with the usual legal regimes regulating venture capital. The DAO had no physical presence, no formal legal existence in any jurisdiction anywhere

50 For details on the FCA sandbox, its admission criteria and its first cohort of accepted start-ups, see FCA, "Regulatory Sandbox", online: <www.fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox>. As pointed out by an anonymous reviewer, the FCA was not the first to establish a "regulatory sandbox." Jessica Rosenworcel of the US Federal Communications Commission developed the idea of government sandbox in a 2014 article, drawing inspiration from the practice of software developers to code "sandboxes" into their programs within which other developers could experiment without altering the entire platform. However, the United Kingdom was the first country to introduce a sandbox of a type that could prove specifically applicable to blockchain and DLT start-ups, and for this reason the FCA sandbox has become the one that is best known among the community of DLT entrepreneurs.

51 Jessica Rosenworcel, "Sandbox Thinking", *DemocracyJournal.org* (Fall 2014) 1–11. Rosenworcel, in turn, drew her inspiration from the practice of software developers to code "sandboxes" into their programs within which other developers could experiment without altering the entire platform.

52 Ethereum is a blockchain ecosystem launched in 2015 that currently operates on a proof of work logic similar to Bitcoin's. Unlike Bitcoin, however, Ethereum is a "Turing complete" system, which means it can be used to power a wide variety of applications beyond simple currency transfers. In other words, it is specifically designed to run smart contracts, whereas Bitcoin is specifically designed to transfer money. The cryptocurrency that is "native" to the Ethereum blockchain is called Ether. It presently has the second-largest cryptocurrency market cap after Bitcoin. For a technical introduction to the Ethereum concept, see Vitalik Buterin, "A Next Generation Smart Contract and Decentralized Application Platform" (2015) Ethereum White Paper, online: <https://github.com/ethereum/wiki/wiki/White-Paper>.

in the world and no designated leadership — neither management, nor employees, nor board of directors. All of its operations were carried out in an autonomous decentralized fashion on the blockchain itself. It was designed to be accountable to no one beyond the fund's anonymous contributors (sandbox characteristic 2). TechCrunch described this as "a paradigm shift in the very idea of economic organization," offering "complete transparency, total shareholder control, unprecedented flexibility, and autonomous governance"[53] (sandbox characteristic 3). However, as The DAO's subsequent history shows — namely, the heist of funds worth US$50 million by a hacker who found a way to exploit a bug in the code[54] — this type of investing does entail serious risks for investors (sandbox characteristic 1.b.). Those risks are the very reason most governments regulate venture capital investing in the first place.

As it happens, The DAO's investors and creators got lucky. The global community of Ethereum developers quickly rallied and found a technical fix — albeit a highly controversial one — that essentially made The DAO's investors whole by wiping out the effects of the hack.[55] (Not all participants in blockchain use cases gone awry have been so fortunate.[56])

It is instructive to consider how this story might have unfolded differently had The DAO's creators first vetted their revolutionary new idea within a global regulatory sandbox before launching it onto the world stage. A team of experienced regulators would no doubt have required The DAO's ambitious young developers to address the many obvious risks they appear to have overlooked in their initial design. For example, merely writing "the code is law" on a project's informational website does not make it so. Nor does disclaiming responsibility for investor losses absolve the involved persons of financial liability when funds go missing.

Of course, any competent lawyer could have pointed out these facts, and The DAO's creators and champions should have been much more careful in obtaining sound legal advice up front. But further, working directly with regulators after doing so could have yielded other important advantages. As public authorities, regulators often exercise broad discretionary powers under their authorizing statutes. This allows them to creatively collaborate with blockchain entrepreneurs to develop blockchain-friendly ways of addressing identifiable regulatory risks. The goal, after all, is not to stifle innovation but to protect important public policy interests.

In the case of The DAO, a team of sandbox regulators might have asked the developers to place a fund-size limit on the experiment so as to limit the overall risk of loss. They might have required the incorporation of an investor "test game," in which potential contributors would be compelled to demonstrate their ability to view, vote on and understand the consequences of DAO-powered investment proposals in a "dry run" environment as a precondition of being allowed to invest in the live fund. Perhaps the regulators would have requested data or forecasts concerning the top originating jurisdictions for DAO contributions so as to pinpoint which countries' investors and markets were most likely to be affected. Numerous other possibilities can be imagined.

