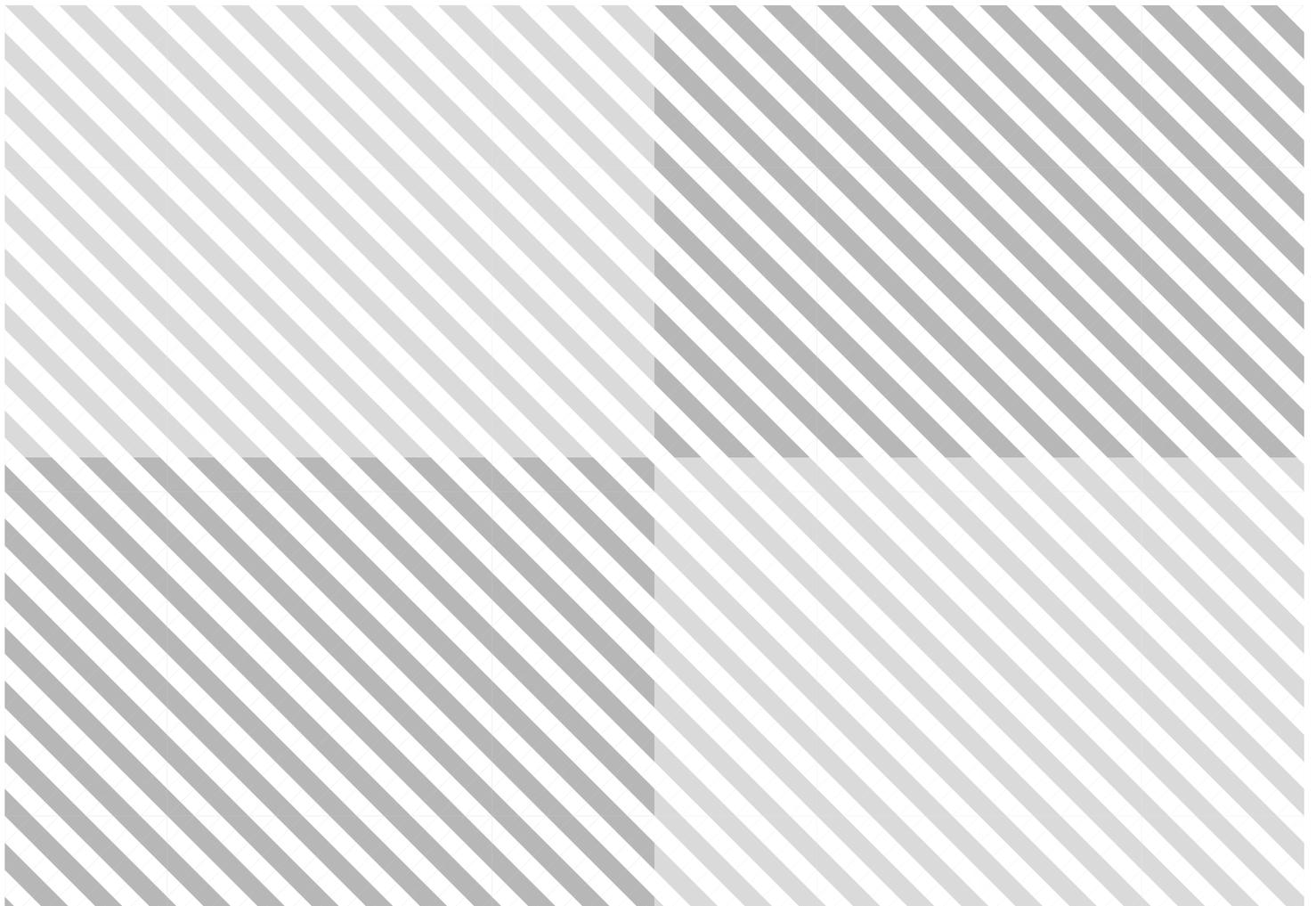


White Paper

Realizing the Potential of Blockchain

A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies

June 2017



White Paper Authors:

Don Tapscott and **Alex Tapscott**

Contents

Preface	2
Executive Summary	3
The Blockchain as a New Global Resource	4
New Thinking in How to Steward a Global Resource: The Internet as a Case Study	5
Blockchain Governance Challenges	7
1. Stewardship of platforms	10
2. Stewardship of applications	24
3. Stewardship of the ecosystem as a whole	27
The Players in the Blockchain Ecosystem	32
The “Global Solution Networks” (GSN) Framework Applied to Blockchain	34
Standards networks: Don’t deify differences; codify common ground	36
Networked institutions: Welcome stakeholders everywhere	37
Advocacy networks: Respect members’ interests and constraints	38
Watchdog networks: Do no harm	38
Policy networks: Participate in debate and coordinate regulation	39
Knowledge networks: Know what you don’t know	40
Delivery networks: Keep incentives for mass collaboration in mind	41
Summary: What Needs to Be Done	42
About the Authors	45
Appendix: Global Solution Networks	46
Knowledge networks	46
Operational and delivery networks	48
Policy networks	49
Advocacy networks	49
Standards networks	50
Networked institutions	51
Acknowledgements	51
Notice	51
Endnotes	53

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

World Economic Forum®

© 2017 – All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

REF 240617 – 00034436

The views expressed in this White Paper are those of the author(s) and do not necessarily represent the views of the World Economic Forum or its Members and Partners. White Papers are submitted to the World Economic Forum as contributions to its insight areas and interactions, and the Forum makes the final decision on the publication of the White Paper. White Papers describe research in progress by the author(s) and are published to elicit comments and further debate.

Preface

Distributed ledger technology promises to have far-reaching economic and social implications. By leveraging a global peer network to assure directly and transparently the integrity of value exchanged between parties, blockchain appears likely to transform a number of important industries that supply or rely upon third-party assurance. It could prove to be a broader force for transparency and integrity in society, including in the fight against bribery and corruption. It could also lead to extensive changes in supply chains and governmental functions, such as central banking.

The extent to which this new technology realizes its potential will depend in substantial part upon how well stakeholders steward its development. There remain important open governance questions regarding both the functioning of the technology and its current and potential applications.

The World Economic Forum and its new Center for the Fourth Industrial Revolution is pleased to publish this foundational survey of blockchain governance challenges and multistakeholder cooperation opportunities. Authored by Don and Alex Tapscott, leading experts on both blockchain and multistakeholder governance, this White Paper provides a structured analytical framework and taxonomy for use by industry, technical, governmental, civil society and other stakeholders in considering how they might collaborate to resolve problems and unlock opportunities beyond the reach of any single actor.

As Don and Alex emphasize, a distributed ecosystem need not be a disorganized one, and improved governance need not imply formal governmental legislation or regulation. A cooperative process of multistakeholder dialogue and stewardship can go a long way in improving trust and helping new technological systems develop in a socially beneficial manner.

This is the animating purpose of the Center for the Fourth Industrial Revolution: to provide an international platform for public-private dialogue and cooperation in respect of the stewardship and agile governance of new technologies. We thank the authors for their contribution, which we believe provides a solid foundation for precisely such a process in respect of blockchain. We also thank members of the World Economic Forum Global Future Council on the Future of Blockchain and others who provided feedback on the White Paper, which expresses the perspectives of the authors alone and not necessarily those of the Forum as an institution or its individual Members and constituents.

Richard Samans

Head of the Center for the Global Agenda and Member of the Managing Board

Zvika Krieger

Head of Technology Policy and Partnerships

Geneva and San Francisco, June 2017

Executive Summary

Like the first generation of the internet, this second generation promises to disrupt business models and transform industries. Blockchain (also called distributed ledger), the technology enabling cryptocurrencies like bitcoin and Ethereum, is pulling us into a new era of openness, decentralization and global inclusion. It leverages the resources of a global peer-to-peer network to ensure the integrity of the value exchanged among billions of devices without going through a trusted third party. Unlike the internet alone, blockchains are distributed, not centralized; open, not hidden; inclusive, not exclusive; immutable, not alterable; and secure. Blockchain gives us unprecedented capabilities to create and trade value in society. As the foundational platform of the Fourth Industrial Revolution,¹ it enables such innovations as artificial intelligence (AI), machine learning, the internet of things (IoT), robotics and even technology in our bodies, so that more people can participate in the economy, create wealth and improve the state of the world.

However, this extraordinary technology may be stalled, sidetracked, captured or otherwise suboptimized depending on how all the stakeholders behave in stewarding this set of resources – i.e. how it is governed.

Like the first era of the internet, this blockchain era should not be governed by nation states, state-based institutions or corporations. How we govern the internet of information as a global resource serves as a model for how to govern this new resource: through a multistakeholder approach using what we call “global governance networks”— a concept developed in our previous multimillion-dollar programme investigating multistakeholder networks for global problem-solving.² We discuss seven types of networks: standards networks, such as the Internet Engineering Task Force; knowledge networks, such as the Internet Research Task Force; delivery networks, such as the International Corporation for Assigned Names and Numbers; policy networks, such as the Internet Policy Research Initiative at the Massachusetts Institute of Technology (MIT); advocacy networks, such as the Alliance for Affordable Internet; watchdog networks, such as the Electronic Freedom Forum; and networked institutions, such as the World Economic Forum.

We explain the core differences between the internet of information as a network of similar networks and the blockchain as a balkanized internet of value, where real assets are at stake. Then we cover what we have found to be the most urgent threats to this resource, which we view as governance challenges. By governance, we mean stewardship, which involves collaborating, identifying common interests and creating incentives to act on them. We do not mean government, regulation or top-down control. We explore governance needs at three levels: platform, application and the ecosystem as a whole.

Unlike the internet of information, which is a vast network of similar networks, this internet of value requires stewardship at not just one level but three. At the platform level, we look at bitcoin’s scalability issue and energy consumption, Ethereum’s switch to proof-of-stake and crisis management by consensus, and Hyperledger’s call for both urgency and moderation around standards. At the application level, we look at the need for oversight, skilled talent and user-friendly interfaces. At the overall ecosystem level, we look at the need for a proper legal structure, regulatory restraint, diversity of viewpoints and scientific research in tandem with business development. We introduce each of the eight stakeholders in the ecosystem: innovators, venture capitalists, banks and financial services, developers, academics, non-governmental organizations (NGOs), government bodies, and users or citizens.

We apply our previously developed “global solution networks”³ (GSN) framework to blockchain governance. We urge stakeholders in the space to codify their common ground through standards networks; welcome stakeholders with radically diverse views of what needs to be done through networked institutions; respect members’ interests and constraints through advocacy networks; ensure that no one does any harm through watchdog networks; participate in policy debates and coordinate regulation through policy networks; get up to speed through knowledge networks; and keep incentives for mass collaboration in mind through delivery networks. Finally, we outline the most pressing governance work to be done, if we are to preserve and steward this new global resource to achieve its vast potential.

The Blockchain as a New Global Resource

The internet is entering a second era that's based on blockchain. The last few decades brought us the internet of information. We are now witnessing the rise of the internet of value. Where the first era was sparked by a convergence of computing and communications technologies, this second era will be powered by a clever combination of cryptography, mathematics, software engineering and behavioural economics. It is blockchain technology, also called distributed ledger technology. Like the internet before it, the blockchain promises to upend business models and disrupt industries. It is pushing us to challenge how we have structured society, defined value and rewarded participation.

Blockchain emerged in the wake of the global economic crisis, when a pseudonymous person or persons named Satoshi Nakamoto released a new protocol for "A Peer-to-Peer Electronic Cash System" using a cryptocurrency called bitcoin.⁴ Cryptocurrencies (digital currencies) are different from traditional fiat currencies because no government issues or controls them. They're not saved in a file somewhere; they're represented by transactions recorded in a blockchain – like a global spreadsheet or ledger, which leverages the resources of a large peer-to-peer bitcoin network to verify and approve each bitcoin transaction. Satoshi's protocol established a set of rules – in the form of distributed computations – that ensured the integrity of the data exchanged among billions of devices without going through a trusted third party. This new resource has six critical qualities.

Each blockchain, like the one that uses bitcoin, is distributed: it runs on computers provided by volunteers around the world; there is no central database to hack or shut down. We can send money and soon any form of digitized value – from stocks and bonds to intellectual property, art, music and even votes – directly and safely between us without going through a bank, a credit-card company, PayPal or Western Union, social network, government or other middleman. Of course, this does not mean that middlemen will disappear. Rather the technology provides profound opportunities for innovative companies and institutions in the middle to streamline processes, increase their metabolism, create new value and enter new markets.

Blockchain is encrypted: it uses heavy-duty encryption involving public and private keys (rather like the two-key system to access a safety deposit box) to maintain virtual security. We needn't worry about the weak firewalls of the US Democratic National Party, a thieving staffer of Morgan Stanley or a perversely incentivized employee of Wells Fargo.

In many cases, blockchain is public: anyone can view it at any time because it resides on the network, not within a single institution charged with auditing transactions and keeping records. No one can hide a transaction, and that makes bitcoin more traceable than cash. It is open-source code: anyone can download it for free, run it and use it to develop new tools for managing transactions online. Private blockchains have emerged that don't use cryptocurrency for consensus.

Blockchain is, for the most part, inclusive. Satoshi imagined that the typical person would be interacting with the blockchain through what he called "simplified payment verification" mode that can work on a mobile device.⁵ Now anyone with a flip phone can participate in the global economy; no documentation is required to be trusted.

Blockchain is immutable. Within minutes or even seconds, all the transactions conducted are verified, cleared and stored in a block that is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. This structure permanently timestamps and stores exchanges of value, preventing anyone from altering the ledger.

Blockchain is historical. If we wanted to steal a bitcoin, we'd have to rewrite a coin's or asset's entire history on the blockchain in broad daylight. So the blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Therefore, we must preserve the blockchain in its entirety. That's why storage matters.

This is much more than the financial services industry. Innovators are programming this new digital ledger to record anything of value to humankind – birth and death certificates, marriage licenses, deeds and titles of ownership, rights to intellectual property, educational degrees, financial accounts, medical history, insurance claims, citizenship and voting privileges, location of portable assets, provenance of food and diamonds, job recommendations and performance ratings, charitable donations tied to specific outcomes, employment contracts, managerial decision rights and anything else that we can express in code.

So important is this new resource that some have called the blockchain a public utility like the internet, a utility that requires public support. Paul Brody, principal and global innovation leader of blockchain technology at Ernst & Young, thinks that all our appliances should donate their processing power to the upkeep of a blockchain: "Thanks to the smartphone business driving very low-cost systems, your lawnmower or dishwasher is going to come with a CPU that is probably a thousand times more powerful than it actually needs, so why not have the appliance mine? Not to make money, but to contribute to the security and viability of the blockchain as a whole," he said.⁶

We've never had this capability before – trusted transactions directly between two or more total strangers, authenticated by mass collaboration, and powered by collective self-interests, rather than by corporations motivated by profit or governments motivated by power. It is the culmination of what Alan Turing started, a true paradigm shift ushered in by decentralized ledger technologies.

In this report, our goal is not to provide specific proposals, though we have suggested a few possible directions. Our goal is to describe the landscape, provide a taxonomy for rich discussions, map the diverse players to the taxonomy, surface the topics of concern and identify the requirements for better stewardship. We encourage all players – not just those in financial services – to think about whole ecosystem and not simply their own narrow interests. We believe that this rising tide should lift all boats.

New Thinking in How to Steward a Global Resource: The Internet as a Case Study

The governance of critical global resources – water, old growth forests, fisheries and the internet itself – has been a key focus of our research over the last five years. When we use the word, *governance*, we mean *stewardship*, which involves collaborating, identifying common interests and creating incentives to act on them. We do not mean *government*, which involves legislating and regulating behaviour and punishing those who misbehave.

Since the end of World War II, state-based institutions have administered most of the world's important resources. Two of the most powerful – the International Monetary Fund and the World Bank – were born at the Bretton Woods Conference in 1944. The United Nations and other groups under its umbrella – the World Health Organization and the World Trade Organization – received a wide berth to exercise their monopoly on global problem-solving. These organizations were hierarchical by design, because hierarchies were the dominant paradigm during the first half of a war-torn century.

But while necessary, these industrial-scale solutions were and still are insufficient for the challenges of the digital era. The rise of the internet marked a significant departure from the traditional culture of governance. “We reject kings, presidents and voting,” said MIT computer scientist David Clark in 1992. “We believe in rough consensus and running code.”⁷ That was the mantra for stewardship of the first generation of the internet when few could imagine how it would transform human existence. Clark's words embodied a philosophy for the leadership of a global resource that was radically different from the Bretton Woods model, yet one that engendered a remarkably effective governance ecosystem. That the internet has become a global resource in so short a time is astounding, in no small part thanks to strong leadership and governance and despite the powerful forces against it.

Governance means stewardship, not government or regulation.

In our 2013-2015 research, we set out to do the definitive investigation into internet governance – *who exactly was providing this stewardship to ensure the development and continuance of the internet and what made the ecosystem tick. No government or group of governments controls the internet or its standards, though several U.S government agencies once funded it.*⁸ Instead, a vast ecosystem of companies, civil society organizations, software developers, academics and state-based

institutions were collaborating in transparent, distributed forums that defied measurement by traditional command-and-control frameworks. In the infancy of the internet as a global resource, this ecosystem has proven that diverse stakeholders, loosely organized in seven types of open networks that operate by consensus, could effectively steward a global resource.

1. Standards networks

Standards networks are non-state, non-profit organizations – such as the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF) – that develop technical specifications and standards, the building blocks of the product, and infrastructure development that leads to mass adoption. To succeed as standards networks, the IAB and IETF regularly engage the expertise of individuals, civil society organizations and private-sector enterprise. Similarly, the World Wide Web Consortium (W3C) develops, tests and implements standards that promote the web's evolution and ensure its interoperability.

2. Knowledge networks

The primary function of knowledge networks is to conduct research and develop new ideas that can help solve global problems. For example, the Internet Research Task Force (IRTF) investigates emerging technologies of potential relevance to the internet. If IRTF creates a specification suitable for standardization, then it proposes it to the IETF. More savvy users can realize the upside of new global resources while minimizing the downside. Internet2 (www.Internet2.edu) is a global research and education network designed to remove barriers to discovering new knowledge and its impact.

3. Delivery networks

This class of networks actually delivers the change it seeks, supplementing or even bypassing the efforts of traditional institutions. For example, the International Corporation for Assigned Names and Numbers (ICANN) delivers domain names. Supporting delivery networks include African Network Information Centre (AfriNIC), American Registry for Internet Numbers (ARIN), Asia-Pacific Network Information Centre (APNIC), Latin America and Caribbean Network Information Centre (LACNIC), and Réseaux IP Européens Network Coordination Centre (RIPE).

4. Policy networks

These networks support policy development or seek alternatives for policy, whether governments support them or not. The goal is to inform, if not shape, the policy-making process of corporations and governments so that it is more transparent, shared and inclusive. For example, Internet & Jurisdiction facilitates transnational cooperation on cybersecurity, human rights, and other legal and economic policies.⁹ The Internet Policy Research Initiative at the MIT Computer Science and Artificial Intelligence Lab also works with technologists and policy-makers to increase the integrity of interconnected digital systems. In 2016, 17 public interest groups collaborated to develop the Internet Policy Platform, which featured specific policy initiatives on internet access, choice, free speech, privacy and transparency.¹⁰

5. Advocacy networks

Advocacy networks seek to change the agenda or policies of governments, corporations and other institutions. Among them are internet.org and the Alliance for Affordable Internet, which advocate for greater inclusion. The Industrial Internet Consortium, a relatively new open group of researchers, companies and public agencies, is advocating the adoption of internet applications across various industries to accelerate the IoT.¹¹

6. Watchdog networks

These networks scrutinize organizations to ensure that they behave appropriately. Topics range from human rights, corruption and the environment, to financial services and commercial practices. In the process, they drive public debate, boost transparency and ignite movements for change. Perhaps the most vocal watchdog of civil liberties online is the Electronic Frontier Foundation.¹² It scrutinizes corporate and government policies and holds them accountable through litigation and grass-roots activism.

7. Networked institutions

Some networks provide such a wide range of capabilities that we describe them as “networked institutions”. They are not state-based but true multistakeholder networks. The value they generate can range from knowledge, advocacy and policy to the actual delivery of solutions. The Internet Society, for example, excels at incorporating the many views of diverse stakeholders, not just the efforts of the IAB, the IETF and the IRTF, but also the International Telecommunications Union, the Organisation for Economic Co-operation and Development, the World Intellectual Property Organization and several other United Nations commissions.¹³ The Internet Governance Forum (IGF) also engages participation across stakeholder groups.

Most governments showed both restraint and foresight in regulating the internet.

In the early days of the internet, governments demonstrated both restraint and foresight. They showed restraint by limiting regulation and control throughout the internet's evolution and they showed foresight by allowing the system to flourish before trying to impose rules and regulations. Now that the internet has permeated every aspect of our lives, courts and legislators have started recognizing new claims, such as the right to be forgotten, and imposing local rules that often conflict in the global realm of the digital. As the best example of a true networked institution (not controlled by nation states), the World Economic Forum has stepped up to caution against such uncoordinated legal efforts that only fragment the internet, creating what some are calling the “splinternet”, and thereby stunting the “internet's enormous capacity to facilitate human progress”.¹⁴

Blockchain Governance Challenges

In our previous research, we determined that the stewardship of the internet of information was relatively simple compared to what this nascent internet of value would need. True, the internet has been a vast “network of networks” with intricate issues of standards and other governance challenges. But we all use basically the same coherent platform globally. On it rests the world wide web and countless other applications.

Blockchain, at least at this stage of its development, is more balkanized and complex. The economic stakes are higher. “This is very different from the somewhat hippy style that the open-source, free software internet movement had,” Joichi Ito, Director of the MIT Media Lab said. “We’re going a little too fast in promising our investors a functioning infrastructure. ... Many companies are raising money as if they’re ready for production. ... These guys are all under the microscope, under the gun. Many of them are heavily funded and it’s really hard.”¹⁵

*The internet is a network of similar networks.
The blockchain is a ledger of different and sometimes competing ledgers.*

“Bitcoin is a car going down the road at 1,000 mph,” said Matthew Roszak, Co-Founder of Bloq Inc. “Developers are not the drivers of this car, yet they are tasked with repairing and upgrading this car without turning it off, stopping it or rebooting it.”¹⁶ Most developers prefer it that way. They think bitcoin is already very well regulated by mathematics, which are not up to the whims of governments. Other developers take issue with the word, *governance*, because they associate it with the belief that the technology is broken and needs to be fixed or that the process has stopped working and needs to be saved. They prefer the word, *stewardship* – and appropriately so.

Where the internet democratized information, the blockchain democratizes value and cuts to the core of legacy industries like banking. It also pertains to the management of money, wealth, intellectual property and other forms of value for which many societies expect government to protect the public interest. So we all need to acknowledge that, while governments and regulators alone lack the knowledge, resources and mandate to govern this technology effectively, government participation and even regulation will likely have a greater influence over blockchain technologies to ensure that we preserve both the rights and powers of consumers and citizens. People in free societies have the right to free speech and have the power to express it on the internet of information but not the power to protect it from piracy, hacking or censorship. One of the defining characteristics of an open

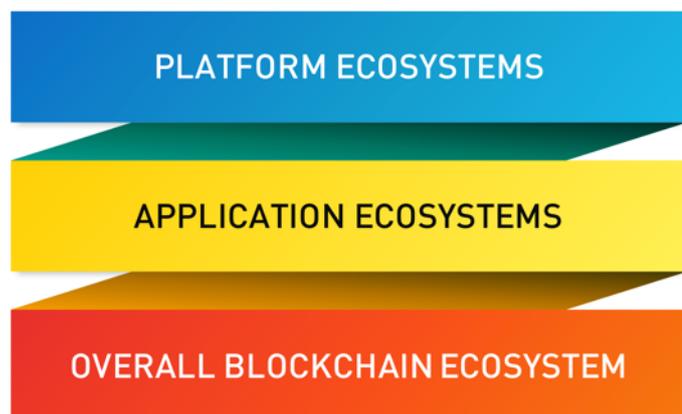
permissionless blockchain is that no one has the right to anything. There are really just powers, what you have the power to do, what you can do. Joichi Ito put it in these terms: “You can regulate networks, you can regulate operations, but you can’t regulate software.”¹⁷ On the internet of value, people will have the power to express themselves and the power to preserve their expression without restriction.

But these differences don’t require government to control, oversee or somehow govern the blockchain revolution. The genius of distributed ledgers is that the technology (and everything that happens with it) is and must be distributed. Power is distributed. Heavy-handed government intervention would kill this embryonic technology in its egg.

Rather, we need self-organizing, bottom-up and multistakeholder governance. In fact, this type of governance is the best protection from government interference and subjugation. According to Primavera De Filippi, faculty associate at the Berkman Center for Internet & Society at Harvard and a permanent researcher at the National Center of Scientific Research in Paris, the absence of a formalized governance structure has two possible effects: either blockchain-based communities have difficulty acting or reacting expeditiously or else informal and invisible power dynamics emerge, often more centralized than they appear.¹⁸ That bears repeating: without governance, invisible powers could emerge.

In our research, we found ourselves exploring three levels of blockchain that warrant stewardship (see Figure 1). *The first is the platform level, the protocols of blockchains such as bitcoin, Ethereum, Ripple or Hyperledger. While people often speak of virtual currency as a financial instrument and blockchain as a payment system – and, therefore, relevant narrowly to banking and finance – we think of them more broadly as an ownership claim on a particular technology platform, a claim represented by a token that comes with decision rights and usually an incentive to ensure the platform’s long-term success. So what we discuss throughout this report applies to all domains, not just finance.*

Figure 1: Blockchain: Three Levels of Governance



Source: Authors

The second is the application level, the tools that run on platforms, tools such as smart contracts, that require massive cooperation between stakeholders to work. As with the internet, entrepreneurs have been quick to seize blockchain business opportunities and innovate business practices. The recent rise of so-called “initial coin offerings” is turbocharging growth at the application layer, raising regulatory questions and accelerating the need for multistakeholder governance. With the internet of information, various companies, governments, NGOs and individuals could simply build an application using either the web or more proprietary mobile platforms like the iPhone or Android. However, because blockchain is all about value, developers are building applications, networks and projects within particular ecosystems – sometimes with a complex assembly of stakeholders who create, exchange and manage value.

Consider the Belt and Road project – the new Silk Road railway linking Hong Kong SAR and Rotterdam. The Hong Kong Monetary Authority (HKMA) led an initiative to develop a proof-of-concept distributed ledger platform for trade finance. The goal was to increase efficiency and productivity by enhancing the transparency and trustworthiness of information for regulatory reporting by putting it on the blockchain, thereby eliminating the need for a central authority. The HKMA continues to sort through the legal, regulatory and governance issues of using blockchain.¹⁹ Launching this type of application requires massive collaboration among companies, governments and other entities. Similarly, this resource will need constant care and tending to onboard more and more users over time. It illustrates the profound differences between managing information creation versus value creation activities. The latter require deep negotiation, contractual and jurisdictional understandings, and the ongoing stewardship of application-level ecosystems.

The third is the overall ecosystem, the ledger of ledgers connecting (or not) bitcoin, Ethereum, Hyperledger, Ripple, Tendermint and other platforms. We found that many of these are quite different in their world views and choice of protocols but present a common set of issues that we think a variety of stakeholders – including consumers and citizens – should understand and be able to discuss. In this section, we cover what we have found to be most urgent for survival in the near term and critical for sustainability in the long term, so this list is by no means exhaustive.

1. Stewardship of platforms

Countless blockchain platforms exit and countless more are in development. Consider Table 1, showing the top 10 platforms where cryptocurrency represents both value and ownership in the platform. For this paper, we review the top two platforms with tokens trading on the marketplace, bitcoin and Ether, and two platforms, Cosmos and Hyperledger, that seek to provide interoperability among other platforms.

Table 1: Top 10 Cryptocurrencies, as of 17 June 2017

Rank	Name	US\$ Market Cap	US\$ Price	Circulating Supply
1	Bitcoin	43,630,891,619	2660.98	16,396,550 BTC
2	Ethereum	34,736,739,597	375.25	92,569,593 ETH
3	Ripple	10,215,346,626	0.266787	38,290,271,363 XRP
4	Litecoin	2,428,105,598	47.06	51,592,007 LTC
5	Ethereum Classic	1,950,098,114	21.04	92,694,964 ETC
6	NEM	1,848,834,000	0.205426	8,999,999,999 XEM
7	Dash	1,295,180,283	175.78	7,368,399 DASH
8	IOTA	1,177,470,178	0.423622	2,779,530,283 MIOTA
9	BitShares	888,444,894	0.342215	2,596,160,000 BTS
10	Stratis	766,295,675	7.79	98,428,282 STRAT

Source: CryptoCurrency Market Capitalizations, <https://coinmarketcap.com/currencies>, accessed 17 June 2017

“The platforms that will win will be the ones that can fulfil both the operational and the governance requirements of a range of applications – because you are not going to move equity settlement, for example, to an environment that cannot meet the disclosure requirements of capital markets regulators,” said Jesse McWaters of the World Economic Forum. “Capital markets regulators are not going to change their view on what should and should not be disclosed simply because the process is now occurring on a blockchain.”²⁰

Perianne Boring, founder and president of the Chamber of Digital Commerce, which has over 100 members from the digital asset, blockchain and traditional capital markets industries, said, “At the platform level, efforts to assist with scaling and interoperability are in most high demand.”²¹
Bitcoin

Bitcoin, the largest cryptocurrency and platform by value, volume and hashing rate (a measure of participation), started as an experiment in monetary theory, where the network functioned in service of the bitcoin token of value. Satoshi Nakamoto attempted to align stakeholder incentives through the code itself, and the technology thrived in its early years, blossoming into the ecosystem we know today.

In our research, we found that code alone has been insufficient. Open-source collaboration is a great organizing principle but it’s not a *modus operandi* for making big decisions and moving forward. Open-source projects like Wikipedia and Linux, despite their meritocratic principles, still have benevolent dictators Jimmy Wales and Linus Torvalds. To many observers, bitcoin has a governance crisis. As with all disruptive technologies, competing interpretations of Satoshi’s vision have emerged. Even the core blockchain contingent has begun splitting into different cryptocamps, each advocating a separate agenda.

Some experts interviewed argued that all will be well, that debate is good and that as the song goes “Don’t worry, be happy.” But virtually all agreed that most recent attempts to get the parties together have been distasteful and deeply unproductive events.

The “open war”, as some called it, is clearly hurting bitcoin. This is likely one of the factors in the looming “blockchain flipping” where the upstart blockchain Ethereum is about to eclipse bitcoin in value. The community is not so happy about the state of bitcoin. For example, blockchain publishing company CoinDesk reported that in a survey of 1,100 virtual currency users, 94% stated they were positive about the state of Ethereum, while only 49% were positive about bitcoin.²²

At one time, the Bitcoin Foundation funded development of the Bitcoin Core protocol (the common standards used by the community), but it nearly collapsed from its own mismanagement: board member Mark Karpeles was arrested in Japan for embezzlement through his Mt. Gox cryptocurrency exchange. Recognizing the profound

importance of this technology, MIT created the Digital Currency Initiative (DCI), which gave a home to some of the Bitcoin Core developers (“core devs”). “We stepped in immediately and provided them with positions at the MIT Media Lab, so they could continue to independently work on supporting the core development of bitcoin,” said Brian Forde, the former White House insider and blockchain advocate who until recently headed the DCI.²³ For core devs, their ability to work autonomously was central to the design. Joichi Ito at the MIT Media Lab said, “We are now supporting Cory Fields, who’s one of the core devs; Wladimir van der Laan, who’s the lead developer of bitcoin; Tadge Dryja, who was the inventor of the Lightning Network. He had originally done a start-up, but now he’s joined us to be a researcher. And he’s hired Robleh Ali, who was the head of digital currencies from the Bank of England.”²⁴ It is a formidable group.

“Making decisions in a decentralized system is not easy,” said Roszak of Bloq Inc. “The bitcoin ecosystem is currently facing some significant growing pains as the number of transactions has been growing exponentially – over 200,000 transactions per day.” Roszak views this growth as “a clear measure of success and a testament to bitcoin’s adoption and evolution.” He told the US House of Representatives, “As it grows, it faces governance challenges which it is currently struggling to overcome. These challenges, I would imagine, are similar to those faced by the US Congress on a daily basis. This industry needs a *call to action* to resolve its differences and find a path forward.”²⁵

“Just because you’re decentralized doesn’t mean you’re disorganized,” said Pindar Wong, Chairman of VeriFi (Hong Kong), former Vice-Chair of ICANN and Trustee of the Internet Society. “People believe, mistakenly, that the blockchain ecosystem, specifically the bitcoin system, is disorganized. They get that impression from the very voluminous and heated debates around this very contentious technology. These disputes, the so-called scaling wars, the block-size debate, are examples of a healthy ecosystem.”

Decentralized doesn’t mean disorganized.

In our decades of research in technology and innovation, deadlock has rarely been a positive, particularly when both sides are accusing the other of spreading falsehoods, censoring opinion and trolling (that is, making provocative or deliberately offensive comments online with the primary intent of upsetting or angering an individual or group and the secondary intent of sounding unnecessary alarms, raising baseless doubt or distracting attention from real issues) rather than seeking common ground on which to have a civil conversation. “Any consensus mechanism that you have is going to be susceptible to marketing – where powerful interests spend money trying to convince people to do a certain thing,” said Stephen Pair, Chief Executive Officer of BitPay.²⁶ Consider this April 2017 exchange on Twitter regarding upgrades to the bitcoin protocol:

“Bitcoin Unlimited is production ready. It’s already producing 40% of all the blocks. More than any other version of Bitcoin,” tweeted Roger Ver, bitcoin angel investor.²⁷

Philip Francis, a digital assets investor, replied, “Come on Roger, you can’t actually believe BU [Bitcoin Unlimited] is production ready. It’s either pure delusion or you’re purposely trying to break Bitcoin.”²⁸

Adam Back, Chief Executive Officer of bitcoin-based Blockstream, responded to two Twitter users, “[Ver]’s paying people to put BU coinbase string. Then trumpeting stats. It’s bug filled, untested, far from production. Even algo[rithm] is defective.”²⁹

Ver retweeted Back with this comment, “Adam, you are telling lies about me again. I’ve paid no one to put BU in the Coinbase string. I await your retraction and apology.”³⁰

Based on our findings, we believe the bitcoin community needs a shared and inclusive vision for the future and a mechanism not just for sorting the important signals from the noise of trolls on social media but also for mobilizing to address them as an ecosystem. We’re not saying that anyone should force anyone else to do anything.

Our concern is that, with every major disagreement absent of a compelling vision beyond the libertarian dream, the network will continue forking into competing chains, each potentially less secure than the previous, putting the enormous value of the platform at risk. Indeed, libertarianism may blind its adherents to their need from time to time for stewardship, and the attitude is one that precludes widespread adoption and investment. If the bitcoin network is to grow, several critical challenges need to be addressed. Here are the three most contentious.

Governance challenge: How to scale without weakening the network

For years now, whether to increase the one megabyte block size has been a divisive subject with no resolution in sight. According to Forde, the former director of DCI, “If you look at the block-size debate, is it really a debate about block size? In the media, it’s a debate about block size, but I think what we’re seeing is that it’s also a debate on governance.”³¹

In August 2015, then-core developer Gavin Andresen advocated Bitcoin XT, a fork of the blockchain that allowed for eight-megabyte blocks. It was a controversial compromise that didn’t take.³² The biggest pushback came from the mining pools in China. Serious bitcoin miners, like hard-core online gamers, need not only seriously powerful computers to find a correct hash but also extremely high-speed bandwidth to broadcast it quickly across the network. China is an exception to Nielsen’s Law of Internet Bandwidth: bandwidth doesn’t increase by 50% each year. If the block-size increase is too large, it would put low-

bandwidth Chinese miners at a disadvantage compared with miners in other parts of the world. Receiving new blocks to build upon would take longer, and when they did find a new block, they would take longer to send it out to the rest of the network. These delays would ultimately result in the network’s rejecting some of their blocks. They would lose out to miners with more bandwidth whose blocks propagated faster.

Opponents of larger block sizes argue that people shouldn’t be using bitcoin to buy cups of coffee or other everyday purchases. “Some developers want every single person in the world to be running a fully validating node that sees every single transaction and has absolutely no trust on anybody else,” said Andresen. “The volunteer contributors who have been actually making the software work for the last few years are worried that they personally may not be able to handle larger blocks if transaction volume ramps up. ... I don’t have a whole lot of sympathy for that.”³³ In other words, if the bitcoin blockchain was to scale and remain secure, then the community couldn’t have it both ways. Some nodes would run full protocols and process more transactions into increasingly larger blocks, and others would run simplified payment verification models and trust that 51% of full nodes get it right. Besides, the 2 billion people currently excluded from centralized payment systems would more likely use cryptocurrencies for smaller than average transactions.

In April 2017, two different camps of core devs emerged again to address block size by launching different updates to the Bitcoin Core protocol. The first was referred to as “segregated witness” (SegWit), proposed by Blockstream Co-Founder Pieter Wuille and favoured by many core devs. SegWit would free up block space by separating (segregating) the signature (witness) information from the transaction data so the network could double the number of transactions processed per second. This solution would maintain the decentralization of power across the network. The other, Bitcoin Unlimited (BU) advocated by investor Roger Ver, would let miners vote on increasing the block size whenever needed, thus ceding them the power to control the number of transactions in a block.³⁴

In May 2017, a group of bitcoin miners and start-up executives met and agreed on what they considered a win-win resolution to the block-size stalemate, essentially a proposal, “Segwit2Mb – combined soft/hard fork,” posted for peer review in March 2017 by RSK Labs developer Sergio Demian Lerner.³⁵ Investment firm Digital Currency Group claimed that, as of 25 May 2017, the signatories to this agreement represented 20.5 million bitcoin users, 58 companies in 22 countries, 83% of hashing power, and \$5.1 billion in monthly onchain transaction volume.³⁶ Yet none of the current Bitcoin Core developers have signed on. Samson Mow, Chief Strategy Officer of Blockstream, a blockchain company that neither attended the meeting nor signed the proposal, cast doubt on whether the proposal had the majority of support needed to influence the bitcoin network’s destiny. Matthew Corallo, Co-Founder of Blockstream and currently an engineer at ChainCode Labs, expressed disappointment in people’s ignoring bitcoin

developer feedback. He said there were better technical solutions to the problem. Jeff Garzik, Founder of bitcoin start-up Bloq, argued that the proposal was attracting new companies to fund technical efforts that would ultimately improve the open-source code. He signed the agreement, as did Erik Voorhees, Founder and Chief Executive Officer of coin exchange ShapeShift. Voorhees told CoinDesk that, while he supported SegWit, he didn't care which solution was chosen as long as a solution was chosen to end the deadlock and increase the block size.³⁷ Jamie Smith, Global Chief Communications Officer of Bitfury, conveyed Bitfury's utmost respect for the Bitcoin Core developers: "We are working to create an agreement and technical roadmap [for the proposal] that suits everyone and is best for the future of bitcoin. We are confident that the road ahead is paved with promise and endless possibility."³⁸

Such a fork would be similar to a stock split.

We see at least four possible outcomes: (1) miners rally around BU; (2) SegWit, as the better technology, prevails; (3) the chain forks and they fight it out in the market; or (4) the sides cooperate and reach a compromise that both can support, the success of which plants the seed for some governance mechanism. We support option four, but we think option two most likely. Pair of BitPay believes that, if a substantial portion of the community feels it would be better served by a different set of consensus rules, then it will very likely create a fork with its preferred set of rules. The fork would likely compete with and either overtake or co-exist in perpetuity with the original chain, each finding its own market. "Such a fork would be very similar to a stock split," he said.³⁹

Without governance, invisible powers could emerge

Our research revealed this recent exchange on Twitter. It is both illuminating and representative of the debate and bitcoin's implicit need for stewardship.

Ryan X. Charles, a software engineer formerly at BitGo, called out the Bitcoin Core developers for "their antisocial culture. Yes, they are good security engineers. No, that doesn't make trolling OK."⁴⁰ He was referring to alleged trolling to promote the adoption of SegWit.⁴¹

Jameson Lopp, software engineer at BitGo, sought clarification: "Seems like you're trying to blame the actions of a few on a larger group. I'm a minor contributor; are you saying I'm responsible?"⁴²

Charles: "I'm sure many or most Core devs are genuine, but a handful of toxic influential devs encourage me to look elsewhere for protocol leadership."⁴³ There it was – the absence of leadership in the bitcoin community.

Lopp: "I agree, though I don't think calling out 'Core' makes much sense – calling out individuals makes more sense."⁴⁴

Charles: "I will do so when the time is right. It makes sense to call out Core for bad culture in the same way as calling out Uber."⁴⁵

"Does it?" tweeted Zooko Wilcox-O'Hearn, Founder of z.cash. "Companies have a structure specifically designed for accountability. If there's a problem, it's the CEO's fault by definition."⁴⁶ He added, "In contrast 'Bitcoin Core' is a fuzzily-defined set and nobody says 'the buck stops here.'"⁴⁷ It was an excellent question: Could we really compare the words and actions of a few members of a large, open, decentralized and liable-free network with the culture of a corporation like Uber accountable for its operations in the world?

John Light, Co-Founder of Bitseed.org, chimed in, "The closest we have to that in Core is Lead Maintainer @orionwl [Wladimir J. van der Laan]. Maybe Core should have Lead Community Maintainer(s) too :)"⁴⁸ We read that as another suggestion for leadership.

"There is not one bitcoin community, nor even one bitcoin core community. Things have grown past that a long time ago," said van der Laan, the aforementioned "lead maintainer" of the Bitcoin Core protocol and a member of the MIT Digital Currency Initiative.⁴⁹ He followed up with, "Some rely on heavy moderation, some on self-regulation, and that's exactly how it should be. I don't get this call for central control."⁵⁰ In other words, to each his own, as long as it's not centralized.