The main obstacle to realizing this kind of collaborative regulatory entrepreneurship is that most modern regulators operate within silos of highly specialized expertise and territorially limited competence, whereas many promising blockchain applications are inherently global and multi-sectoral. Indeed, blockchain's major promise is its ability to enable global peer-to-peer markets of all stripes. This may be one reason the UK FCA's

53 Seth Bannon, "The Tao of 'The DAO' or: How the Autonomous Corporation is Already Here", *TechCrunch* (16 May 2016), online: <https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/>.

54 For a technical analysis of the hack, see Phil Daian, "Analysis of the DAO Exploit", *Hacking, Distributed* (18 June 2016), online: <hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>.

55 The details of the fix are highly technical. A more succinct overview is provided in "The DAO, The Hack, The Soft Fork, and The Hard Fork", *Cryptocompare* (11 November 2016), online: <www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>. For one lawyer's legal assessment of The DAO, its hack and the actions taken by the developer community to ameliorate the effects of the hack, see Drew Hinks, "A Legal Analysis of the DAO Exploit and Possible Investor Rights", *Bitcoin Magazine* (21 June 2016), online: <https://bitcoinmagazine.com/articles/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-1466524659>.

56 There are a number of helpful websites that publish information on Bitcoin, Ethereum and other blockchain-based scams. See e.g. Badbitcoin.org, online: <www.badbitcoin.org/thebadlist/>; lwww.bitx.co/blog/bitcoin-scams/; "List of SCAMs and Not Working ETHEREUM FAUCETS", online: <eth.best-loved.com/faucets/scams/scams>. In addition to outright scams, blockchain users and investors have lost significant sums to various types of hacks and/or outright financial mismanagement – most of them involving cryptocurrency exchanges. See e.g. Robert MacMillan, "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster", *Wired* (3 March 2014), online: <www.wired.com/2014/03/bitcoin-exchange/>; "Bitcoin worth $72 Million Was Stolen in Bitfinex Exchange Hack in Hong Kong", *Reuters* (3 August 2016), online: <fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/>.

regulatory sandbox has proven of limited interest to many notable blockchain start-ups, since Brexit in particular.[57] A sandbox geared toward delivering UK regulatory approvals only for fintech innovations affecting UK markets is too small a field of application for most blockchain technologies.[58]

A regulatory sandbox for blockchain, then, would need to exhibit at least four distinctive features to be effective:

- *Global reach:* A blockchain sandbox must have the capacity to tap competent authorities from any national jurisdiction in evaluating and working toward creative regulatory solutions for new use cases. This does not mean that all countries' regulatory authorities need to be involved all the time. The sandbox could instead take a telescoping approach in which blockchain innovators are asked to identify the major markets they believe their innovation will reach first (target markets). An initial sandbox team could be assembled on the basis of these predictions and then adjusted as needed from there.

- *Cross-sectoral flexibility:* A blockchain sandbox must be able to assemble competent authorities from any sector that a blockchain innovation might conceivably touch. Depending on the use case, a sandbox team might comprise authorities across diverse areas, including tax, securities, consumer protection, banking supervision, health and labour. The sandbox team's composition must follow the use case. A corollary to this point is that it would not be advisable to situate a regulatory sandbox for blockchain technologies within an existing international body that exhibits a limited and specific subject-matter expertise, such as the FATF. A better strategy would be to involve authorities from international as well as national bodies in sandbox teams as the circumstances warrant. This reduces the risk that every blockchain use case will be viewed through the lens of a particular group's narrow set of regulatory concerns.