Then Charles made a critical distinction: "Leadership and control are not the same thing."⁵¹

Wilcox-O'Hearn suggested a representative body with some responsibilities: "It would be *possible* to set up a system in which 'Bitcoin Core' has publicly verifiable membership and spokespeople. But you don't want. ?[sic]"⁵²

Matthew Corallo, a developer at ChainCode, asked, "But, really, do you *want* Core folks to be tied to a hierarchy like BU [Bitcoin Unlimited], instead of speaking for themselves?"⁵³ So Bitcoin Unlimited was perceived as a hierarchy.

"Let's separate out whether it is possible to have such controls and whether it is desirable. I think people are shifting between the two," Wilcox-O'Hearn suggested. "I assert that it is possible, and I argue that it might be better in at least some ways."⁵⁴ So some type of stewardship could be positive for the platform.

Corallo disagreed on both counts: "It is neither possible nor preferable." He explained, "Not possible in part because of the group contributing now – we'd all fork and go create a competitor that had no strict hierarchy again" and "Not preferable as it results in a system with little advantages over other systems."⁵⁵

In the gauntlet-throwing tone typical of these threads, Daniel Robert Plante raised another issue, and it's a big one: "Then do it Matt. Fork. No permission. It's what Satoshi would do/did. But do you believe you have a grasp on the needs of the future?"⁵⁶ He nailed it. If someone didn't agree on a way forward as the future emerged, then he or she was more than welcome to fork and create a new chain.

To us, this Twitter exchange reveals the lack of a shared view of what the community will require of its technology and a desire for leadership that can rise above the individual camps and seek common ground and a unifying vision. Nature abhors a vacuum. In this absence of explicit governance, we may be witnessing the emergence of what Primavera De Filippi called "informal and invisible power dynamics".⁵⁷

Governance challenge: How to maintain incentives for mass collaboration

We found that miners do have an incentive to maintain the bitcoin infrastructure because, if the network fails, all the unconverted bitcoin they'd earned (or could earn) through mining would be lost, worthless or at risk. Before we dig into incentives, let's be clear about the service that miners provide: it is *not* transaction validation. Every full node can validate transactions. Rather, miners preserve the distribution of power – the power to decide which transactions to include in each block, the power to mint coins, the power to vote on the truth.

Any design change to the original bitcoin protocol, whether through an altcoin or an upgrade, must keep in mind appropriate economic incentives to sustain hardcore miner decentralization, so the network gets good value from miners in exchange for the large sums of bitcoin. To Bitcoin Core developer Peter Todd, that means that smaller miners in geographically dispersed locations should be able to compete nose to nose with larger miners that are geographically centralized, that is, large mining pools in Iceland or China.⁵⁸

Is that possible? As the number of new bitcoins minted halves every four years, what will happen when the reward drops to zero? The mining cycle depends on the market price of bitcoin. When the price drops, some bitcoin miners park their supply, but they continue to play the lottery until the price increases. Other miners can't afford to park and play; they just dry-dock their mining rigs or divert their processing power to another altchain that might be more profitable. Still others join mining pools, pooling their computing power with nodes with the hope of increasing their odds and at least getting some fraction of the winnings rather than nothing at all.

One answer is fees. Satoshi wrote, "There will be transaction fees, so [mining] nodes will have an incentive to receive and include all the transactions they can. Nodes will eventually be compensated by transaction fees alone when

the total coins created hit the pre-determined ceiling."⁵⁹ So once all bitcoins have been minted, a fee structure could emerge if the core developers agree on one. The Bitcoin Unlimited upgrade would give miners power to set transaction fees now. Because each block has a fixed maximum size, there is a limit to how many transactions a miner can include. Therefore, miners will add transactions with the highest fees first, leaving those with low or zero fees to fight for whatever space might be left over. If a transaction fee is high enough, a miner will likely include it in the next block; but if a fee is too low and the network is busy, it might take two, three or more blocks before a miner eventually records it in the blockchain.

What do fees mean for people who can't afford fees today? Won't levying fees lower the blockchain's advantage over traditional payment methods? According to venture capitalist Pascal Bouvier, the "fees reflect the marginal cost of verifying a transaction". Without fees to incentivize miners, as the block reward keeps halving, the hash rate would likely drop. If hash rate drops, network security declines.⁶⁰

That leads us to the 51% attack, where a huge mining pool or a cartel of large mining pools controls 51% of the hash rate. With that much firepower, they would constitute a majority vote of miners and could hijack block generation and thrust their version of the truth on the bitcoin network. They wouldn't necessarily get rich. Far from it. All they could do is to reverse their own transactions within a previous block, rather like a credit-card chargeback. Let's say the attackers bought some big-ticket item from the same merchant, waited until it shipped, then attacked the network to get their money back. That wouldn't mean tacking its own block to the end of the blockchain. That would mean going back and redoing the block that contained all their purchases as well as all subsequent blocks, even as the network continues to generate new blocks. When the cartel's branch became longer, it would become the new valid one. Satoshi bet on that being wildly more costly than mining new coins.

"Trying to bootstrap or change a network protocol [such as IPv6] is just a monumental task," said Austin Hill, a blockchain entrepreneur. "You just don't want to be making changes ad hoc or very fast on an ecosystem that's managing anywhere from 3 to 10 billion dollars' worth of people's wealth and assets."⁶¹ At the end of the day, said Andresen, "That governance model is driven very much by what code the people actually want to run, what standards people want to implement in the equipment they sell." He said that bitcoin, like the internet, will "have a similar messy, chaotic governance process that will eventually come down to what codes the people choose to run."⁶² That worked well for the internet of information, which had decades to evolve before commercial adoption, but it could prove risky for assets on the internet of value, which companies have already adopted and deployed in commercial ventures.

Governance challenge: The energy consumed is unsustainable

Our research findings are unequivocal; the proof-of-work method has been critical to building people's trust in these primordial days of the bitcoin blockchain. Years from now, we will look back and appreciate the genius of its deployment, from minting and allocating new bitcoins to assigning identity and preventing double spending. Pretty remarkable. And pretty unsustainable, according to critics of cryptocurrencies that use proof of work to keep the network safe and pseudonymous.

Hashing, the process of running pending transactions through the secure hash algorithm 256 (SHA-256) to validate them and solve a block, burns a lot of electricity. Some people in the blockchain ecosystem are making back-of-the-envelope calculations that become memes in the community. Estimates liken the bitcoin network's energy consumption to the power used by nearly 700 average American homes at the low end of the spectrum and to the energy consumed by the island of Cyprus at the high end.⁶³ That's more than 4.409 billion kilowatt-hours,⁶⁴ a Godzilla-sized carbon footprint, and it's by design. It's what secures the network and keeps nodes honest.

In early 2015, *The New Republic* reported that the combined processing power of the bitcoin network was hundreds of times greater than the aggregate output of the world's top 500 supercomputers. "Processing and protecting the more than \$3 billion worth of bitcoins in circulation requires more than \$100 million in electricity each year, generating a volume of carbon emissions to match." The article's author, Nathan Schneider, wrote what has been on our minds ever since: "All that computing power, which could be curing cancer or exploring the stars, is locked up in machines that do nothing but process bitcoin-type transactions."⁶⁵ As citizens who care about our planet, we should all be concerned.

The more people adopt bitcoin, the more energy is consumed. There are two issues, one around the electricity used to run the machines and another around the energy used to cool them so they don't fail. Here's a rule of thumb: for every dollar a computer burns up in electricity, it needs 50 cents to cool down.⁶⁶ The acute drought in California has raised serious concerns over using precious water to cool data centres and bitcoin mining operations.

As the value of bitcoin increases, the competition for mining new bitcoin increases. As more computing power is directed at mining, the computational problem that miners need to solve becomes more difficult. One measure of the total processing power of the bitcoin network is the *hash rate*. When we were writing our book in 2015, Gavin Andresen told us, "Let's say we have millions of transactions per block, each paying an average of a dollar transaction fee. Miners would be paid millions of dollars per block, and they would spend a little less than that in

electricity to do that work. That's how the proof-of-work economics work out. It really is the price of bitcoin and however much reward is in a block that drives how much hashing is done."⁶⁷

The hash rate has been increasing considerably over the last two years, rising from 1.5 exahashes per second in mid-2016 to 4.2 exahashes in May 2017. That's more processing power than the most powerful supercomputers on the planet.⁶⁸ And the trend is towards using more energy, not less. "If bitcoin really does become a global team network, I think we will need to slowly move away from proof of work as the only way it's secure," said former core dev Andresen. "In the very long run, maybe we will move away from proof of work as the way the network is secured, and we'll combine it with something else."⁶⁹

"The cost for having no central authority is the cost of that energy," said Eric Jennings, Chief Executive Officer of Filament, an industrial wireless sensor network.⁷⁰ That's one side of the argument. *The energy is what it is*, and it's comparable to the cost incurred in securing fiat currency. Think of the big vaults, the bunkerlike architecture with majestic Grecian facades, with heating, ventilation and air conditioning systems pushing air into bright lobbies, competing branches on every corner, and ATMs in between.

Now let's consider computer architecture itself. The Bitfury Group has built a massively parallel bitcoin problem-solver with application specific integrated circuits that are energy efficient and designed solely to mine bitcoins. Its Founder and Chief Executive Officer, Valery Vavilov, argued that machines and mining operations overall will continue to become more energy efficient and environmentally friendly. Some of that depends on relocating to cold climates where energy is cheap and preferably renewable, such as hydro or geothermal, and where either Mother Nature handles the cooling or manufacturers figure out an efficient way to capture the heat. Bitfury, for example, has two data centres – one in Iceland and another in the country of Georgia – with plans for additional centres in North America, and it acquired the Hong Kong-based start-up Allied Control, which specializes in immersion cooling technology.⁷¹ And so Bitfury is working to reduce the ecological impact of the bitcoin infrastructure.

Even if these initiatives limit mining's carbon footprint, we still have the rapid consumption and disposal of these continually upgraded devices. Miners who want to make a career of it must continually upgrade and specialize their systems. Most mining equipment has a useful life span of three to six months.⁷² Vendors such as MRI of Australia are applying new approaches to recycling, first disassembling rather than shredding all these computing components, and then managing resulting waste streams. Such creative processes are enabling them to reclaim precious metals and reuse up to 98% of product by weight.⁷³ Unfortunately, hardware recycling is still not widely available to most consumers of computing and communicating technology.

Ethereum

In our research for *Blockchain Revolution in 2015, when everyone was talking about the bitcoin phenomenon, we spent time learning about Ethereum and projects in that ecosystem.*⁷⁴ It turned out to be time well spent. Ethereum is emerging as one of the most important blockchain platforms today. Ethereum started as an open-source software platform for decentralized applications, where stakeholders needed Ether the token to pay for computational steps and storage operations on the platform, said Joseph Lubin, Co-Founder of the Ethereum Project. “We earned revenue, \$18 million, by selling a token. Before running the sale, we needed a legal structure that would (a) protect those funds; and (b) be the legal entity that could shepherd the platform potentially for a long time. We did discuss and commit to decentralized governance once we built sufficiently capable tools.”⁷⁵

The Ethereum Foundation, a non-profit consisting of 40 or so developers and researchers, was part of the plan. According to Co-Founder Vitalik Buterin, the Foundation’s core tasks include (a) research on the next version of Ethereum protocol and standards; (b) co-development and maintenance of the six different clients such as C++ and Go; and (c) community outreach to both newcomers and existing community members, publishing transcript of core developer calls, promoting developer events and keeping channels of communications open.

For example, if a company wanted to issue its own asset on top of Ethereum, it would write a piece of code that basically implements a bank so that the company could conduct transactions that decrease its own balance and increase other people’s balances.⁷⁶ There are an infinite number of ways to do that, most of which are not compatible with each other. Some blockchains like Mastercoin and XC have a transaction type for issuing and transferring assets specific to their platforms.

Ethereum is a general-purpose code platform. So its developers wanted the most common way to be some compatible standard. Someone from the Ethereum community proposed such a token standard as a document on GitHub two years ago. The Foundation helped to standardize it and then put it to the community for rigorous review. The ERC-20 standard resulted from this collaborative effort. It’s by and for Ethereum people, so that other Ethereum people can better interact with each other.⁷⁷

Another kind of standard enables the Ethereum ecosystem to interact with outside ecosystems and support outside standards. For example, the Foundation is considering integrating a set of optimized operations into the Ethereum virtual machine so that it can more easily process RSA cryptography, a fairly popular kind of cryptography used in other mainstream applications and named after Ron Rivest, Adi Shamir and Leonard Adleman who created the first practical public-key system for communications.

The Enterprise Ethereum Alliance (EEA) was founded to gather requirements for deployment of Ethereum within enterprise blockchains and to establish technical specifications and standards to add these capabilities to Ethereum, via the Enterprise Improvement Process (EIP). With over 100 organizations participating, the EEA objectives are to understand industry requirements, leverage current standards and develop new open-source standards alongside the Ethereum Foundation’s platform-level work, all to provide roadmaps for the deployment of enterprise and industry-wide applications on the blockchain. EEA is an inclusive organization, with a rotating board comprised of giants like Microsoft (represented by senior blockchain executive Marley Gray) and start-ups like Nuco (represented by Chief Executive Officer Matthew Spoke). EEA is implementing a multi-tiered governance structure to meet the needs of large enterprises while maintaining open-source, rapid collaborative-development. This includes leveraging current decentralized governance tools, as well as the potential to experiment with blockchain-based governance tools such as Boardroom.

Governance challenge: How to address major threats by consensus

Ethereum’s governance mechanisms faced a big test early on. In May 2016, a new breed of organization called the DAO, for decentralized autonomous organization, crowdfunded a record-breaking \$160 million from tens of thousands of global investors. What distinguished the DAO from all other start-ups was the absence of management. The DAO was a blockchain application, a collection of smart contracts that ran on the Ethereum blockchain. Its stakeholders – human beings – could review and vote on proposals for how the DAO allocated its funds.

The DAO allowed token holders to withdraw their Ether from the DAO through a “split function”. This function allowed users to revert the process and get back the Ether they sent to the DAO. In June 2016, a hacker exploited the function by asking the DAO to return Ether multiple times (a “recursive call”) before the DAO could update its own balance. The hacker succeeded in draining around \$70 million of Ether from the DAO into a separate DAO where, per the terms of the smart contract, it would have to sit for 28 days before the hacker could send it to another account.

That gave the Ethereum community several weeks to decide what to do, if anything. Members began circulating proposals. One proposed a soft fork designed to blackball any transaction from the DAO, but a few members discovered a bug that would have opened the DAO up to a denial-of-service attack.⁷⁸

Another proposed a hard fork in the codebase designed to claw back all the Ether hacked from the DAO through the recursive call exploit and to implement a new contract with only a “withdraw” function. DAO token holders could request a refund of one Ether for every 100 DAO tokens.

Those who had paid more than one Ether for 100 tokens could request a refund of the difference.

“Virtually everybody agrees that you shouldn’t fix an application-layer problem with a protocol-level solution,” said Joe Lubin. “Initially, most of the core Ethereum people did not want to have a fork, did not want to bail out ... the promoters, developers and investors. ... They should have taken the serious losses as an appropriate teaching signal.”⁷⁹ But it was an existential threat. “If the hacker’s goal was to destroy Ethereum, then the hacker could have staged denial-of-service attacks for many years, messing up the network’s ability to process transactions efficiently. We would have been chasing this person in and out of different smart contracts, in a sort of a cat and mouse game,” Lubin said.⁸⁰

Don’t fix an app-layer problem with a protocol-level solution.

Lubin identified six different classes of stakeholders – developers, exchanges, miners, mining pools, token holders and other community members – who weighed in, in the very vigorous debate over whether to fork. Those who argued for the hard fork sought to prevent the hacker from taking control of a very sizable portion of all the Ether in circulation. Those who argued against sought to prevent what they considered censorship of the Ethereum blockchain. Some viewed the code as the law: the terms of the DAO contract, however flawed, should stand, and those who invested should suffer for the greater good of Ethereum’s reputation as an immutable chain.

The six stakeholder groups voted overwhelmingly (89%) in favour of the hard fork. Users of the Ethereum platform then had to decide for themselves whether to use the forked version or continue on the non-forked version, now known as Ethereum Classic. “The Foundation itself, which is a legally conservative, risk-averse entity, did not take a position early on.” Instead, it gathered information. After the vote, it acknowledged Ethereum Classic’s right to exist. “I don’t think the verdict is in on whether it was good governance, but it was quite decentralized governance, and I continue to applaud Vitalik for the studied approach he takes to decision-making and the care he takes in not issuing rash communications,” said Lubin.⁸¹ He continued:

These systems are complex and subtle and they’re protecting important and valuable assets in cryptography that we need a few hundred or so global experts to take a good look at them and try to beat the **** out of them for three or five years, then we’ll have some well-vetted frameworks that we can all share that handle certain foundational functions like escrowing money, enabling deposits and withdrawals, issuing new token allocations, etc. Layers of increasingly sophisticated functionality will have to be built and the deeper layers will need to be very well vetted so that they don’t need to change much because many will build on them.⁸²

Ethereum is by no means alone in anticipating and responding quickly to worst-case scenarios. Other core developers and blockchain companies have moved quickly to secure their networks. For example, in 2014, thieves stole 8 million VeriCoins, a proof-of-stake cryptocurrency, from the MintPal exchange. Within days of the attack, VeriCoin developers released new code that forked the VeriCoin blockchain prior to the hack – like Ethereum, they rolled back time – and collaborated with exchanges to make sure it was adopted.⁸³

What they could do differs from what they have, as a group, committed to do in the interest of preserving the resource, and that is to engage the community in reaching consensus on key issues. That’s stewardship.

Governance challenge: Managing the switch to proof-of-stake

The first version of the Ethereum blockchain – Frontier – also uses proof of work. For Vitalik Buterin, the concern about energy consumption is legitimate and worth solving. That’s what other chains have done: explored alternative consensus algorithms for securing the network while retaining decentralization. The open-source nature of the bitcoin protocol makes it technically easy to do. Remember, the purpose of consensus algorithms is to distribute the authority to decide on the state of the blockchain to a decentralized set of users. To the mind of Buterin, there are only three securely decentralized sets of users, and each set corresponds to a set of consensus algorithms: owners of computing power, with standard proof-of-work algorithms; stakeholders, with various proof-of-stake algorithms in wallet software; and members of a social network, with a “federated style” consensus algorithm.⁸⁴ Note that only one of those consensus mechanisms includes the word power.

The developers of Ethereum expect to replace Frontier with Caspar, a proof-of-stake mechanism. Proof-of-stake requires miners to invest in and hang on to some store of value (i.e. the native token of the blockchain such as Ether) in order to vote on the state of the chain. They are no longer miners; they are validators. They needn’t spend energy to vote. If they break the rules, they may lose their holdings. The plan is to phase in the proof-of-stake. According to CoinDesk’s Alyssa Hertig, “Since [Casper] has been pushed back several times, detractors see this hybrid as the latest evidence that proof-of-stake won’t ever be fully implemented successfully on Ethereum.” Thoughtful discussions have sprung up on Reddit, such as “Fundamental problems with Casper” and “Vlad Zamfir said it’s a reasonable possibility Casper won’t be implemented on Ethereum... is this cause for concern?”⁸⁵ The latter referred to a couple of tweets by Vlad Zamfir who, according to Ethereum’s blog, has worked on proof-of-stake blockchain architecture since September 2014.⁸⁶

Zamfir tweeted, “I sold most of my ether at least [four] times... incl[uding] before this rally really started (\$16) ... lol :(But I absolutely will walk if I stop having sufficient hope that the Ethereum community will adopt Casper-style PoS and sharding. Which I think is a serious possibility, given how much money we are giving Ethereum miners.”⁸⁷

Buterin tweeted to Zamfir, “You think our large PoW rewards make it more likely Casper will stall? That is so interesting; I completely disagree.”⁸⁸

Zamfir replied, “Interesting! I think the more money miners have the more incentive they have to participate in governance. Where their incentive is to block.”⁸⁹

Others shared that view: “You’re never going PoS. You’ll personally be forked before that happens, maybe literally by angry miners.”⁹⁰

Of these alternatives to proof of work, veteran cryptographer Austin Hill cautioned against using other methods for securing consensus. “Experimentation with your proof-of-work algorithm is dangerous, and it’s a new area of computer science.”⁹¹ It adds a dimension to innovation: not only must developers worry about whether their new features and functions will work in their own right, but they must also check how the choice of consensus algorithm keeps them secure and distributed to the most appropriate economic set.

Where 51% of attacks on proof-of-work models stem from concentrated mining power, attacks on proof-of-stake models come from concentrated coin control, and coin exchanges are typically the biggest stakeholders. In some jurisdictions, exchanges must be licensed and are under regulatory scrutiny. They also have reputation at stake, and so they have multiple incentives to protect the value of their brand and the value of the coins held in account wallets. However, with more coins in circulation, a greater diversity of value and more strategic assets registered on PoW and PoS blockchains, an attacker might not care about any of these costs.

Finally, there is the considerable task of bringing along a super-majority of Ethereum stakeholders to the proof-of-stake model, since it may run atop the Ethereum platform like a smart contract reminiscent of the DAO. Unlike bitcoin whose visionary Satoshi Nakamoto has receded from the debate and left others to interpret his vision, Ethereum’s creator, Buterin, is very present, very communicative and working tirelessly on both the technical and the theoretical aspects of the platform. He is enormously influential and inspiring, not just because of his brilliance but because of his basic decency, his concern for human rights and the health of the planet. He may not be the ultimate arbitrator as Linus Torvalds is over Linux, but Buterin certainly stewards the Ethereum ecosystem.

Tendermint

Tendermint is what Co-Founder and Chief Technology Officer Ethan Buchman called “general purpose blockchain middleware”, that is, software that operates between blockchain protocols and blockchain applications, so that developers can create applications in their programming language of choice for their environment of choice.⁹²

According to Buchman, Tendermint met “the highest standards of security”, meaning that it worked even if a third of the nodes in a network arbitrarily failed.⁹³ Large distributed peer-to-peer networks, where parties could have wildly different types of machines under wildly different circumstances, need such a high level of fault tolerance, including attacks on machines that turned them into malicious nodes. He referred to this ability to tolerate arbitrary failure as “Byzantine fault tolerance”, a theory put into practice in distributed ledgers such as bitcoin and Ethereum.

Tendermint has two components: its proof-of-stake consensus mechanism ensures that every faultless machine records the same transactions in the same order. Its application interface enables machines to process transactions in any programming language. It emerged, as many alternatives to bitcoin did, as a proof-of-work blockchain with a native token, the Atom, which users bonded in a security deposit (which they could lose if they misbehaved) to participate in consensus. Tendermint has developed into “a general purpose blockchain consensus engine that can host arbitrary application states. That means it can be used as a plug-and-play replacement for the consensus engines of other blockchain software.”⁹⁴

In September 2016, Tendermint won an innovation award and a 20,000 renminbi prize at the International Blockchain Week Demo Day in Shanghai, where it announced plans for a new Cosmos Network.⁹⁵ Buchman described Cosmos as “the Internet of Blockchains ... designed to solve many of the outstanding problems in the cryptocurrency community, including scalability, interoperability, security and flexibility.”⁹⁶ To fund its development and launch, Cosmos, the entity building out the Tendermint protocol, held an initial coin offering of Atoms in April 2017 and raised \$16.8 million in 28 minutes.⁹⁷ Cosmos coalesced around what Buchman called “a crisis of legitimacy of our institutions and a crisis of value of our mediums of exchange”, as a means of developing currencies that supported community values and keeping organizations transparent and accountable. Its website refers to Cosmos as “a heterogeneous network of proof-of-stake blockchains that can interoperate with one-another”.

“There are lots of discussions about interoperability,” said David Treat, Managing Director of Accenture’s Capital Markets Blockchain practice, “but with limited progress to date as the primary platforms and codebase creators are still focused on achieving their first production versions and building market share. Given current progress on the first wave of production systems, making progress on interoperability is growing in urgency.”⁹⁸

Hyperledger

Hyperledger is an open-source collaborative effort launched to advance blockchain technologies across such industries as banking, IoT, manufacturing and supply chains. The effort, hosted by the Linux Foundation, is focusing on distributed ledgers and smart contracts separate from cryptocurrencies, for scenarios where participants in a network want to share a record-keeping system and to automate additional transactions on top of that shared ledger.

Its Chief Executive Officer, Brian Behlendorf, sees distributed ledger technology as an operating system for decentralized market places and digital communities, “foundational in the same way that the Linux operating system is foundational in the cloud, the same way that internet protocols are foundational”.⁹⁹ Developers could build a cryptocurrency or a system for tracking other digital assets on top of it.

According to Behlendorf, “We don’t believe in one big chain to rule them all; we believe in adapting the governance models that exist today and facilitating them using this technology.”¹⁰⁰

As a project of the Linux Foundation, Hyperledger’s charter borrows from the Linux governance framework. Its mission is clear, to create “an enterprise grade, open-source distributed ledger framework and codebase” and “an open-source, technical community”, and to “promote participation of leading members of the ecosystem” and “host the infrastructure for [the project], establishing a neutral home for community infrastructure, meetings, events and collaborative discussions and providing structure around the business and technical governance.”¹⁰¹ The charter provides for a governing board, its composition, conduct and responsibilities. Like the Internet Engineering Task Force, it provides for a technical steering committee and a process for reaching consensus, and voting if necessary, on changes to the codebase. It also provides for a marketing committee and an end user technical advisory board for industry outreach and education. Finally, it sets forth codes of conduct, including transparency so as to preclude the formation of trusts.

Its membership already exceeds 130 different organizations, from IBM and Intel to J.P. Morgan and Wells Fargo. Casey Kuhlman, Chief Executive Officer of Monax Industries, explained why his start-up joined Hyperledger: “[T]o get our software into production in enterprises, we need not only to prove the technology itself, but also to develop the mechanisms to build and deliver that software collaboratively.” Kuhlman observed quite astutely, “The old one-to-one approach dominated by account managers walking the halls of incumbent enterprises pitching the IT company’s ‘new’ thing may still work for a lot of technology, but it isn’t likely to work for blockchains and smart contracts.”¹⁰² It was an astute observation: to cross that chasm of obscurity between the fanatic early adopters and the more pragmatic early majority of adopters, we need to collaborate. Collaboration is the glue that will make this technology stick.

Governance challenge: The need for industry standards as soon as possible

In our research, the development of industry standards emerged as a big issue. Behlendorf sees two major challenges. “In any one marketplace or ecosystem, we want everyone using the same code, the same chain and the same kinds of transactions to get the efficiency,” he said. That means engaging industry associations specific to each industry and educating them on the trade-offs between (a) sharing enough data in the chain to reassure everybody of the integrity of, for example, the provenance tracking process; and (2) providing enough confidentiality to participants that competitors cannot figure out each other’s businesses or deduce terms of agreement with other members of the market or ecosystem.

Designing these systems to be both confidential and auditable is a very big challenge – not just a technology challenge, but a business challenge. How much data will companies share to make the whole effort meaningful? Behlendorf did not know. “We might have some proof of concepts, we might have people playing on the perimeter, between one or two partners in an ecosystem, but we really want to get the whole of the industry to adopt a common standard and give an industry the time to convert,” he said.¹⁰³

Jesse McWaters of the World Economic Forum agreed on the magnitude of this challenge. He used the creation of a know-your-customer (KYC) utility for financial institutions as an example:

There is an enormous appetite in the financial services community for a KYC utility, and blockchain is one way that such a utility could be operationalized. However, before this can happen, institutions need to agree on standards and practices for the exchange of KYC data. Reaching that agreement among enough institutions to start building a network effect is the hard part and blockchain doesn’t actually do anything to fix that problem for us.¹⁰⁴

Industries also differ in their need for speed. For the bitcoin blockchain network, the process of clearing and settling transactions takes about 10 minutes, which is far faster end to end than most payment mechanisms today. But clearing transactions at the point of sale instantaneously is not the issue; the real problem is that 10 minutes is simply too long for the IoT where devices need to interact continuously. Former core developer Gavin Andresen said solving for a trillion connected objects is “a different design space from bitcoin”, a space where low latency is more critical and fraud is less of an issue or where parties could establish an acceptable level of trust without the bitcoin network.

Ten minutes is also too long for financial transactions where timing matters to get an asset at a particular price, and where latency exposes traders to time-based arbitrage weaknesses such as market timing attacks.¹⁰⁵ The immediate solution for entrepreneurs has been to fork the bitcoin codebase, that is, to modify the source code by tweaking a few parameters, and to launch a new blockchain with an altcoin in place of bitcoin as incentive to participate. Litecoin is a popular altcoin with a block time of 2.5 minutes, and Ripple and Ethereum are entirely re-engineered blockchain platforms that have latency of seconds, not minutes. So does each industry need its own blockchain?

Governance challenge: Premature anointment of any protocol as an industry standard

Our research surfaced the downside of arriving quickly at industry standards. “The space is still so young that the desire for standards, while well-placed, runs the risk of hardening projects that have really just come out of the lab,” said Behlendorf, which he sees as the second big challenge: preventing widespread adoption of an inferior technology. “People were in such a rush to take credit-card orders over the internet that they would use anything we came up with.” The result was the suboptimal internet security paradigm still in use. Behlendorf still feels bad about the cookie header, intended as short-term memory for storing items in a virtual shopping cart but deployed as “a tracking device that has turned the web into a giant surveillance machine”. People have all but written off the possibility of anonymity on the internet.

“Anybody running systems in this space needs to anticipate a period of five or 10 years of fairly rapid progress in the underlying technologies,” Behlendorf said. “Right now we should be in a ‘let a thousand flowers bloom’ mode, and let these technologies find their footing.” The ones that fail will become obvious. The ones that succeed will have a choice, either to remain independent or to merge with somebody else. Sorting the winners from the losers requires more than “white papers, essays and academic research”, he said. It requires “people going out and exercising the different stacks, seeing what they’re good for, fixing bugs and adding features”. That means deployment, real production experience.

Here’s where knowledge, advocacy and stewardship of standards processes are critical: “We need to avoid making serious architectural decisions that first become legacy and then become hindrances. That means conducting experiments and then throwing away the failures as quickly as we can. And it’s harder to throw away failures once they’ve become industry standards,” Behlendorf said.¹⁰⁶

“I think it’s okay at this point to have a number of different consensus systems out there competing. But you don’t want protocols competing for very long, because then you can’t build anything,” said Joichi Ito. “I have a feeling, though, that we may be still a few years out before we settle on what we think the wireline layer is going to be. If you look at the layers of the internet now, it wasn’t predetermined exactly how the layers were going to be cut, right?” IBM’s Token Ring “was sort of layer two and layer three together. It wasn’t obvious where the layers would be cut”. Similarly, with blockchain technology, “Where does the accounting live? What should the accounting do?”¹⁰⁷

According to Behlendorf, “This stuff is ready to leave the lab as the web was in 1993 or 1994. Let’s just make sure we don’t encumber it with too much legacy and too much commitment.”¹⁰⁸

Governance challenge: The lack of robust infrastructure

To paraphrase science fiction author William Gibson, the future is here; its *infrastructure is just unevenly distributed*. For example, had Greek citizens known about bitcoin during their country’s economic crash in 2015, they still would’ve been hard-pressed to locate a bitcoin exchange or a bitcoin ATM anywhere in Athens. They wouldn’t have been able to transfer their drachmas into bitcoins to hedge against the plummeting fiat currency. Computer scientist Nick Szabo and information security expert Andreas Antonopoulos both argued that robust infrastructure matters and can’t be bootstrapped during catastrophes. Greece’s blockchain infrastructure was lacking at the time of the crisis, and there was insufficient bitcoin liquidity for an entire population to move its troubled fiat currency into it.

The blockchain also falls short on security controls for such a massive bump in usage. It lacks the *transactional capacity* to onboard millions and millions of people. Such an immature technology would be susceptible to capacity problems, system failures, unanticipated bugs and, perhaps most damaging, the huge disappointment of technically unsophisticated users, none of which it needs at the moment.

Governance Challenge: The lack of constructive discourse

“The current challenges do not really reside in any specific technical component,” said Roszak of Bloq and the Chamber of Digital Commerce. “The issues reside in the human factor of communication and finding a way of building consensus during the early days of this \$6.5 billion railway. The debates, fights and passions involved are in many ways a feature and not a bug of the network.”¹⁰⁹

Debate is a feature, not a bug.

“If I were to criticize the blockchain technical community, it’s not very respectful,” said Pindar Wong. “There’s a lot of bravado, a lot of posturing, as you would expect, and it doesn’t even involve tech.” He mentioned the practice of shouting down people in public. When we asked whether that happened frequently, he said, “Go online; ALL CAPS, all of the time.” So we did and found many a heated thread related to bitcoin block size. So nasty have the exchanges become that Andreas Antonopoulos, technologist, serial entrepreneur and author of *Mastering Bitcoin*, recently tweeted, “I wish people wouldn’t put me in mentions when bashing @rogerkver. I am never ok with personal attacks or abuse. Stop it.”¹¹⁰ A person with the Twitter handle @veryevilone replied, “Roger has been happy to attack other people and insult their intelligence. He is not interesting and he doesn’t [sic] deserve respect”¹¹¹ to which Antonopoulos responded, “Lack of respect is a measure of the speaker, not a reflection of the subject. I will block accordingly.”¹¹² He wanted no part in hostilities and would block those who did.

“The rough-and-tumble should not exclude people who want to contribute,” said Wong. That’s an important point. The nature of the discourse may put off otherwise really talented developers. Some might say, “Stay out of the kitchen if you can’t stand the heat.” Others might say that it’s a hostile tactic for defending one’s position. When it comes to solving big and important problems, hostility is a failed strategy. Deep thinkers like Antonopoulos opt out. Wong added, “At the very risk of being facetious, I would say we all need training in active listening. ... We’re hearing what we’re expecting to hear, not necessarily what the person is meaning to say.” Meeting people in person helps to understand what they mean online. “If anything, one of the big rewards as a volunteer in scaling is to see people meet each other and come out with, ‘You’re an asshole, I’m an asshole, but we can now be assholes together. Maybe we agree on something now.’ That’s humanity at work, and I think that’s wonderful.”¹¹³

2. Stewardship of applications

“Traditionally, centralized organizations were responsible for the ‘coordination’ and ‘governance’ of online applications,” said Primavera De Filippi. “Today, with blockchain technologies, we are witnessing the emergence of global networks or organizations, which operate in a distributed manner without any centralized middleman” to mediate the rollout of new tools that sound great.¹¹⁴ Our research bears this out. To understand what we mean by blockchain applications, consider this analogy: email is to the internet what cryptocurrencies are to the blockchain – the first application – and just as postal mail (now “snail mail”) was to email, digital currency is an application with a physical world antecedent – fiat coins and bills (soon to be “slow dough” or “anonymoney”) – that helps all stakeholders to wrap their heads around it. But compelling analogies can lead to faulty thinking, induce a false sense of security or limit the imagination altogether, as the “page” metaphor for web screens did by anchoring minds to a print medium (e.g. “landing page”, “page views”, “retail catalogue”) and then using the web primarily as a publishing platform and somewhat belatedly as a town hall, a crowdfunding event, a collaborative workshop, a multiplayer arena or a worldwide genomic laboratory. Of the asset classes on blockchain platforms (see Table 2), the rising popularity of the initial coin offering (ICO) is a case in point.

Table 2: Top 10 Digital Assets, as of 17 June 2017

Rank	Name	Platform	US\$ Market Cap	US\$ Price	Circulating Supply
1	Golem	Ethereum	493,919,905	0.595621	829,252,000.00
2	Augur	Ethereum	336,539,500	30.59	11,000,000.00
3	Gnosis	Ethereum	270,024,758	244.46	1,104,590.00
4	Basic Attention	Ethereum	220,787,000	0.220787	1,000,000,000.00
5	MaidSafeCoin	Omni	219,171,586	0.484301	452,552,412.00
6	Iconomi	Ethereum	209,038,380	2.4	87,000,000.00
7	Ardor	Nxt	199,448,251	0.199648	998,999,495.00
8	DigixDAO	Ethereum	185,485,200	92.74	2,000,000.00
9	Veritaseum	Ethereum	143,919,531	74.58	1,929,609.00
10	SingularDTV	Ethereum	129,022,800	0.215038	600,000,000.00

Source: CryptoAsset Market Capitalizations, <https://coinmarketcap.com/assets>, accessed 17 June 2017

As blockchain applications have evolved from potential to actual use cases, we can see that particular use cases will raise specific governance questions best answered at the level of each use case (e.g. payments, smart contracts, securities clearance, insurance, etc.). There will not be a single blockchain but many, some of which may serve specific industries or geographies. At the highest level, we need to focus on interoperability. Commercial blockchain applications are taking off, and governance will be critical to their success. For example, Ripple’s global payments steering group, a blockchain bankers network with defined rules and governance, has been a major step forward in terms of adoption and industry acceptance.¹¹⁵

Governance challenge: Oversight of applications whose off-chain equivalents are regulated

The ICO is an application whereby organizations of any size can raise money peer-to-peer by offering tokens or coins in a new venture, project or network. In 2016, blockchain organizations raised nearly \$200 million through ICOs. These aren’t just new cryptocurrencies masquerading as companies. They represent digital rights management platforms (SingularDTV), distributed venture funds (the DAO) and even new platforms for investing in ICOs (ICONOMI). The euphoria around them is palpable. “The token launch (some are calling certain forms of these ICOs), the first killer app for crowdfunding, is a powerful tool to enable the ecosystem to build itself out, with the issuance of protocol tokens,” said Lubin of Ethereum.¹¹⁶

They have been likened to the initial public offering (IPO), the process through which a privately held firm raises capital through public markets by issuing stock that investors can buy. Here’s where the analogy breaks down: IPOs are highly regulated affairs, involving a number of intermediaries, such as investment bankers, exchange operators, auditors, lawyers and crowdfunding platforms (such as Kick-starter and Indiegogo), whereas ICOs are not. IPOs are issuances of securities, mostly equities. With ICOs, the classification really depends on the purpose

of the coin. ICOs can be very equity-like, where tokens represent a fractional ownership in the underlying value of an organization, subject to profit or loss, and presumably – at a later date – entitlement to shares of profits.

However, often ICOs are not offering equity-like value at all. Augur did one of the first ICOs granting token owners the right to participate in its prediction markets. Others still are offering something more akin to access, for developers to build applications and for users to run them. Bilaji Srinivasan, partner at Andreessen Horowitz, likened them to a “paid API key”. He said, “When you buy an API key from Amazon Web Services for dollars, you can redeem that API key for time on Amazon’s cloud. The purchase of a token like Ether is similar, in that you can redeem ETH for compute time on the decentralized Ethereum computer network. This redemption value gives tokens inherent utility.”¹¹⁷

While the definitions are still evolving, the value is clear, which is why the New York-based venture capital firm Union Square Ventures (USV) broadened its investment strategy so that it could buy ICOs directly. Menlo Park-based venture capital firm Andreessen Horowitz joined USV in investing in Polychain Capital, a hedge fund that buys only tokens.

Blythe Masters, consummate Wall-Street-insider-turned-blockchain-pioneer, expressed her concern: “Newcomers are simply able to do things that regulated institutions are not able to do, but one needs to think very carefully about why those regulations exist, and what purpose they serve, before one can conclude that exposing consumers to unregulated financial activities is a good thing.”¹¹⁸

Lubin of Ethereum does not even call them financial instruments: “There are no investors. There are stakeholders who bought a software product called Ether that enables business and software developers to build on and use the decentralized application platform.”¹¹⁹

Stress-testing and debugging are left to the issuers, not to independent bodies with expertise in software auditing. There is potential for these new instruments to blow up in less-than-savvy investors' faces and give ICOs a bad name before they have a chance to do any good in the economy.

Patrick Murck, Special Counsel at Cooley and a fellow with Harvard University's Berkman Center, said that some of these tokens are securities and are already regulated under existing rules. Some are not and should not be regulated. Law enforcement didn't need new rules to catch criminals on the bitcoin blockchain. The US Securities and Exchange Commission (SEC) didn't need a new process for reviewing Tyler and Cameron Winklevoss' application to start a bitcoin exchange traded fund. The SEC posted the application, invited public commentary and issued its decision: No. It ruled that bitcoin markets were largely unregulated, and so such a fund would be unduly risky.

Should issuers of ICOs or funds pegged to cryptocurrencies let the buyer beware? Should regulators come in and write the rules? Or should key stakeholders come together and provide community guidelines and oversight?

Governance challenge: The lack of skilled developers

"At the application layer," said Perianne Boring, Founder and President of the Chamber of Digital Commerce, "business and technical skills to bring these projects to market are important."¹²⁰ Our findings were unambiguous on the need for skilled workers. The space needs talent, and talented people from anywhere in the world can contribute. Despite flair-ups on social media, many of the exchanges (on GitHub, for instance) among developers are educational, and those like Matthew Corallo of Chaincode Labs are known for encouraging new developers.¹²¹

Brian Behlendorf at Hyperledger would like to see "many more developers who are familiar enough with the technology and the concepts that they can move among different technologies".¹²² For example, if you know how to build mobile apps, you actually have a range of different technologies to do that. If you work at a place like Uber, you might know how to build an iPhone app and an Android app and bounce between them and make them look consistent. So being multilingual is not a unique challenge, but understanding what works in a mobile setting is the hard part.

He estimated that there are only between 1,000 and 2,000 developers who understand how to build blockchain applications, whether on Ethereum, Hyperledger or other platforms. He would like that number to increase substantially: "We are ready for the crowd to show up." A subset of those will build the infrastructure, "those second-tier developers, the ones who come in and jump into the black box, so to speak, and make it work better, faster, more feature-full". The space also needs people with production experience, and that's a function of time. The demand begs for creative education programmes, perhaps enabling young talented coders to earn their degree or other relevant professional certifications through their contributions to blockchain projects.