- *Start-up-friendly operating structure:* A blockchain sandbox must be accessible and useful to start-ups with small budgets and staffs. Most blockchain start-ups satisfying the sandbox criteria face a chicken-and-egg problem. They cannot scale without obtaining some modicum of regulatory certainty, but they do not have sufficient bandwidth to engage with labyrinthine regulatory processes across the multiple jurisdictions whose approvals they would need in order to scale safely. To solve this problem, a Global Regulatory Sandbox for Blockchain Technologies could follow the lead of national investment promotion authorities by establishing a single national contact point for global blockchain sandboxing.[59] The national focal points would then act as the internal coordinating authorities responsible for getting the necessary representatives from their respective national regulatory bodies onto the team for each specific global sandboxing exercise. A single global blockchain sandbox supported by an underlying network of national focal points promises to be a much more start-up-friendly model than the rapid proliferation of separate national regulatory sandboxes, which the UK initiative seems to be setting off around the world.[60]

57 The FCA admitted 24 applicants into its first sandbox cohort. Among these, nine are described as blockchain or DLT firms: see FCA, *supra* note 49. However, because the application process for the FCA's first sandbox cohort preceded the Brexit vote, there is an open question as to how many firms applied under the (now tenuous) assumption that they might "passport" UK regulatory approval into other EU markets.

58 Other reasons may have to do with the FCA's intake criteria for its regulatory sandbox, which may be perceived as too restrictive for some blockchain start-ups to satisfy (for example, consider the requirement that the start-up have a "significant UK nexus"). It is important to recall, however, that the FCA's experiment is brand new. Its operating parameters will no doubt improve over time as both authorities and innovators gain more experience with the model.

59 Here it is important to note that several jurisdictions are currently attempting to follow the United Kingdom's lead by establishing national regulatory sandboxes of their own. This makes little sense in the blockchain space, since national regulatory approvals will have to be coordinated across nation-state borders at some point.

60 Competing national regulatory sandboxes have recently been announced or proposed in Singapore, Australia and the United States. See e.g. Monetary Authority of Singapore, "Consultation Paper on Fintech Regulatory Sandbox Guidelines" (6 June 2016), online: <www.mas.gov.sg/News-and-Publications/Consultation-Paper/2016/Consultation-Paper-on-FinTech-Regulatory-Sandbox-Guidelines.aspx>; Rachel Witkowski, "U.S. House Bill Aims to Set Up 'Sandbox' for Fintech Innovation", *Wall Street Journal* (22 September 2016), online: <www.wsj.com/articles/u-s-house-bill-aims-to-set-up-sandbox-for-fintech-innovation-1474539893>; Australian Securities and Investments Commission, "Further Measures to Facilitate Innovation in Financial Services", Consultation Paper 260 (specifically citing, at 38, developments in the United Kingdom, United States and Singapore as grounds for acting), online: <asic.gov.au/regulatory-resources/find-a-document/consultation-papers/cp-260-further-measures-to-facilitate-innovation-in-financial-services/>.

→ *Use case-tailored parameter-setting practices:* A blockchain sandbox must be capable of tailoring both the experimentation parameters it sets (things like timelines, test customer profiles, etc.) and the oversight and data monitoring requirements it imposes to the specifics of the use case in question. For example, certain sandbox innovations might implicate only sophisticated actors, others ordinary consumers. Hence, different informed-consent conditions might need to be formulated for the distinct target audiences. Likewise, the data the sandbox regulators seek to collect may differ across the two scenarios. Because blockchains can be employed in so many different ways by so many different actors for so many different purposes, the sandbox parameters applied should make sense in light of the underlying constellation of regulatory concerns raised in each case.

These ideas represent only a rough sketch and require further refinement to be properly operationalized. But there is clear potential for a global regulatory sandbox to yield significant dividends for blockchain technologies. It might be the fastest and most efficient way to realize the full developmental potential of these extraordinary innovations.

One question that arises is whether governments with diverse policy objectives will prove willing to cooperate on such an initiative, given the continuing persistence of entrenched internet governance challenges and competitive national interests. The timing seems auspicious for blockchain regulatory cooperation for several reasons. Leading governments all over the world have only recently awoken to the transformative possibilities of blockchain technologies. So far, very few concrete regulatory measures have been announced, leaving open a window of opportunity to build a transnational approach from the outset. Moreover, poorly received early regulatory interventions by certain jurisdictions — notably the State of New York's BitLicense scheme[61] — have helped to underscore that blockchain technologies and the people who build them are highly mobile, and this mobility dramatically reduces the incentive for regulators to "go it alone."[62] It makes little sense, after all, to develop competing national regulatory sandboxes for technologies that can operate from anywhere and everywhere with global reach.