Governance challenge: The lack of user-friendly interfaces

Our research indicated that there's much work to be done in basic user interface and experience. Many of these apps are inaccessible to the average person. There's not enough wallet support, and many interfaces are user-unfriendly, requiring a high tolerance for alphanumeric code and geekspeak. Most bitcoin addresses are simply strings of between 26 and 35 characters beginning with a one or a three, quite tedious to type. As Tyler Winklevoss said, "When you go to Google.com, you don't type an IP address into your web browser. You type in a human-readable name, something that you can remember, that's mapped to its IP address. The same should be the case with bitcoin addresses. Actual bitcoin addresses shouldn't be exposed to the average user. Little things like that make a difference."¹²³

3. Stewardship of the ecosystem as a whole

“Because they lack a central point of control, these networks, applications and organizations require new distributed governance systems to coordinate on matters such as interoperability, privacy and security, in a collaborative manner,” Primavera De Filippi said. “We need to figure out new decentralized governance systems that can be easily deployed on top of these decentralized infrastructures.”¹²⁴

Decentralized governance systems for decentralized infrastructure

The ecosystem needs “a proper regulatory framework that understands and accommodates blockchain technologies”, De Filippi said.¹²⁵ Such a framework would mitigate some of the strong legal uncertainty surrounding these emergent technologies, thereby helping start-ups and larger companies alike to move beyond the proof-of-concept stage. Proper legal and regulatory frameworks also favour long-term, more sustainable and more technically sound business models over short-term high-risk ones.

Governance challenge: The lack of a proper legal structure for stewardship

De Filippi and Cardozo Law School Professor Aaron Wright, co-authors on a forthcoming Harvard University Press book on the blockchain, questioned whether the current legal framework could handle the questions raised by smart property deployed globally at scale. Smart contracts both define *and* manage ownership rights. Their code makes no assumptions about the assignment of rights, and code can't arbitrarily seize, divest or transfer these rights. For example, if during the process of land registration, government officials assigned the ownership of a parcel of land to someone who wasn't the legal owner of that parcel, that person would have absolute sovereignty over the parcel, and the legal owner couldn't simply reverse the assignment.

Right now there is a lack of legal recourse in a world of irrevocable transactions and unavoidable smart contracts. According to De Filippi and Wright, “People are, indeed, free to decide the particular set of rules to which they want to abide, but – after the choice has been made – can no longer deviate from these rules, to the extent that smart contracts are automatically enforced by the underlying code of the technology, regardless of the will of the parties.”¹²⁶ This very high degree of certainty – mathematical certainty – as to the outcome of a transaction or a smart contract is unprecedented in society. It delivers greater efficiencies and effectively eliminates non-performance risk because we have no choice of breach, no choice of damages. But that's also a downside. It allows no room for human beings. To Josh Fairfield of Washington and Lee University School of Law, that means “more messiness, not less. We're going to see more fights. ‘You didn't actually renovate my house, I want my money back.’

We're going to see more human messiness, but more human messiness doesn't mean the technology is bad.”¹²⁷

But will people actually take the counterparty to court? De Filippi estimates that, in the analogue world, 80% of contract breaches aren't enforced because they're too costly to pursue in court, too expensive to go into proceedings. Why should those numbers improve in a blockchain world? When the code indicates that the contract has been fully executed rather than breached, except one party is dissatisfied with the outcome, will the dissatisfied party actually pursue a lawsuit? Will the courts recognize the case? Will the small business owner back away from the corporate legal team of Dewey, Cheatham and Howe or – with his modest resources – even be able to identify his anonymous counterparty, so that he could file a lawsuit in the first place?

“The courts are going to get it wrong. They've already started to get it wrong, applying intellectual property rules to anything that is intangible. They think that physicality is the dividing line between virtual property and intellectual property, and it's not,” said Fairfield. “There's no intellectual property element, there's no part of a bitcoin that is intellectual property, there's no creative spark for copyright, there's no patentable idea, there's no patent, there's no trademark.”¹²⁸ So their challenge is formidable. They must oversee the unforeseeable. On the one hand, they must avoid stifling innovation by overreacting to worst cases – human trafficking, illicit drug trade, gunrunning, child pornography, terrorism, tax evasion and counterfeiting, for instance. On the other hand, they must not twist new but unproven applications such as blockchain-based platforms for identity management to restrict civil liberties. There must be a stable approach to regulation, legislation and the international negotiation of treaties to minimize regulatory uncertainty, so that investors will continue to support the technology's global development.

Fairfield focused more on process: “The common law isn't affecting technology law; the common law *is* technology law. The common law is the process of adapting human systems to technological change ... the real fight is how do we take old rules meant for old technology and adapt them rapidly and competently,” so they are recognizable when we start using them but iterated so they're state of the art when the technology really hits.¹²⁹

The common law is technology law.

Last but not least, and this should be no surprise, identity matters big-time – or at least how we construct it on the blockchain matters. If we combine a precisely coded version of personhood with a precisely coded version of society, we get the stuff of science fiction novels and Arnold Schwarzenegger movies. De Filippi and Wright conjured images of “self-enforcing contracts, *walled gardens* or *trusted systems*, owned and managed by a sophisticated network of decentralized organizations that dictate what people can or cannot do, without any kind of constitutional safeguards or constraints”. In other words, a machine-driven totalitarian regime.

Governance challenge: Premature legislation or regulation will stifle the blockchain revolution

In 2013, Benjamin Lawsky, former Superintendent of Financial Services for the State of New York, reviewed New York's existing statutes governing money transmissions and found them woefully inadequate for virtual currency.¹³⁰ The department initially wanted to regulate this technology by enforcing rules written around the time of the Civil War. Those laws couldn't possibly address any kind of digital technology like the internet, let alone bitcoin traded on a blockchain. "The more I learned, the more interested I got in how powerful this technology is, and I saw all the various applications and platforms that were going to be built over time," he said. If he "could get regulation right, to make sure the bad stuff we didn't want to see happening in the ecosystem was avoided, and at the same time not have regulation be too overbearing, then we had a real chance of helping a very powerful technology make serious improvements to our system".¹³¹

Lawsky concluded, "Maybe we need a new type of regulatory framework to deal with something that is just qualitatively different?"¹³² His proposal, the BitLicense, was the first serious attempt to provide a regulatory lens onto this industry. A controversial piece of law, it revealed how even well-intentioned regulations can produce unintended consequences. When the BitLicense went into effect, there was a mass exodus of companies, such as Bitfinex, GoCoin and Kraken from New York; they cited the prohibitive cost of the license as a main cause. The few that stayed were well-capitalized and more mature businesses.

"There needs to be a balanced approach applied [so] as to not impair investment flows, job creation and innovation," Roszak told the Committee on Energy and Commerce of the US House of Representatives. "There are currently over 1,000 start-ups betting their lives on blockchain-enabled technologies. Applying light touch regulation – similar to the [United Kingdom], Singapore and Canada – with a 'wait and see attitude' (much like the early internet) will create jobs for Americans and help keep innovation in the United States."¹³³

Jurisdiction already matters when it comes to using bitcoin. Some governments have banned it or banned state banks from exchanging it, as some countries have done. Jerry Brito of the cryptocurrency policy think tank Coin Center said, "In a typically Chinese way, it's not illegal, but it could be at any moment and everybody knows it."¹³⁴ China has allowed a serious professional mining community to flourish and those mining pools have become quite influential in debates over upgrades to the bitcoin protocol. What happens to blockchain security if China suddenly bans mining, too? Other jurisdictions have moved to define bitcoin narrowly, as the US Internal Revenue Service has done. The IRS has labelled bitcoin as an asset for calculating taxes on the appreciation of value.

"Whatever the particular policy issue is, if you don't understand the technology and you don't understand the implications, you're setting yourself up for failure," said Brito. "If you don't understand it, you can introduce law and policy that's going to harm the development of the technology."¹³⁵ Pindar Wong recalled a phrase from his internet governance days: "Don't regulate what you can't control, because you're just going to get embarrassed."¹³⁶ Given the interdependence of economies around the world, we have a sense of urgency around global coordination of any policy-setting.

Governance challenge: Business development outpaces scientific research

Unlike the internet, which had a long incubation period with much experimentation in non-profit mode before venture capitalists started to invest heavily in dotcom start-ups, blockchain technology is already supporting business applications. A lot of money has flowed to blockchain entrepreneurs with high expectations for business results. "We're investing as if it's 1999, but the standards are 1989," said Joichi Ito of MIT Media Lab. There's so much we don't know about this resource.

For starters, how will it affect human behaviour? We mean behavioural change in a deeper sense than Netiquette. Today, many people count on their bank or credit-card company, even talking with a real person, when they make an accounting error, forget their passwords, or lose their wallets or chequebooks. Most people with bank accounts in developed economies aren't in the habit of backing up their money on a flash drive or a second device, securing their passwords so they needn't rely on a service provider's password reset function, or keeping these backups in separate locations so that, if they lose their computer and all other possessions in a house fire, they don't lose their money. Without this discipline, they might as well stuff their mattress with cash. On the blockchain, such distributed applications ("dapps") will reside with each user and run on the user's machine regardless of the service provider rather than on the web and in the cloud. Yet, 230,000 users of Microsoft Windows 7 in 150 countries had not developed the essential habit of keeping their computer software up to date and were attacked by the WannaCry ransomware with an estimated total damage of \$4 billion.¹³⁷

In developing economies, those who still rely on barter may be able to make a behavioural leap of sorts, leapfrogging not only a whole generation of technology but also a century of banking habits and attestation practices that might otherwise become liabilities in a blockchain world. In other words, their lack of access to traditional financial or other centralized resources may put them at a behavioural advantage on the blockchain. With greater freedom – better privacy, stronger security and autonomy from third-party cost structures and system failures – comes greater responsibility. For those consumers who don't trust themselves to keep safe backups of their private keys, third-party storage providers could provide backup service.

There is also a societal dimension that we don't yet understand. Money is still a social construct representing what a society values. It is endogenous to that society, it manifests because of human relationships, and it adapts to evolving human needs. "You can't take the social out of money," said Izabella Kaminska of the *Financial Times*. "A lot of these protocols attempt to do that by creating an absolutist and very objectified system. It just doesn't reflect the world as it is." She pointed to the euro system as an example of how one size – one set of protocols – doesn't fit all countries.¹³⁸ She echoed what Antonopoulos said about the very human need for societies to forgive and forget in order to move on. "There's a very long tradition in finance of obliterating records, because we as a society believe that it's wrong to persecute or discriminate against individuals for something they did 10 or 15 years ago. We have this whole debt jubilee-esque mentality because we think people should be given another chance. Creating a system that never forgets is slightly sociopathic," she said.¹³⁹ Is that where we're heading? Is that what we want?

Governance challenge: Lack of diversity of viewpoints

As many have observed, the blockchain movement is overpopulated with men. In technology compared to other sectors of the workforce, people of colour are under-represented by 16-18%, and women hold only 25% of all computing jobs.¹⁴⁰ "Everyone in Silicon Valley complains of the gender bias, and perhaps in the blockchain ecosystem even more so," said Pindar Wong. "That's unhealthy. We're not getting enough diverse views. Going back to cybernetics' first principles, Ashby's Law of Requisite Variety,¹⁴¹ we need a variety of viewpoints, be it male, female, gay straight, old, young, whatever you want to perceive it to be." When problem-solving has deadlocked, a key question to ask is, "Do we have enough variety in the room or online?" The goal is to maintain requisite variety to avoid thinking errors, said Wong. "You avoid thinking errors by having a wide variety of views that get equal treatment."¹⁴² No discrimination.

There are certainly high-profile women who have founded and are managing companies in the space: Blythe Masters, Chief Executive Officer of Digital Asset Holdings; Cindy McAdam, President of Xapo; Melanie Shapiro, Chief Executive Officer of Case Wallet; Joyce Kim, Executive Director of Stellar Development Foundation; Elizabeth Rossiello, Chief Executive Officer and Founder of BitPesa; and Pamela Morgan, Chief Executive Officer of Third Key Solutions. Many of them have suggested the industry is very welcoming to all voices, male and female alike. Venture capital in blockchain is also gaining in diversity. Arianna Simpson, former Head of Business Development at BitGo, is now an investor in the sector. Jalak Jobanputra is an investor whose venture capital (VC) fund focuses on decentralized technology. But how diverse is the developer community? In our research, we came across comments like this that resonated: "More women ... in the #blockchain ecosystem would mean better collaboration, more sensible governance."¹⁴³ Studies have shown this to be true.¹⁴⁴ We need to attract more women and more minorities to the ecosystem, with such groups as Women in Blockchain advocating their achievements.

Governance challenge: Powerful incumbents will usurp domains

A question that kept coming up was, "What's to prevent the behemoths of the old, closed paradigm – huge corporations or powerful nation-states – from appropriating applications or the networks they run on for their own narrow interests?" For example, a repressive state could aim all its state processing assets and all its mining pools at the bitcoin blockchain to stage a 51% attack or at minimum destabilize the process. Or a wealthy despot decides that immutable posts on the blockchain are eroding his power. This despot could seize all the mining power within reach and purchase the rest from countries that still tolerate his bad behaviour, to put him over the 50% hash rate threshold. He could then decide which transactions to include in blocks and which to reject. With controlling interest, he could also decide whether to fork the code and introduce a few prohibitions, maybe blacklisting addresses associated with gambling or free speech. So do honest nodes adopt this centrally controlled fork or do they fork over to a new code? Andrew Vegetabile, Director of the Litecoin Association and Senior Systems Engineer at Avionics Test and Analysis Corporation, said there would be no escape from such a scenario because the despot controlled 51% of the network. And he needn't represent a government; he could be one of the world's wealthiest people or an executive of a highly profitable company with substantial purchasing power.¹⁴⁵

Incumbents have taken notice of ICOs. Companies like Goldman Sachs, NASDAQ Inc. and Intercontinental Exchange, the American holding company that owns the NYSE, which dominate the IPO and listing business, have been among the largest investors in blockchain ventures. At some point, they could attempt to defend their territory, either gobbling up the most successful new ventures or lobbying to make sure existing regulations for well-established firms apply to small start-ups, and suing any start-up that survives the regulatory inquisition. This litigate-not-innovate strategy may buy them time to sort out a strategy. Or it may simply drain the incumbent of whatever real value it contains.

Think of those twin tyrants – legacy systems and active inertia. Academics have well documented the effects of lock-in and switching costs and have identified the challenges of postmerger systems integration. Organizations with huge technology investments in their installed base may be more likely to throw more money at their old system, sharpening their knives for the pistol fight rather than conducting strategic experiments on the blockchain. "If money and power do try to capture the network, the miners would stop them by going to the real version of bitcoin and initiating a fork," according to Keonne Rodriguez, Senior Manager, Digital and User Interface/User Experience Lead at Synechron.¹⁴⁶

Governance challenge: Dictator's learning curve, quantum computing and utter failure

Scenarios emerged in our research that didn't fit cleanly into any bucket, and so we have put them here, loosely under the category of unknowns and unintended consequences. AI expert Steve Omohundro threw this phrase at us: the dictator's learning curve, or how cave dwellers end up with space-age technology. Think about all the AI labs out there staffed by the world's smartest PhDs with access to the world's most powerful computers. PhDs might fork the bitcoin code or write a smart contract that controls a drone's delivery of package, where bitcoin is held in escrow until that exact moment when the package arrives. Let's say these PhDs post that software as open-source code to the internet, because that's what they do to move their ideas forward; they share ideas. So now ISIS doesn't need an AI lab, it doesn't need a software development team. It just needs to substitute a grenade for the package. That's the dictator's learning curve, and it's not steep. But don't blame the code or the culture of sharing. It's not necessarily what we do with the code; it's what we don't realize we're doing with it – the unintended consequences of a friction-free world.

Looming in the distance is quantum computing, the cryptographer's Y2K problem. It combines quantum mechanics and theoretical computation to solve problems – such as cryptographic algorithms – vastly faster than today's computers. Said Omohundro, "Quantum computers, in theory, can factor very large numbers very rapidly and efficiently, and most of the public key cryptography systems are based on tasks like that. And so if they turn out to be real, then the whole cryptography infrastructure of the world is going to have to change dramatically."¹⁴⁷

Pindar Wong spun a worst-case scenario. "It could break," he said. The whole experiment with blockchain technologies could fail. In his view, "that would be a good thing, because we only learn once we make mistakes. If we make mistakes early enough, then the cost is much less than if we let them fester." Bitcoin is not even a decade old, its market capitalization is "a rounding error on a rounding error in the global financial system", he said. "It's materially irrelevant. We haven't moved all of e-commerce onto any blockchain platform."

So what might we learn? "One reason why this technology works is that it has socially engineered the game mechanics based on one assumption, that there are more good people than bad people," Wong said. "If that turns out to be wrong, that there are actually more bad than good people, then we will have learned something."¹⁴⁸ As satirist James Branch Cabell observed, "The optimist proclaims that we live in the best of all possible worlds. The pessimist fears this is true."

The Players in the Blockchain Ecosystem

Although blockchain technology emerged from the open-source community, it quickly attracted many stakeholders, with different backgrounds, interests and motives. Each has a role to play. There are early signs that many of the core stakeholders see the need for leadership and are stepping up. "Anyone or organization that is working to promote the acceptance and use of blockchain-based technologies is a steward of the ecosystem," said Perianne Boring of the Chamber of Digital Commerce.¹⁴⁹ Here are the players and their perspectives on governance:

Blockchain innovators

Vanguards in the industry, from Erik Voorhees, Chief Executive Officer and Founder of ShapeShift, to Roger Ver, an investor also known as "Bitcoin Jesus", believe any form of formal governance, regulation or oversight is not only foolish, but antithetical to the principles of bitcoin. However, as the industry has expanded, many entrepreneurs are seeing a healthy dialogue with governments, and a focus on governance more broadly, as a good thing. Companies like Coinbase, Circle and Gemini have joined trade organizations, and some even maintain close relations with emerging governance institutions, such as the Digital Currency Initiative at MIT.

Venture capitalists

What started as a clique of cryptoinsiders snowballed into technology's most influential VCs, such as Andreessen Horowitz. Then financial services titans joined the mix: Barclays, Deloitte, Goldman Sachs, NYSE, UBS and Visa among others have made direct investments in start-ups or supported incubators that nurture new ventures. Pension funds are entering the fray. OMERS Ventures, the billion-dollar venture arm of one of Canada's largest public-sector pensions, made its first investment in 2015. Jim Orlando, who runs that group, is looking for the next killer app that "does for blockchain what the web browser did for the Internet."¹⁵⁰ Investment has exploded. According to data in PricewaterhouseCoopers' DeNovo platform, "funding in blockchain companies increased 79% year-over-year in 2016 to US\$450 million."¹⁵¹ Tim Draper of Draper Fisher Jurvetson told us that, if anything, "Financiers are underestimating the potential of blockchain."¹⁵² Digital Currency Group, a venture firm founded by Barry Silbert, has appointed academics and other nontraditional advisers to its board to accelerate the development of a better financial system through both investment and advocacy.

Banks and financial services

Before 2015, few major financial institutions had announced investments in the sector. In its *Global FinTech Report 2017*, PricewaterhouseCoopers reported that 77% of survey respondents in financial services expected “to adopt blockchain as part of an in production system or process by 2020”.¹⁵³ Today, Bank of Montreal, BNY Mellon, CIBC, Commerzbank, Commonwealth Bank of Australia, ING, Macquarie, Mitsubishi UFJ Financial Group, Mizuho Bank, Nordea, RBC, Société Générale, State Street, TD Bank, UniCredit, Wells Fargo and dozens of others are investing in the technology and wading into the leadership discussion. Many of the world’s biggest banks have signed up to the R3 CEV consortium. Stakeholders must remain cautious of any powerful incumbents looking to control this technology, just as they had to tread cautiously in the early days of the internet.

Coders and developers

Blockchain developers lack formal oversight bodies such as ICANN, the IETF or W3C to anticipate development needs and guide their resolution – *and the bitcoin community prefers it that way. Members do have a few norms, such as participating in online forums, posting protocol improvement proposals publicly for peer review, discussing and addressing other members’ concerns, advocating for particular solutions, testing proposed code and jumping in to debug code – that is, not just suggesting but implementing a fix. Bypassing peer review is a real no-no, while trolling to improve ideas is OK.*¹⁵⁴ When we spoke with Bitcoin Core developer Gavin Andresen in 2015, he was at the centre of the block-size debate. He told us, “I’d prefer to stay in the engine room, keeping the bitcoin engine going” rather than spending every waking moment advocating for bitcoin’s future.¹⁵⁵ At the time, he viewed the internet governance network as a useful starting point. “I always look for role models. The role model is the IETF.”¹⁵⁶ It’s “kind of chaotic and messy”, he said, but it works and it’s reliable. However, in the absence of clear and transparent leadership, Andresen either found himself or put himself too much in the spotlight. It was a Catch 22 of sorts that cost him his developer privileges.¹⁵⁷

Academics and scholars

Academic institutions are funding labs and centres to study this technology and collaborate with colleagues outside their silo. Joichi Ito, Director of the MIT Media Lab, saw an opportunity for academia to step up: “MIT and the academic layer can be a place where we can do assessments, do research and be able to talk about things like scalability without any bias or special interests.”¹⁵⁸ Notable universities such as Stanford, Princeton, Duke and New York also teach courses on blockchain, bitcoin and cryptocurrencies.¹⁵⁹

Non-governmental organizations

The year 2015 proved transformative for the burgeoning constellation of NGOs and civil society organizations focused specifically on this technology. Groups include Jerry Brito’s Coin Center and Perianne Boring’s Chamber of Digital Commerce. These groups are gaining traction in the community. Brito said, “Governance comes into play when there are serious decisions that need to be made and you need a process or institution for that to happen.”¹⁶⁰

Governments, regulators and law enforcement

The internet of value will deal with money, stocks, bonds and other financial assets, deeds, votes, identities and other assets that governments tend to originate, register or otherwise oversee to preserve the public interest. When it comes to transactions involving these assets – the foundation of our economies – they would be right to express both curiosity and concern for the common good.

For example, central banks are each taking different steps to understand this technology. Benjamin Lawsky, former Superintendent of Financial Services for the State of New York, said strong regulations are the first step towards industry growth.¹⁶¹ Carolyn Wilkins, Senior Deputy-Governor of the Bank of Canada, believes central banks everywhere should seriously study the implications of moving entire national currency systems to digital money. The Bank of England’s top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom.¹⁶² The Deputy Chief of the Bank of Russia, Olga Skorobogatova, said that it was “time to develop national cryptocurrencies”, and the People’s Republic of China has been experimenting with Ethereum to develop a digital yuan.¹⁶³

However, governments around the world are uncoordinated in their approach to blockchain – some favouring laissez-faire policy, others diving in with new rules and regulations, such as the BitLicense in New York. Some regimes are openly hostile, increasingly a fringe response. Even those stakeholders who resist government intervention acknowledge the merit of regulator participation in governance debates. Adam Draper, a prolific VC in the industry, reluctantly acknowledged, “Government endorsement creates institutional endorsement, which has value.”¹⁶⁴

Users

All of humanity and every company and institution will use this technology as foundational. People have a legitimate right to care about identity, security, privacy, human rights in general, fair adjudication and the long-term viability of this resource. Yet there is no shared taxonomy or categorization of the space: Does blockchain refer to the bitcoin blockchain or the technology in general? Is it big “B” Blockchain or little “b” blockchain? Is it a currency, commodity or technology? Is it all of these things or none of them?

The “Global Solution Networks” (GSN) Framework Applied to Blockchain

We’ve outlined the major issues and a few successes in addressing them. They are significant. To date, many are still unsolved, with only pockets of collective movement to resolve them. We cannot underscore it enough: for this technology to reach its next stage and fulfil its long-term promise, we still need coordination, organization and leadership. Human beings must step up and lead.

Questions persist over how much leadership will come from the internet governance community, and rightly so. Initially, many organizations involved in internet governance viewed digital currencies and blockchain technologies as outside their purview, but that is changing. Vint Cerf, who co-created the internet itself and led the creation of the Internet Society and the Internet Engineering Task Force, suggested that a good starting point for blockchain would be to create a “birds of a feather” interest group within the IETF.¹⁶⁵ The W3C has made web payments a priority, and blockchain is central to that discussion.¹⁶⁶ Additionally, the IGF has hosted sessions about blockchain and bitcoin, where participants have explored new decentralized governance frameworks enabled by this technology.¹⁶⁷

Here’s the thing. Many of our concerns about the first generation of the internet have come true. Large corporations and authoritarian regimes have captured much of the technology and are using it in their vast private empires to extract most of the value. They have closed off opportunity and privatized much of our digital experience. We use proprietary stores or government-owned channels to acquire new apps for our phones, tablets and watches. Search engines and marketing (or propaganda) departments alike interrupt our content with advertising and state messaging. Big organizations that promote and prosper from consumer data are notoriously secretive about their activities, plans and information assets. To be sure, some of these behemoths have opened up voluntarily, but many others have merely reacted to the sunlight of whistle-blowers and investigative journalism. Such disclosures are dwarfed by efforts to hide operations and conceal information. Simply put, these stakeholders haven’t been good stewards of the public trust, and existing internet governance networks haven’t been effective in representing all interests equally.

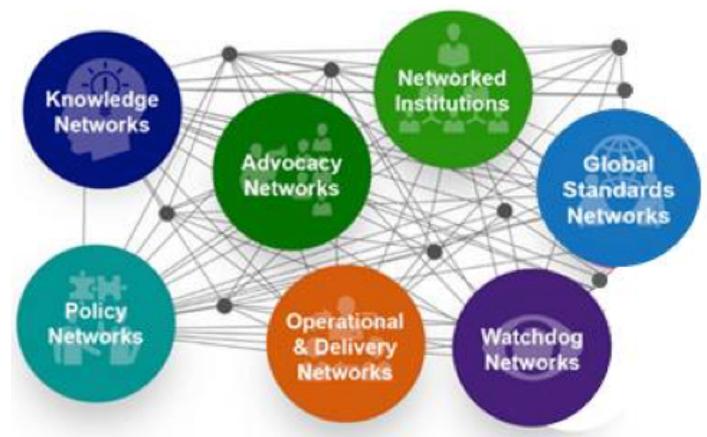
Case in point: the banking industry. “Banks are traditionally secret keepers,” according to Kaminska of the *Financial Times*. She explained that banks make good judgments about whom to lend to and how to process payments when they have good access to private information, and

they get that information by promising to keep the secret. The more secrets they hold, the greater the information asymmetry and the greater their advantages, but those advantages have harmful systemic implications in both civic and commercial spheres.¹⁶⁸

Pindar Wong, former Trustee of the Internet Society, was quite reflective: “I spent most of my adult life trying to build an internet, and it turned out that internet actually shouldn’t be trusted. It is, in fact, a trustless internet. I grabbed this blockchain technology with two hands and have run with it as fast as I can because, in some sense, it is a second bite of the cherry. It’s penance. It’s the ability to right a wrong, which I didn’t know that we were making with the internet.”¹⁶⁹

So we cannot leave governance of such complex global innovations solely either to governments or to the private sector: political and commercial interests have proven insufficient to ensure that this new resource serves society. Rather, and more than ever, we need multistakeholders to collaborate as equals and provide global leadership. We need all three pillars of modern civilization – the private sector, the public sector and civil society – to participate in stewarding this new global resource. According to The Economist, “‘Multistakeholderism’ may be, like democracy, the worst form of governance except for all the other ones.”¹⁷⁰ We believe that non-state, multistakeholder networks (which we call “global solution networks” or GSNs) are the most effective means we have to steward global resources (see Figure 2).

Figure 2: Seven Types of Global Solution Networks



Source: Global Solution Networks, gsnetworks.org

Overall, the expression “If there is a will, there is a way” applies. The smartest technologists on the planet are working on creative solutions to some of these challenges. Further, as computers become inexorably smarter, they will undoubtedly provide their own solutions. Investor Roger Ver said, “Say the smartest human has an IQ close to 200. Imagine artificial intelligences with an IQ of 250, or say 500, or 5,000 or 5 million. There will be solutions, if we humans want them.”¹⁷¹ In this section, we look at how diverse stakeholders can come together and forge new understandings and new action plans.

Standards networks: Don’t deify differences; codify common ground

Most urgent is the need for standards at both the platform and application levels. Gavin Andresen was among the original core developers who believed leadership was required to move the agenda forward on common standards. “Maybe you can design light socket set waves by committee, but you can’t design software standards that way,” he said. Pointing to the early days of the web, Andresen said, “The internet model shows that you can have technologies where consensus does arise, even though there’s no one clear leader,” but “You can either have a process, or a person, or a process that ends in a person. You definitely need one or the other.”¹⁷² Consensus mechanisms alone can’t support standards development.

“We’re missing a Jon Postel,” said Joichi Ito of one of those “[US Department of Defense]-funded guys who were slightly hippy but thought this government work was kind of cool”, an attitude Ito would not use to characterize either the Bitcoin Core developers who can be “hard to talk to” or the Chinese miners who can be “very aggressive”. In contrast, Postel was a tireless steward who, for decades until his death, shepherded the Internet Assigned Numbers Authority and served as the Request-for-Comments Editor, managing and maintaining the internet’s documents of record.

“When you’re dealing with a technology that is so leading edge, groundbreaking, and relies on cryptography, you need to think slightly differently. I’m trying to think slightly differently and break away from what I called binary thinking. Binary thinking is black and white, are you secure or insecure, and I don’t think those lead to very fruitful debates,” said Pindar Wong. “When you’re dealing with a technology as sophisticated as bitcoin, which is the only blockchain we currently know that works, that is unhackable, you’re dealing with nuance, with very sophisticated discussions in a highly technical domain that you don’t need everyone to participate in. Everyone has the opportunity to participate, but you don’t need everyone to participate.”¹⁷³ Who should participate? Within the bitcoin ecosystem, there “is a very exceptionally smart and gifted group, the brightest people in the room”, Wong said.

“When it comes to governance, we cannot expect a small group of engineers to figure out a perfect protocol for economic transactions and social interactions. This is not an engineering problem,” said Primavera De Filippi. It is “a social and political problem”. She recommended “involving all relevant stakeholders across diverse disciplines in a neutral forum”.¹⁷⁴ That’s what ColliderX provides: an independent R&D hub for deep technical research, which will be peer-reviewed and open access. To maintain impartiality, it’s crowdfunding its operations and administering the funds to researchers via grants. Iliana Oris Valiente, Founder of ColliderX, said, “The ColliderX initiative has been received with great enthusiasm from the blockchain tech community, academics and industry partners alike. All stakeholders are rallying behind ... a new model to fund and promote core technical research to move the blockchain industry forward.”¹⁷⁵

Yale Law School Professor Elizabeth Stark, another emerging star in governance, took up the mantle of convener-in-chief for the industry. Like another prominent woman – Dawn Song, MacArthur Fellow and Computer Science Professor at Berkeley, and an expert in cybersecurity – Stark came from a distinctly academic background but has other ambitions. To solve the blockchain’s scalability issue, she organized Scaling Bitcoin, convening developers, industry players, thought leaders, government officials and other stakeholders in Montreal, and collaborated on the Bitcoin Lightning Network.

In financial services, both R3 CEV and Hyperledger are tackling critical standards issues. Invariably, there will have to be standards networks on a variety of things, from the blockchain protocol that forms the basis of the financial services industry of the future, to common standards for privacy and payments in the IoT.

While these groups attack the problem from different angles and with different agendas, each shares a common goal to make this technology ready for prime time – by building infrastructure, developing standards and making it scalable.

Networked institutions: Welcome stakeholders everywhere

Members of the blockchain ecosystem need opportunities to collide, so to speak, with other stakeholders so that they can hear each other's concerns and positions. When asked what we need most, Perianne Boring said, "A public dialogue on the importance of encryption. With many high-profile terrorist attacks, like Manchester [England], there is a renewed call throughout the world to ban encryption. This is a grave mistake. Cybersecurity attacks, like identity theft and ransomware, continue to be a multibillion-dollar drain on the economy." Decentralized, blockchain-based security systems could address cybersecurity issues head on. "The blockchain industry is not participating in the global encryption debates, and they should be," she said.¹⁷⁶

Joseph Lubin called for decentralized inclusiveness:

We set out at the start of Ethereum to be as inclusive as possible, so any person or company that might want to be exposed to the technology should be able to use it. There were certainly some crypto-anarchists in the space broadly who were disgusted that banks might be spoken to or that we, any of us, would educate or collaborate with a bank, let alone a central bank. But if this technology is to have profound impact on the planet, then it needs to be, or it should be, everywhere and widely distributed in terms of different use cases.¹⁷⁷

The World Economic Forum has been a vocal proponent of blockchain technology. The blockchain was front and centre at the Annual Meeting in Davos in January 2016. Jesse McWaters, Financial Innovation Lead at the World Economic Forum, believes blockchain technology is a general-purpose technology, like the internet, which we can use to make markets radically more efficient and improve access to financial services. He tells non-technologists in the finance sector, "Don't worry about blockchain. Don't worry about block size or any of that to start. What you should really care about is the future-state architecture of your industry. Focus on the characteristics you believe that future-state infrastructure needs to have and that will necessarily have a governance component to it."¹⁷⁸

A great example of this mindset is Moog Inc., a \$2.5 billion provider of precision motion control equipment and a leading supplier in additive manufacturing (3D printing). It is using governance to attract the right platform partners. The company envisions a blockchain-enabled digital supply chain where it can exchange intellectual property on a point-of-use/time-of-need basis as both a producer and consumer. "Users must have absolute control of the value created by their IP," said George Small, Principal Engineer of Moog.¹⁷⁹ "We are focusing on governance first as a means to building a consortium" of industry equals who have earned their community's trust and would like to help create such an IP exchange. "Stewardship must be transparent, fair and stable," he said. "We will not be able to build upon a moving target or one that fails to support absolute trust across ecosystem members." Collaborators such as Hyperledger are providing the infrastructure. The

governance body of the consortium will provide what Small referred to as curation, meaning human interaction and arbitration as needed. "The network will not reach its full potential" if certain members can gain unfair through their status or visibility.¹⁸⁰

The World Economic Forum predicted that within a decade, we could store 10% of global gross domestic product on blockchains.¹⁸¹ As an organization, the World Economic Forum has championed and advanced big issues, such as income inequality, climate change and even remittances. Other networked institutions, from the smallest groups to the biggest foundations in the world, such as the Clinton Foundation and the Bill & Melinda Gates Foundation, would be wise to champion this technology to advance such major issues as financial inclusion and healthcare delivery. Networked institutions often have a role to play in influencing government policy-making, making them a critical link and strategic partner in overcoming a number of major showstoppers.

Advocacy networks: Respect members' interests and constraints

There is strength in numbers when it comes to advocating for the ecosystem. Each stakeholder cannot focus narrowly on its concerns and hope to achieve results. Advocacy networks arise with the disillusionment with traditional political and civic institutions, making them a logical fit for the blockchain community, which is trying to upend how those traditional institutions solve problems. However, in these early days, advocacy networks must work with government as a partner.

To advocate for the blockchain ecosystem, Perianne Boring founded the Chamber of Digital Commerce (CDC), a trade-based association in Washington DC. Within a year, CDC attracted a high-profile board (e.g. Blythe Masters, James Newsome, George Gilder). The movement needed "boots on the ground in Washington to open a dialogue with government", she said. With her background in journalism, Boring focused on messaging, positioning and polish. Her organization is "open to anyone who is committed to growing this community", she said, and is now a leading voice in policy, advocacy and knowledge in the burgeoning blockchain governance ecosystem.¹⁸²

Some stakeholders have very different cultures from others. "You can get to a point where you have transparency in certain things. You don't need transparency in everything. You wouldn't want to run a bank consortium necessarily that way, at least, in the legacy world," said Joseph Lubin of Ethereum. "We found out with all the different banks in the alliance that they have some very rigorous constraints, that it's not natural for them to operate with us freewheeling blockchain start-ups and that we need to respect their constraints."¹⁸³

Non-profits focused on human rights and economic empowerment can especially benefit from advocacy networks. For example, BitPesa, the universal payment and trading platform, operates mainly in Sub-Saharan Africa. It belongs to multistakeholder groups like the US state department's task force on Africa, where it sits alongside IBM, Microsoft and other tech firms that have greater influence over African governments and can lobby on BitPesa's behalf.¹⁸⁴

Advocacy networks are closely tied to policy networks, and Coin Center and CDC are taking the lead in this area. We could also include here the Coalition of Automated Legal Applications (COALA), MIT's Digital Currency Initiative, and others. Advocacy is critical to scaling blockchain technology. In the absence of strong advocates who speak up for stakeholders and stand up for stakeholder rights, governments and other powerful institutions could try to stifle, twist or usurp this powerful open network to their exclusive advantage.

Watchdog networks: Do no harm

Blockchain is still in its Wild West phase. People are experimenting because they can, some making extraordinary claims, and not all participants are equally versed in the technology. The ecosystem needs the equivalent of an Electronic Freedom Forum to watch what organizations are doing in the space.

"Governance comes into play where there are serious decisions that need to be made, and you need a process for that to happen," said Jerry Brito, one of the most prominent legal voices in the space – first at the Mercatus Center at George Mason University and now as Director of Coin Center, a not-for-profit advocacy group.¹⁸⁵ He recommended starting with the Hippocratic Oath: first, do no harm. The current bottom-up approach that bitcoin's core developers are using "is showing a little bit of its rough edges right now with the block-size debate. It's going to be very difficult to get any consensus", Brito said, but he doesn't think any organization could or should impose order on it. "We want to help develop that forum and foster a self-regulatory organization if it comes to that."¹⁸⁶ By *self-regulatory organization*, he means "self-regulation by the companies in the industry, specifically of their consumer protection and privacy practices" and not of core protocol development, which he thinks "is best left to an admittedly messy open-source process" outside the scope of Coin Center's policy mission.¹⁸⁷

The Blockchain Alliance is a partnership between law enforcement, NGOs, trade organizations and the private sector, and is the first true advocacy network to form in the space. Coin Center and the CDC, with support from Bitfury, Bitfinex, BitGo, Bitnet, Bitstamp, Blockchain, Circle, Coinbase and others have partnered with US law enforcement agencies, such as the Department of Justice, the Federal Bureau of Investigation, the Secret Service and the Department of Homeland Security.

These watchdogs have an important advocacy role as well. In the aftermath of the Paris terrorist attacks, some European lawmakers, regulators and law enforcement blamed bitcoin as the source of terrorism financing. The Blockchain Alliance called for patience: "Let's not regulate out of fear," they said.¹⁸⁸ Other than the self-policing role of community members who convene, collaborate and debate on forums and on Reddit, few other watchdog networks have stepped up. Partnerships with law enforcement are a helpful start, but the blockchain ecosystem needs fully independent organizations, perhaps traditional watchdogs such as Amnesty International and Human Rights Watch, to sound the alarm when corrupt and unscrupulous governments find ways to use blockchain as surveillance tool.

What about central banks as watchdogs? They have considerable regulatory power in their respective countries, but they do not operate in silos. They coordinate and collaborate with other central banks and with global institutions like the Financial Stability Board, the Bank for International Settlements, the International Monetary Fund, the World Bank, and others. We need stronger global coordination to address blockchain issues. Today, central bankers are asking important questions. Carolyn Wilkins, Senior Deputy-Governor of the Bank of Canada and a central banking veteran, told us, "It's easy to say that regulation should be proportionate to the problem, but what is the problem? And what are the innovations that we want?"¹⁸⁹ These are great questions that we could address more effectively in an inclusive environment.

Policy networks: Participate in debate and coordinate regulation

Rather than simply regulating, governments can improve the behaviour of industries by making them more transparent and boosting civic engagement – not as a substitute for better regulation but as a complement to the existing systems. We believe effective regulation and, by extension, effective governance come from a multistakeholder approach where transparency and public participation are valued more highly and weigh more heavily in decision-making.

Open-mindedness is a virtue. Elizabeth Rossiello, Founder and Chief Executive Officer of BitPesa, described how her organization does its on-the-round due diligence and makes sure that its operations comply with existing laws. Where appropriate laws don't yet exist, BitPesa has a hand in writing them. It does a comparative check, works with companies in other regions, and understands what they've been doing with their governments. For example, in India, companies are also writing their regulation for this type of payments network, and so BitPesa is collaborating and sharing knowledge.¹⁹⁰

Primavera De Filippi of the Berkman Center at Harvard has emerged as one of academia's clearest and most eloquent voices on governance. She said that we cannot establish "a proper policy and regulatory framework for blockchain technologies ... at a local or national level". She recommended international cooperation, multistakeholder dialogue and a forum for "lawyers and engineers to talk more with each other and understand each other's language better".¹⁹¹

De Filippi formed the COALA with her colleagues, lawyer-turned-entrepreneur Constance Choi of Seven Advisory, and Adroit Lawyers' Amor Sexton, the leading digital currency lawyer in Australia. They have led a series of blockchain workshops at Harvard, MIT and Stanford, as well as in London, Hong Kong SAR and Sydney. Through COALA, a participant in the Internet Governance Forum, they liaise with key stakeholders, regulators and policy-makers to help them understand the impact that blockchain technology might have on existing legal and political institutions. De Filippi said, "We invite them to contribute to the elaboration of policies, regulations and standards for this emergent ecosystem."¹⁹²

Today, a nascent policy network is emerging. Coin Center, a not-for-profit policy group in Washington DC, focuses on five core verticals: innovation, consumer protection, privacy, licensing and anti-money laundering/know your customer. The CDC, a trade organization, focuses on promoting the acceptance and use of digital currencies.¹⁹³ When the Chamber opened its doors in 2014, the public policy community was sceptical, even fearful, of bitcoin and blockchain. A US Senator was calling for a ban on bitcoin. "We attributed this sentiment to a general misunderstanding and miscommunication from highly publicized events including Silk Road and Mt. Gox," said CDC Founder, Perianne Boring. Since then, the Chamber has made huge strides in educating the community. "In the past 12 months, we have held over 100 briefings for policy-makers at the state, federal and international level. Today, we have many bitcoin and blockchain champions through the world's policy community; we even have a Congressional Blockchain Caucus."¹⁹⁴

The United Kingdom has its own Digital Currency Association, as does Australia and Canada, who speak for industry. Promoting and uniting many strong voices in the policy arena will ensure that blockchain has a better chance of fulfilling its potential.