Finally, the learning curve with blockchain is steep. Simply understanding how the technology operates — much less how one might regulate its innumerable use cases — requires a significant investment of time and resources. Blockchain expertise remains rare and expensive, even in the private sector. This complexity has already prompted the establishment of numerous cross-border consortia and blockchain working groups — not only in the private sector but also in traditionally non-cooperative regulatory sectors like central banking.[63] These factors point toward cooperation rather than competition as the preferable pathway for developing future regulatory approaches to blockchain technologies.

61 The BitLicense regime is described on the website of the New York Department of Financial Services, online: <www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm>.

62 At least a dozen well-known blockchain start-ups (Bitfinex, BitQuick, BTCGuild, Eobot, Genesis Mining, GoCoin, Kraken, LocalBitcoins, Paxful, Poloniex, Shapeshift and Xapo) chose to decamp to other jurisdictions rather than submit to the New York BitLicense regime. See Daniel Roberts, "Behind the 'Exodus' of Bitcoin Start-ups from New York", *Fortune* (14 August 2015), online: <fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/>. Dozens of newer start-ups are rumoured to have eschewed New York from the outset as a result of the BitLicense.

63 Michael del Castillo, "90 Central Banks Seek Blockchain Answers at Federal Reserve Event", *CoinDesk* (6 June 2016), online: <www.coindesk.com/central-banks-blockchain-federal-reserve/>. The same trend (cooperation among competitors) has been observed in the private sector, with the establishment of global consortia in diverse industries from banking to insurance to health care. See William Mougayar, "The State of Global Blockchain Consorita", *CoinDesk* (11 December 2016), online: <www.coindesk.com/state-global-blockchain-consortia/>.

Conclusion

Blockchains and other DLTs are rapidly transforming the way the world economy works. For the first time in history, they make it possible for people all over the world to transact securely on a peer-to-peer basis without trusted intermediaries. While this opens up exciting new pathways for individualized, human-centred markets, it also poses challenges for law makers, policy makers and regulators. Protecting and advancing the collective social good within an increasingly disintermediated global economy necessitates global regulatory innovation and adaptability on three fronts.

First, blockchain use cases falling into the recycle box call on national and international regulators faithfully to apply their existing regulatory regimes while making minor adjustments to ensure their continued smooth operation under blockchain implementations. Second, dark box use cases — the per se illegal ones — challenge regulators to find new modes of cross-border cooperation to clamp down on public menaces like blockchain-enabled drug trafficking and terrorist financing. Doing so effectively and responsibly requires building robust public consensus around and accountability mechanisms to control government collection and use of blockchain-based and other large-scale data analysis programs.

Third, there is a rapid proliferation of blockchain and DLT innovations promising to deliver clear social benefits by displacing or circumventing traditional regulatory choke points. This provides an opportunity for regulators to collaborate directly with entrepreneurs to find new ways to carry out important regulatory prerogatives. Establishing a global regulatory sandbox for blockchain and DLT that is cross-sectoral, start-up friendly and use-case specific is the most sensible way forward. Broadly representative national and international bodies with strong and cross-cutting development mandates are arguably best placed to advance this kind of global sandbox initiative.

Appendix 1: Blockchains in Brief

Author's note: what follows is a cursory introduction intended for non-technical readers. Readers in search of greater precision should consult the sources listed in Appendix 2.

Blockchains are shared ("distributed" or "decentralized") digital ledgers that use cryptographic algorithms to verify the creation and transfer of digitally represented assets or information over a peer-to-peer network.[i] They operate via an innovative combination of distributed consensus protocols, cryptography and in-built economic incentives based on game theory. The digital asset "native" to the first blockchain ever developed is the cryptocurrency known as Bitcoin — a non-state form of digital money that went into circulation in 2009 and has since enjoyed considerable success.[ii] Beyond non-state cryptocurrencies, blockchains can be used to represent, track and trade many other types of assets and information, including:

- fiat (government-issued) money;[iii]
- stocks, bonds, options, derivatives and other financial products;[iv]
- real and intellectual property rights;[v]
- contract rights;[vi]
- the movement of goods and services across a global supply chain;[vii]
- the expenditure of public[viii] or private[ix] funds; and
- personal and sensor-based data and messages.[x]

Blockchains can be set up in either public (permissionless — anyone can use them) or private (permissioned — restricted to use by approved parties) configurations, each of which entails distinct advantages and disadvantages. They can also be configured to accommodate greater or lesser degrees of user privacy. These and other design choices must be tailored to the specific goals pursued in each blockchain use case. Broadly speaking, however, blockchains can be specified to exhibit certain innovative properties that make them a highly useful tool in structuring our global economy, for instance:[xi]

- *distributed consensus*: no central point of control or failure (no choke points or intermediaries);
- *transaction transparency/auditability*: every ledger entry can be verifiable and retraceable across its full history (accountability); and
- *party identity abstraction*: individual parties can transact with one another across the network without revealing their full identities (enhanced privacy).

It is thanks to these and other properties that blockchains are often called the Internet of Value. They allow individuals and organizations to exchange value (for example, money, or assets, or assets for money) across borders in the same way the internet allows us to exchange information on a global, decentralized, peer-to-peer basis. And much like exchanging information on the internet, exchanging value on a blockchain is fast and cheap — often considerably faster and cheaper than the existing "legacy" systems of our global financial order. This makes blockchains an attractive vehicle for accomplishing a number of economic and non-economic objectives, as discussed above.

---

i For more detailed descriptions, see e.g. "Bitcoin", *supra* note 1; Volpicelli, *supra* note 7; and "Blockchains: The Great Chain of Being Sure About Things", *supra* note 7.

ii For a technical explanation, see Nakamoto, *supra* note 1. For non-technical readers, the Bitcoin Wiki page provides an accessible introduction: "Bitcoin", *supra* note 1.

iii Jane Wild, "Central Banks Explore Blockchain to Create Digital Currencies", *Financial Times* (2 November 2016), online: <www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a>.

iv See DTCC White Paper, *supra* note 12.

v Shin, *supra* note 10.

vi Morrison, *supra* note 14.

vii Higgens, *supra* note 8; Parker, *supra* note 9.

viii Samburaj Das, "UK Trials Blockchain-Based Social Welfare Payments", *CryptoCoins News* (7 July 2016), online: <www.cryptocoinsnews.com/uk-trials-blockchain-based-social-welfare-payments/>.

ix Parker, *supra* note 13.

x Some projects are beta testing Masked Authenticated Messaging (MAM). See e.g. the IOTA Development Roadmap and Github repository, online: <https://blog.iota.org/iota-development-roadmap-74741f37ed01> and <https://github.com/iotaledger/MAM.ixi>.

xi These and other characteristic are explained in DTCC Connection, "Eight Key Features of Blockchain and Distributed Ledgers Explained" (17 February 2016), online: <www.dtcc.com/news/2016/february/17/eight-key-features-of-blockchain-and-distributed-ledgers-explained>.

Appendix 2: Select Technical References

Satoshi Nakamoto (pseudonym), "Bitcoin: A Peer-to-Peer Electronic Cash System" (October 2008), online: <https://bitcoin.org/bitcoin.pdf>.

Vitalik Buterin, "A Next Generation Smart Contract and Decentralized Application Platform" (2015) Ethereum White Paper, online: <https://github.com/ethereum/wiki/wiki/White-Paper>.

Sergui Popov, "The Tangle" (2016) White Paper, online: <https://iota.org/IOTA_Whitepaper.pdf>.

Kyle Croman et al., "On Scaling Decentralized Blockchains" (Position paper delivered at the Financial Cryptography & Data Security 20th International Conference, Barbados, 22–26 February 2016), online: <fc16.ifca.ai/bitcoin/papers/CDE+16.pdf>.

QingChun ShenTu12 & JianPing Yu, "Research on Anonymization and De-anonymization in the Bitcoin System" (2015), Working Paper, online: <https://arxiv.org/abs/1510.07782>.

Ian Miers, Christina Garman, Matthew Green & Aviel D Rubin, "Zerocoin: Anonymous Distributed Cash from Bitcoin" (Paper delivered at the 2013 IEEE Symposium, Berkeley, 19–22 May 2013), online: <ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6547123>.

Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer & Madars Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin" (Proceedings of the IEEE Symposium on Security & Privacy, Oakland, 2014), 459–74, online: <zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org