Knowledge networks: Know what you don't know

"The scale of the transformation under way in a new global modus vivendi is barely understood. Education is key," said a vice-chairman in the corporate banking sector. "That transformation requires collaboration between the public and private sectors, which was not needed – and was not possible – over the past two decades before the emergence of the new technologies." He expected members of the ecosystem to learn "through mistakes, some of them affecting civil liberty and personal privacy. Enlightened organs of the public and private sectors will increasingly work together on anticipating, avoiding, mitigating or correcting these mistakes".¹⁹⁵

There are hundreds of pilots under way. For example, Bitfury's Blockchain Trust Accelerator, in partnership with the New America Foundation and the National Democratic Institute, is creating responsible, innovative and cutting-edge pilot projects to advance knowledge for the global good.¹⁹⁶ Brian Behlendorf of Hyperledger hopes that communities will share what they've learned from both their successes and failures, what works, what doesn't, and what needs to be fixed in terms of architecture and product. Knowledge networks support this iterative learning and sharing and developing evidence-based policies. They give advocates relevant information for lobbying efforts and serve as a repository of data, which standards networks, such as the International Organization for Standardization, can use to develop specifications for decentralized ledger technologies (DLTs), FinTech and blockchain technologies.

For example, COALA is doing foundational research "to ensure that blockchain-based applications can operate in the current regulatory framework and interact with existing institutions governed by the rule of law". It has launched initiatives such as COALA-ID, a blockchain-based framework for credentials management and access control in collaboration with MIT; Elethron, a blockchain-based system for renewable energy trading in collaboration with Commonwealth Bank of Australia and Hewlett-Packard; and COALA LEX, an interface between smart contracts and legal contracts to bridge the gap between traditional legal frameworks and blockchain technologies. The Coalition intends to elaborate upon "meta-languages for hybrid techno-legal agreements" and develop "an open-source library of standardized and certified smart contract modules". It has representation at technical standards-setting bodies such as W3C and IETF, and has partnered with such academic institutions as Harvard, Stanford, Cambridge and Oxford universities, University of California at Berkeley, University College London, National Center of Scientific Research, and Hong Kong University of Science and Technology, all "to drive scientific and fact-based research for the blockchain ecosystem".¹⁹⁷

“There should be a forum to present proposals or ideas,” Tyler Winklevoss of Winklevoss Capital said.¹⁹⁸ Both formal and informal knowledge networks provide such forums. Through collaborative research, experimentation and deliberation, they create and disseminate new knowledge to other GSNs, stakeholder groups and the broader public. For example, MIT’s Digital Currency Initiative is uniting and exciting academics and universities globally. Informal gatherings like the San Francisco developer meetup and the New York developer meetup are also making knowledge a priority. Blockchainworkshops.org has convened stakeholders to share key lessons. Reddit, the online community, is also a medium for debate in the space, and GitHub is a repository of conversations about code and the code itself. The Blockchain Research Institute is commissioning research on how the blockchain will transform core verticals in the economy and core functions in organizations. Its publishing programme will feature white papers, case studies and conferences.

COALA also provides an open, neutral and collaborative forum for discussions around the core issues of legal and technical interoperability. “We gather together a global community of blockchain experts, including lawyers, academics, institutional leaders, policy-makers, computer scientists and entrepreneurs,” De Filippi of COALA said.¹⁹⁹

Joichi Ito of the MIT Media Lab underscored the need for basic research that was solution neutral. “I intentionally divested all of my shares in bitcoin-related companies, like Guardtime and Blockchain, because I felt that I had to be able to speak without having a conflict [of interest]. Some people think that was a little bit overboard. At least for our core team, we decided that that was important. When we talk to some of the more careful people like the central banks, we’re not trying to sell them anything.”²⁰⁰

Ito has worked to build “some capacity and some funding that was relatively neutral”. He envisaged communities of academic expertise around whichever standards develop, a community at each layer – platform, application, industry – that could facilitate standards conversations as they came along. The lab is also trying to help its 90 member companies to understand how they might participate in this open standards process.²⁰¹ He reiterated the neutrality of solutions; the lab would have *no skin in the game*. “It’s important to have people who can have non-financially motivated, non-conflicted points of views on both the technology and the standards,” he said.²⁰²

Delivery networks: Keep incentives for mass collaboration in mind

“Just as you can’t have fire without fuel, oxygen and heat, you can’t have effective globalization without interoperability in goods, data and money,” said Chris Larsen, Executive Chairman of Ripple’s board of directors and former Chief Executive Officer and Co-Founder of Ripple. “The internet of value is about creating a world where money can be sent as easily as information. Using simple, open protocols like Interledger Protocol, we can connect all the places where value lives – ledgers, blockchains and payment networks. They all have to work together to make this a reality.”²⁰³

How do we ensure that the incentives are adequate for interoperability and distributed mass collaboration, making the technology ready for prime time? We need an “ICANN moment” for blockchain, where organizations will form to deliver essential functions. However, whereas ICANN and many other GSN types in the internet governance network are distinctly American, blockchain leaders should push to make these organizations international. Joichi Ito said, “I do think there’s already a big push to make governance non-American and international from the beginning because that’s one thing we learned from ICANN, that it’s hard to get out from under America once you get started as part of America.”²⁰⁴ COALA is a global organization that performs a few key roles: It disseminates knowledge, influences policy and advocates for blockchain technology, and supports the development and deployment of blockchain-based applications, all critical to overcoming major potential showstoppers.²⁰⁵

Don’t roll your own crypto.

“The much greater focus on smart-contract auditing is incredibly important. There’s a maxim in the cryptography space: ‘Don’t roll your own crypto.’ So, you really want to use extremely well-vetted software packages,” said Joseph Lubin.²⁰⁶ The ecosystem could use far more independent cryptographic auditors to provide this vital function. It’s more than quality assurance.

Summary: What Needs to Be Done

While our goal was to create a language and structure to think about the stewardship of blockchain and not to make specific recommendations to particular stakeholders, some sensible next steps did emerge. The time for global action is now. We believe people, institutions and industries throughout the world need blockchain technology and we must do all we can to make it available. Here is a set of actions that will move this technology forward. Our hope is that these will prompt discussion and provide positive steps that could be taken.

- 1. Networked institutions:** To attract the necessary level of stakeholder participation, we recommend that respected global networked institution (e.g. the World Economic Forum, the Internet Society, the Internet Governance Forum, etc.) convene, through an online platform and a series of meetings, a discussion of the governance issues outlined in this report. The goals would be to (a) include key players in the room; (b) provide participants with the taxonomies and frameworks developed in this report so that everyone has a shared understanding of governance challenges and solutions; and (c) forge some informal actions to improve governance, primarily at the overall ecosystem level, but possibly at the two other levels of governance.
- 2. Standards networks:** To break the deadlock of bitcoin platform development, we recommend the creation of the Bitcoin Engineering Task Force (BETF) as a loosely self-organized, grass-roots technical group comprised of the nine stakeholder groups. It would not be a formal body with a board of directors or any hierarchy. It could operate as a working group of the IETF, W3C or other appropriate organization. Its mission would be the adoption of standards and the engineering and sustainability of blockchain technology, and it would develop, test and implement new protocols and standards, according to the broad consensus of its membership prior to implementation. Instead of formal membership, attendance at BETF meetings and participation in any BETF online forum would be open to all volunteers. Participants would contribute as individuals, not as representatives of companies or organizations. The community could learn much from the consensus mechanisms and decision-making processes of the IETF and other standards bodies, such as the W3C.
- 3. Advocacy networks:** To forestall regulatory, legislative, judicial or executive action that might stifle further innovation, blockchain needs stronger advocacy. The policy and advocacy work of the Chamber of Digital Commerce is exemplary, but the ecosystem needs more. We encourage organizations in every country to join the CDC and participate in its work. Networked institutions with global influence could convene heads of state and chief executive officers so that they might discuss their common interests in developing this new global resource. In collaboration with these leaders, for example, the ecosystem needs a roadmap and action plan for future government officers, representatives and judges at the municipal, state, national and regional levels, designed to help them monitor blockchain initiatives, assess potential harms and unintended consequences, engage the blockchain community in discussions, and coordinate with their peers in other jurisdictions prior to issuing legislation or regulation of the technology.
- 4. Policy and watchdog networks:** Much must be done to address the need for better monitoring of blockchain problems and challenges. Consider initial coin offerings. The first jurisdiction to come up with a workable policy for ICOs will attract a flood of ICO activity and economic development for that state. Also consider the environmental impact of blockchain technology. Under the joint auspices of the World Economic Forum Climate Project and Energy Initiative, we recommend forming a multistakeholder network to look not exclusively at the energy consumed by mining but also at the energy expended in current production lines and service delivery methods where industries intend to deploy blockchain technology. The goal would be to explore methods for capturing the heat produced by mining, harnessing the unused computing power of appliances, and for reducing energy consumption across whole systems. We would like policy-makers to collaborate more deeply and more rapidly.
- 5. Delivery networks:** The Hyperledger Project, the Enterprise Ethereum Alliance and the Trusted IoT Alliance are three important organizations providing feedback on protocols and doing work at the applications level. Every company, not just technology companies but users of these applications, should join these open initiatives, depending on the platform(s) they have chosen. To build out the necessary infrastructure, we recommend greater outreach to industry associations both at the corporate and professional levels, including outreach to the professional services firms that support them, with the goal of identifying projects as bold and forward-looking as the Belt and Road Initiative, where they might incorporate blockchain technology to facilitate collaboration, consensus-building, the transparency of reporting and other aspects to increase the efficiency, effectiveness and accountability of project management.

- 6. Knowledge networks (education):** To address the urgent need for diverse talent and expertise in the ecosystem, every university should be organizing blockchain courses in their computer science programmes and strategic courses in their business programmes, and there should be a massive open online course (MOOC) or series of courses available for credit and certification. We recommend forming an industry-academic collaborative under an organization such as Coursera or edX to encourage the development of advanced programming skills in the blockchain space around the world, potentially modelled after, led by or including such organizations as Coursera, edX, Khan Academy, Stanford Engineering Everywhere, Udacity and other non-profit open education platforms. Such a collaborative would also support the development of course shells and teaching materials across areas of the academy: not just computer science, mathematics and engineering but finance, accounting, operations and logistics, marketing, law, economics, sociology and medicine. Above all, it would be inclusive, perhaps with additional outreach to girls, women and their teachers in regions of need.
- 7. Knowledge networks (applied research):** Blockchain may be the least known and least understood technology of the Fourth Industrial Revolution. AI, for example, has become a mainstream topic even though it may ultimately have less impact on our economy. To address the need for better strategic knowledge about blockchain transformations, we need better use-case research and awareness-building programmes. The Blockchain Research Institute has launched a programme of 40 projects to explore blockchain transformation of industries, government, competitiveness and management challenges.
- 8. Knowledge networks (scientific research):** To accelerate research so that knowledge catches up with investment, we recommend funding fundamental research projects, such as those under way at the MIT Media Lab. All member countries should be conducting, categorizing and analysing experiments with blockchain technology – organizations, networks and individuals around the world – so that no country or region comes to dominate the technology or its expertise. The goal of such research would be to identify key gaps in scientific knowledge and expertise, create a set of principles for ecosystem players to help them self-organize and address these gaps, and create a comprehensive “network of networks” to help coalesce the scientific community.

All stakeholders in the ecosystem – all three levels – must understand these governance challenges and opportunities. Today most players are focused on building their own companies, organizations or platforms and are paying little attention or devoting little effort to the challenges of building a healthy ecosystem. No organization can succeed in an ecosystem that is failing or stalled. Every organization should assign resources, however small, to participate in ecosystem governance.

This second era of the internet promises to create new opportunities for a more prosperous world. Prosperity is about one’s standard of living. To achieve it, people must have the means, tools, and prospects for creating material wealth and thriving economically. For us it includes more – security of the person, safety, health, education, environmental sustainability, chances to shape and control one’s destiny and to participate in an economy and society. This is the promise of the blockchain, the promise of a future where there is prosperity for everyone. But we must act now.

About the Authors

The opinions expressed in this report are those of the authors.

Don Tapscott is the Chief Executive Officer of the Tapscott Group, a think tank exploring the Digital Economy, and author of 16 books about the Digital Age. He is Adjunct Professor at the Rotman School of Management at the University of Toronto, Chancellor of Trent University and Senior Adviser to the World Economic Forum. In 2013, he founded the Global Solution Networks Program, a \$5 million investigation into multistakeholder networks.

Alex Tapscott is the Chief Executive Officer of Northwest Passage Ventures, an advisory firm building early-stage companies in the blockchain space. He is a founding member of the International Monetary Fund's High Level Advisory Group on FinTech, a founding member of the World Economic Forum Global Future Council on the Future of Blockchain and a member of the Elections Canada Advisory Committee.

Together they began investigating blockchain in 2013. They are authors of the 2016 bestselling book *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. In 2016, they convened the first meeting of The Muskoka Group, a collaboration to promote blockchain stewardship. In 2017, they launched the Blockchain Research Institute, a knowledge network conducting 40 projects on the strategic implications, opportunities and challenges of this technology.

Comments, suggested changes and additions to this report are welcome at info@tapscott.com.

Appendix: Global Solution Networks

Knowledge networks

Bitcoin Wiki

Accessible globally through Wikipedia and updated through decentralized academic peer review, its entries span blockchain protocol specifications, cryptocurrency, data mining and links to blockchain company directories.

Bitcoin & Blockchain Leadership Forum (Bank of England)

Founded by the Digital & Social Media Leadership Forum, this group operates under the very popular membership-model, where participants collaborate on blockchain research projects and showcase proof of concepts for advanced applications of decentralized ledger technologies (DLTs). <http://bbf.info>

Blockchain Association of New Zealand (BANZ)

Membership of BANZ, a non-profit blockchain research association in New Zealand, includes law firms, developers, academics and companies that pool resources to build blockchain applications for specific industries, such as agriculture and supply chain management.

Blockchain Canada

Founded by Ethan Wilding and Alan Wunsche to aggregate information about blockchain technology, this Toronto-based non-profit organization maintains a blockchain repository that helps policy-makers pass legislation that will enable cryptocurrency adoption. <http://blockchaincanada.org/>

Blockchain Collaborative Consortium (BCCC)

Founded by Yoichiro "Pina" Hirano, this Japanese organization facilitates information exchanges about decentralized ledger technologies among stakeholders in the financial industry, ultimately to create blockchain-neutral solutions for industries and to integrate Japan's knowledge with the rest of the world. <http://bcc.global/>

Blockchain Education Network (BEN)

BEN began as a Facebook messenger group of bitcoin student leaders from MIT, Stanford, Delaware, Michigan and Penn State and has expanded into a 1,000-member community with initiatives to boost morale, encourage participation and share blockchain know-how. <https://blockchainedu.org/swarm/>

Blockchain Research Institute (BRI)

This non-profit organization identifies subject matter experts to research and develop reports and case studies on blockchain topics of critical interest to leaders of business, government and NGOs. <https://www.blockchainresearchinstitute.org>

DC Blockchain Center

This resource for technology providers and governments educates entrepreneurs and policy-makers on the potential benefits of blockchain and provides a platform for the public and private sectors to collaborate on blockchain use cases.

<http://digitalchamber.org/initiatives/dc-blockchain-center/>

Dubai Future Foundation

Run by the Global Blockchain Council, a public-private initiative, this group is exploring blockchain-based solutions to replace outdated bureaucratic and business frameworks. Pilot projects include health records, diamond trading, title transfers, business registration, wills and shipping.

Financial Blockchain Shenzhen Consortium

This consortium provides access to relevant blockchain information and collective project testing in the financial sector. Its efforts have resulted in a prototype blockchain platform for securities trading and related new services in credit, digital asset registry and invoice management.

GitHub

This open-source, online software development tool serves as a repository for code and a platform for code development, peer review and problem-solving. Unlike client-server systems, every Git directory resides on every computer as a full record and complete history of every change to the code.

Global Solution Networks (GSN)

Founded by Don Tapscott, GSN seeks to (a) identify, analyse and summarize the potential components of a global governance network; (b) place the requisite tools in the hands of global problem-solvers; and (c) facilitate connections among multistakeholder networks.

<https://gsnetworks.org>

Input Output Cryptocurrency Collaborative Research Chair (Tokyo)

Established by former Ethereum Co-Founder Charles Hoskins with the Tokyo Institute of Technology, this research chair differs from traditional academic–corporate research partnerships in that its R&D is open-source and patent-free so industry participants can share research findings.

MIT Media Lab Digital Currency Initiative (DCI)

This global hub supports deep research in such areas as healthcare and medical records, global rights management, decentralized publishing, user-controlled credit identities, central bank and digital currency adoption, and securitized financing for solar microgrids.

Muskoka Group

Founded by blockchain practitioners, advocates, theorists and policy experts in 2016, this group supports the global solution networks framework and multistakeholder approach to stewardship of blockchain technologies as a global resource used for achieving prosperity worldwide.

P2P Foundation (P2P wiki)

Known for hosting Satoshi Nakamoto's first paper on the bitcoin protocol, the P2P Foundation hosts wiki sites on various use cases for decentralized, commons-based societies, where peers review insights via such wiki portals as P2PF Blog, P2PF Wiki and P2PF Lab.

<https://p2pfoundation.net/>

Post-Trade Distributed Ledger (PTDL) Group

Launched by 40 financial institutions and prominent market infrastructure stakeholders, this group identifies best practices for leveraging decentralized ledger technologies and strategies for overcoming barriers to widespread adoption.

<http://www.ptdlgroup.org/presentations-and-documents.html>

Reddit

This online platform describes itself as “the front page of the internet where conversations begin”, with communities forming around cryptocurrencies (Dogecoin, Litecoin), blockchain platforms (bitcoin, Ethereum) and ecosystem issues (block size, consensus mechanisms).

<https://www.reddit.com/r/btc>

Trust in Digital Life (TDL) Blockchain Working Group

A membership association founded by the Intel Corporation, TDL consists of industry leaders and academic institutions that exchange research on customer, market and technology insights into improving DLT to expedite a trusted single European digital market.

<https://trustindigitallife.eu/>

UCL Centre for Blockchain Technologies

Launched by University College London (UCL), the centre generates multidisciplinary, multistakeholder research across such topics as cryptography, law, smart contracts, automation and the sociological impact of decentralized decision-making systems. <http://blockchain.cs.ucl.ac.uk/>

WhiteChapel Think Tank (WTT)

Founded by Jeremy Wilson of Barclays and John Edge of Red Rose in London, this group produces reports that bring decentralized ledger technology use cases to life and shares information among industries, government and non-governmental organizations. <http://www.wthinktank.org/>

Operational and delivery networks

Blockchain Alliance

Co-founded by Coin Center and the Chamber of Digital Commerce, this group seeks to protect public safety on the blockchain, detect and combat blockchain-related criminal activity and promote a long-term vision for regulatory efforts that do not stifle decentralized ledger technology innovation.

Decentralized Arbitration and Mediation Network (DAMN)

Launched by Key Solutions, DAMN is developing decentralized dispute resolution frameworks and an opt-in decentralized justice system designed and used by the blockchain community for commercial transactions. <https://forum.daohub.org/t/decentralized-arbitration-and-mediation-network/3062>

Ethereum

The Ethereum virtual machine is a decentralized platform for uploading and running programmes, conducting transactions, executing smart contracts and automating traditional processes like settlement, accounting and supply-chain tracking.

Enterprise Ethereum Alliance (EEA)

This consortium of Fortune 500 companies, cryptographers, academics and veteran Ethereum developers delivers protocols and standards for decentralized applications, interoperable across industries on the Ethereum blockchain.

Hyperledger Project (HLP)

Launched by the Linux Foundation, this project is creating open-source protocols and standards for blockchain interoperability across industries, platforms that developers can use to build applications for global business transactions.

Industrial Internet Consortium (IIC)

Co-founded by AT&T, Cisco, GE, IBM and Intel, this non-profit group seeks to identify requirements for open interoperability standards and common architectures across industries to connect physical and digital assets and capabilities on the industrial IoT. <http://www.iiconsortium.org>

R3CEV LLC (R3)

This consortium of banks and financial services firms is designing an open-source distributed ledger to record, manage and synchronize financial agreements securely, transparently and efficiently among financial institutions only.

Trusted IoT Alliance

Cisco Systems, Bosch, Foxconn Technology Group, Gemalto and several other companies have set up a consortium to develop a shared blockchain protocol for IoT and to secure and improve IoT applications.²⁰⁷ <https://github.com/Trusted-IoT-Alliance>

Policy networks

Australian Digital Currency Commerce Association (ADCCA)

ADCCA promotes industry best practices and consistent regulatory frameworks to shape the policy-making process and advocate for appropriate blockchain regulatory framework for FinTech businesses in Australia. <http://adcca.org.au/mission-statement/>

Coin Center

The center makes sure policy-makers understand the advantages of cryptocurrencies before issuing regulation. With the Uniform Law Commission (US), it drafted the “Model Regulation of Virtual Currency Business Act”. It has created a state digital currency regulation tracker. <https://coincenter.org>

Digital Assets Tax Policy Coalition

Formed by the Chamber of Digital Commerce and Steptoe and Johnson, this Washington DC-based coalition develops effective US tax policies for the growing virtual currency markets, policies that work for both industry and government.

Global Blockchain Forum (GBF)

This initiative of the Chamber of Digital Commerce promotes industry best practices and consistent regulatory frameworks across jurisdictions to shape blockchain regulation and coordinate advocacy around the world.

Smart Contracts Alliance (Chamber Working Group)

This initiative of the Chamber of Digital Commerce promotes acceptance and use of smart contract technologies by (a) developing policy related to smart contracts; (b) identifying best practices and advancing interoperability; and (c) engaging public policy-makers and regulators.

Advocacy networks

Bitcoin Foundation

Formed to standardize, protect and promote the development of the Bitcoin Core protocol, this non-profit, member-driven organization offers a range of resources: best practice guides, educational resources, meeting minutes, speaker's bureau, workshops and conferences. <https://bitcoinfoundation.org/>

Blockchain Association of Canada (BAC)

BAC supports employment growth and career opportunities in blockchain technologies. Its members speak at issue-based conferences in Canada and participate in discussions with the Canadian government on critical policy issues. <https://blockchainassociation.ca/>

Blockchain Trust Accelerator (New America and Bretton Woods II)

Co-founded by New America, the Bitfury Group and the National Democratic Institute, this initiative created a new business model for strategic capital ownership. Its model addresses the root causes of volatility.

Chamber of Digital Commerce (CDC)

CDC advocates for appropriate rather than oppressive regulation of cryptocurrencies and blockchain technologies. It represents diverse views in the blockchain space, acts as a reliable source of information for lawmakers and offers a suite of services in government affairs. <http://digitalchamber.org>

Global Blockchain Business Council (GBBC)

Founded by Bitfury, GBBC brings together the world's leading businesses and business leaders to highlight the latest innovations and advances in blockchain technology, advocates for its global adoption and provides a forum for education, collaboration and dialogue.

State Working Group

This initiative of the Chamber of Digital Commerce advocates for digital currencies and decentralized ledger technologies to US state and local governments and suggests appropriate state and local legal and regulatory requirements. <http://digitalchamber.org/initiatives/state-working-group/>

Wall Street Blockchain Alliance (WSBA)

This non-profit trade association speaks with such blockchain stakeholders as market participants, policy-makers and technology innovators, and produces reports of its findings. It also hosts Wall Street Education Day to educate the public and advance mainstream adoption.

Standards networks

Coalition for Automated Legal Applications (COALA)

COALA assembles domain experts, global institutions and leading academic research institutions to develop blockchain standards and applications enabling innovative legal and policy frameworks.

ColliderX

ColliderX is an open-source, crowdsourced and crowdfunded R&D hub for blockchain and adjacent technologies. It brings together academic researchers and open-source developers to compile and answer challenging technical questions from industry participants. Its approach will produce independent, impartial and peer-reviewed foundational research freely available to the ecosystem.

CryptoCurrency Certification Consortium (C4)

Co-founded by Andreas Antonopoulos and Vitalik Buterin, this non-profit organization certifies professionals who intend to offer cryptocurrency-related services. Those who have demonstrated proficiency receive Certified Bitcoin Professional designations. <https://cryptoconsortium.org>

CryptoCurrency Security Standard (CCSS)

Funded by C4, CCSS is an open standard that helps secure information systems that use cryptocurrencies. It has evolved into 32 controls for anyone building a new system on the blockchain. The standards cover the entire life cycle of the crypto private key usage in blockchain applications.

Digital Assets Accounting Consortium (DAAC)

This working group of the Chamber of Digital Commerce advocates for updated Generally Accepted Accounting Principles, practices and reporting standards for digital assets in collaboration with the Association of Independent Public Accountants and Financial Accounting Standards Board.

Institute for Innovation and Data Driven Design (ID3)

Affiliated with the MIT Media Lab, this non-profit organization develops and field-tests legal and software trust frameworks for data-driven services, infrastructures and enterprises.

International Securities Association for Institutional Trade Communication (ISITC) (Blockchain Working Group)

ISITC represents financial institutions and technology providers striving to improve the financial industry in Europe. Its blockchain working group is creating a list of benchmarks to help standardize blockchain tools. <https://isitc-europe.com/isitc-europe-blockchain-working-group/>

International Standards Organization (ISO)

This independent international NGO brings together experts from 164 national standards bodies to develop market-relevant international standards and support innovation.

ISO/TC 307 (ISO Initiative) (Blockchain Standards Committee)

ISO established three new technical committees (TCs) for developing international standards for decentralized ledger technologies: one for blockchain and electronic distributed ledger technologies, one for chain of custody and one for organizational governance.

World Wide Web Consortium (W3C) (Blockchain Community Group)

W3C hosts several decentralized community groups to develop standards, guidelines, software applications and protocols. Its blockchain community group is working on, for example, message format standards and guidelines for blockchain storage.

<https://www.w3.org/community/blockchain/>

Networked institutions

World Economic Forum

The World Economic Forum is an independent international organization committed to improving the state of the world by engaging all four pillars of society – business, political, academic and other civic leaders – to shape global, regional and industry agendas. <https://www.weforum.org>

Acknowledgements

The authors acknowledge the generous support of the World Economic Forum and the Blockchain Research Institute. In addition, the authors extend their heartfelt thanks to the people who generously shared their time and insights. In alphabetical order: Jeremy Allaire, Marc Andreessen, Gavin Andresen, Andreas Antonopoulos, Brian Behlendorf, Perianne Boring, Jerry Brito, Paul Brody, Richard Brown, Ethan Buchman, Vitalik Buterin, Bruce Cahan, Nicolas Cary, Vint Cerf, Ben Chan, Constance Choi, Timothy Cook Draper, Michael Cooper, Matthew Corallo, Primavera De Filippi, Adam Draper, Joshua Fairfield, Brian Forde, Vinay Gupta, Mike Hearn, Austin Hill, Joichi Ito, Eric Jennings, Izabella Kaminska, Andrew Keys, Joyce Kim, Chris Larsen, Benjamin Lawsky, Marcus Leef, Charlie Lee, Joseph Lubin, Adam Ludwin, Dino Mark Angaritis, Blythe Masters, Cindy McAdam, Jesse McWaters, Carlos Moreira, Patrick Murck, Anoop Nannra, Steve Omohundro, Jim Orlando, Lawrence Orsini, Jose Pagliery, Stephen Pair, Eric Piscini, Keonne Rodriguez, Elizabeth Rossiello, Matthew Roszak, Richard Samans, Kirsten Sandberg, Marco Santori, Barry Silbert, George Small, Jamie Elizabeth Smith, Thomas Spaas, Balaji Srinivasan, Elizabeth Stark, Jutta Steiner, Lynne St. Amour, Nick Szabo, Bob Tapscott, Peter Todd, David B. Treat, Jason Tyra, Iliana Oris Valiente, Valery Vavilov, Andrew Vegetabile, Roger Ver, Erik Voorhees, Joseph Weinberg, Zooko Wilcox-O’Hearn, Carolyn Wilkins, Cameron Winklevoss, Tyler Winklevoss, Jeremy Wilson, Pindar Wong and Aaron Wright.

Notice

We have obtained the information in this report from sources we believe to be reliable and accurate. However, we have not independently verified information from third-party sources. We make no representation or warranty, express or implied, as to its accuracy or completeness. In addition, the statements in this report may provide current expectations of future events based on certain assumptions and include any statement that does not directly relate to a historical fact or a current fact. These statements involve known and unknown risks, uncertainties and other factors that are not exhaustive. The individuals and companies contributing to this report operate in a constantly changing environment and new risks emerge continually. We caution readers not to place undue reliance on these statements. The individuals or companies contributing to this report undertake no obligation to revise or update publicly any statements, whether as a result of new information, future events or otherwise; they shall in no event be liable for any loss or damage arising in connection with the use of the information in this report.

The Tapscott Group, Toronto, June 2017

© 2017 – All rights reserved.

All rights reserved. No one may reproduce, store in a retrieval system or transmit any part of this publication in any form or by any means, electronic, mechanical, photocopying or otherwise without the prior permission of the Tapscott Group.

Endnotes

- 1 The Fourth Industrial Revolution is a concept developed by Klaus Schwab and the World Economic Forum. <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>
- 2 Global Solution Networks Program. A programme conducted by The Tapscott Group for the Rotman School of Management, 2014-2016. <http://gsnetworks.org/>, accessed 20 June 2017.
- 3 Global Solution Networks. <http://gsnetworks.org/>, accessed 20 June 2017.
- 4 Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". www.bitcoin.org, 1 November 2008. www.bitcoin.org/bitcoin.pdf, accessed 20 June 2017.
- 5 Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". www.bitcoin.org, 1 November 2008. www.bitcoin.org/bitcoin.pdf, accessed 20 June 2017.
- 6 Interview with Paul Brody, 7 July 2015. Updated via email from Brody, 16 June 2017.
- 7 David D. Clark. "A Cloudy Crystal Ball", presentation, IETF, 16 July 1992. http://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf, accessed 20 June 2017.
- 8 Don Tapscott and Lynne St. Amour. "The Remarkable Internet Governance Network – Part I" Global Solution Networks Program, Martin Prosperity Institute, University of Toronto, 2014.
- 9 Internet & Jurisdiction. www.Internetjurisdiction.net, accessed 17 May 2017.
- 10 InternetPolicyPlatform.org; Timothy Karr. "17 Organizations Release 2016 Internet Policy Platform". 13 June 2016. <https://www.freepress.net/press-release/107452/17-organizations-release-2016-Internet-policy-platform>, accessed 17 May 2017.
- 11 Industrial Internet Consortium. www.iiconsortium.org, accessed 17 May 2017.
- 12 Electronic Frontier Foundation. <https://www.eff.org/about>, accessed 17 May 2017.
- 13 Internet Society. "Policy & Development". <http://www.Internetsociety.org/who-we-are/related-and-partner-organisations/our-community-and-partners>, accessed 17 May 2017.
- 14 "Online governance. Lost in the splinternet". *The Economist*. 5 November 2016.
- 15 Interview with Joichi Ito, 1 May 2017.
- 16 Matthew Roszak. Written statement prepared for the Committee on Energy and Commerce of the United States House of Representatives. 16 March 2016. <http://docs.house.gov/meetings/if/if17/20160316/104677/hrg-114-if17-wstate-roszakm-20160316.pdf>, accessed 15 June 2017.
- 17 Interview with Joichi Ito, 24 August 2015.
- 18 Email from Primavera De Filippi, 24 May 2017.

- 19 TheStreet. "Hong Kong's monetary authority unveils trade finance platform based on blockchain technology". *South China Morning Post*. TheStreet.com. 30 March 2017. <https://www.thestreet.com/story/14065398/2/hong-kongs-monetary-authority-unveils-trade-finance-platform-based-on-bitcoin-tech.html>, accessed 27 May 2017.
- 20 Interview with Jesse McWaters, 10 May 2017. Edited by McWaters via email, 19 June 2017.
- 21 Email from Perianne Boring, 26 May 2017.
- 22 Alex Sunnarborg. "Survey: Enthusiasm for Ethereum Hit an All-Time High in Q1". <http://www.coindesk.com/charts-enthusiasm-ethereum-hit-time-high-q1/>, accessed 20 June 2017.
- 23 Interview with Brian Forde, 26 June 2015.
- 24 Interview with Joichi Ito, 1 May 2017.
- 25 Matthew Roszak. Written statement prepared for the Committee on Energy and Commerce of the United States House of Representatives. 16 March 2016. <http://docs.house.gov/meetings/if/if17/20160316/104677/hrg-114-if17-wstate-roszakm-20160316.pdf>, accessed 15 June 2017.
- 26 Interview with Stephen Pair, 11 June 2015.
- 27 Roger Ver. @rogerkver. www.Twitter.com. 22 April 2017. <https://twitter.com/rogerkver/status/855793613711618049>, accessed 29 May 2017.
- 28 Philip Francis @philfrancis77. Reply to @rogerkver. www.twitter.com. 22 April 2017. <https://twitter.com/philfrancis77/status/855797290476417026>, accessed 29 May 2017.
- 29 Adam Back. @adam3us. Reply to @theonevortex @alansilbert. www.twitter.com. 22 April 2017. <https://twitter.com/adam3us/status/855828660363776000>, accessed 29 May 2017.
- 30 Roger Ver. @rogerkver. www.Twitter.com. 22 April 2017. <https://twitter.com/rogerkver/status/855842827606962176>, accessed 29 May 2017.
- 31 Interview with Brian Forde, 26 June 2015.
- 32 Daniel Palmer. "Scalability Debate Continues as Bitcoin XT Proposal Stalls". CoinDesk LLC. 11 January 2016. <http://www.coindesk.com/scalability-debate-bitcoin-xt-proposal-stalls/>, accessed 27 May 2017.
- 33 Interview with Gavin Andresen, 8 June 2015.
- 34 Oscar Williams-Grut and Rob Price. "A Bitcoin civil war is threatening to tear the digital currency in 2". BusinessInsider.com. 26 March 2017. <http://www.businessinsider.com/bitcoins-hard-fork-bitcoin-unlimited-segregated-witness-explained-2017-3>, accessed 16 May 2017; JP Buntinx. "Bitcoin Core vs Bitcoin Unlimited". *The Merkle*. 19 March 2017. <https://themerke.com/bitcoin-core-vs-bitcoin-unlimited/>, accessed 27 May 2017.
- 35 Sergio Demian Lerner. "[bitcoin-dev] Segwit2Mb – combined soft/hard fork – Request for Comments". Linux Foundation. 31 March 2017. <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-March/013921.html>, accessed 2 June 2017.
- 36 Digital Currency Group. "Bitcoin Scaling Agreement at Consensus 2017." www.medium.com. 23 May 2017. <https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77>, accessed 2 June 2017.
- 37 Pete Rizzo and Alyssa Hertig. "Bitcoin's New Scaling 'Agreement': The Reaction." CoinDesk LLC. 24 May 2017. <http://www.coindesk.com/bitcoins-new-scaling-agreement-reaction/>, accessed 2 June 2017. See this excellent CoinDesk summary for quotations from Samson Mow, Matthew Corallo, Jeff Garzik and Erik Voorhees.
- 38 Email from Jamie Elizabeth Smith, 1 June 2017.
- 39 Email from Stephen Pair, 16 June 2017.
- 40 Ryan X. Charles. @ryanxcharles. Verified account. Twitter.com. 8 April 2017. <https://twitter.com/ryanxcharles/status/850785821443620865>, accessed 24 May 2017.
- 41 Joël Valenzuela. "Secret Bitcoin Troll Army Pushes for SegWit Adoption: Emin Gun Sirer." CoinTelegraph.com. 12 April 2017. <https://cointelegraph.com/news/secret-bitcoin-troll-army-pushes-for-segwit-adoption-emin-gun-sirer>, accessed 27 May 2017.
- 42 Jameson Lopp. @lopp. Verified account. Twitter.com. 8 April 2017. <https://twitter.com/lopp/status/850788612673331201>, accessed 24 May 2017.
- 43 Ryan X. Charles. @ryanxcharles. Verified account. Twitter.com. 8 April 2017. <https://twitter.com/ryanxcharles/status/850603618243923968>, accessed 24 May 2017.
- 44 Jameson Lopp. @lopp. Verified account. Twitter.com. 8 April 2017. <https://twitter.com/lopp/status/850790778402213890>, accessed 24 May 2017. Punctuation edited for consistency with report.
- 45 Ryan X. Charles. @ryanxcharles. Verified account. Twitter.com. 8 April 2017. <https://twitter.com/ryanxcharles/status/850791057340026880>, accessed 24 May 2017.
- 46 Zooko Wilcox-O'Hearn. @zooko. Twitter.com. 8 April 2017. <https://twitter.com/zooko/status/850795487766642689>, accessed 24 May 2017.
- 47 Zooko Wilcox-O'Hearn. @zooko. Twitter.com. 8 April 2017. <https://twitter.com/zooko/status/850795692977254400>, accessed 24 May 2017. Punctuation edited for consistency with report.
- 48 John Light. @lightcoin. Twitter.com. 8 April 2017. <https://twitter.com/lightcoin/status/850797274837995520>, accessed 24 May 2017.
- 49 Wladimir J. van der Laan. @orionwl. Twitter.com. 8 April 2017. <https://twitter.com/orionwl/status/850963439468113920>, accessed 24 May 2017.
- 50 Wladimir J. van der Laan. @orionwl. Twitter.com. 8 April 2017. <https://twitter.com/orionwl/status/850964225577152512>, accessed 24 May 2017.
- 51 Ryan X. Charles. @ryanxcharles. Verified account. Twitter.com. 9 April 2017. <https://twitter.com/ryanxcharles/status/851090319470845953>, accessed 24 May 2017.
- 52 Zooko Wilcox-O'Hearn. @zooko. Twitter.com. 9 April 2017. <https://twitter.com/zooko/status/851137975257899010>, accessed 24 May 2017. Quotation marks edited for consistency with style. All other punctuation marks are the author's.
- 53 Matthew Corallo. @TheBlueMatt. Twitter.com. 9 April 2017. <https://twitter.com/TheBlueMatt/status/851138900475076608>, accessed 24 May 2017.
- 54 Zooko Wilcox-O'Hearn. @zooko. Twitter.com. 9 April 2017. <https://twitter.com/zooko/status/851217435483148288>, and <https://twitter.com/zooko/status/851217601879564288>, accessed 24 May 2017.

- 55 Matthew Corallo. @TheBlueMatt. Twitter.com. 9 April 2017. <https://twitter.com/TheBlueMatt/status/851218049482883072>, <https://twitter.com/TheBlueMatt/status/851218283126599680> and <https://twitter.com/TheBlueMatt/status/851218609095430145>, accessed 24 May 2017.
- 56 Daniel Robert Plante. @Daniel_Plante. Twitter.com. 10 April 2017. https://twitter.com/Daniel_Plante/status/851661157538463744, accessed 24 May 2017.
- 57 Email from Primavera De Filippi, 24 May 2017.
- 58 Peter Todd. "Re: [Bitcoin-development] Fwd: Block Size Increase Requirements". *The Mail Archive*, 1 June 2015. www.mail-archive.com/pk4ordw, <http://tinyurl.com/pk4ordw>, accessed 26 August 2015.
- 59 Satoshi Nakamoto. "Re: Bitcoin P2P e-cash paper". Email posted to listserv. 17 November 2008, 09:04:47 -0800. Mailing List. *Cryptography*. Metzger, Dowdeswell & Co. LLC. www.mail-archive.com/cryptography%40metzdowd.com/msg10006.html, accessed 13 July 2015.
- 60 Pascal Bouvier. "Distributed Ledgers Part I: Bitcoin Is dead". *FiniCulture* blog, 4 August 2015. <http://finiculture.com/distributed-ledgers-part-i-bitcoin-is-dead/>, accessed 28 August 2015.
- 61 Interview with Austin Hill, 22 July 2015.
- 62 Interview with Gavin Andresen, 8 June 2015.
- 63 Izabella Kaminska. "Bitcoin's Wasted Power – and How It Could Be Used to Heat Homes". *FT Alphaville*, *Financial Times*, 5 September 2014.
- 64 CIA. "The World Factbook". www.cia.gov, 2012. <http://tinyurl.com/hoxwvle>, accessed 28 August 2015. Note that Cyprus's carbon gas emissions in the same period were 8.801 million metric megatons (2012).
- 65 Nathan Schneider. "After the Bitcoin Gold Rush". *The New Republic*, 25 February 2015. www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle, accessed 15 May 2015.
- 66 Interview with Bob Tapscott, 28 July 2015.
- 67 Interview with Gavin Andresen, 8 June 2015.
- 68 Jamie Redman. "Bitcoin Network Hashrate Surpasses Four Exahash per Second." www.bitcoin.com. 8 May 2017. <https://news.bitcoin.com/bitcoin-hashrate-four-exahash-per-second/>, accessed 2 June 2017.
- 69 Interview with Gavin Andresen, 8 June 2015.
- 70 Interview with Eric Jennings, 10 July 2015.
- 71 Interview with Valery Vavilov, 24 July 2015.
- 72 Hass McCook. "Under the Microscope: Economic and Environmental Costs of Bitcoin Mining." CoinDesk Ltd. 21 June 2014. www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining/, accessed 28 August 2015.
- 73 MRI e-cycle solutions. "PC Recycling." MRI of Australia. <https://mri.com.au/recycling/pc-recycling/>, accessed 20 June 2017.
- 74 Don Tapscott and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Toronto: Penguin Random House, 2016.
- 75 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 76 Interview with Vitalik Buterin, 9 April 2017.
- 77 Interview with Vitalik Buterin, 9 April 2017.
- 78 CryptoCompare. "The DAO, The Hack, The Soft Fork and The Hard Fork." 20 April 2017. <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>, accessed 17 May 2017.
- 79 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 80 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 81 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 82 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 83 Andrew Vegetabile, "An objective look into the impacts of forking blockchains due to malicious actors". Digital Currency Council, 9 July 2015. www.digitalcurrencycouncil.com/professional/an-objective-look-into-the-impacts-of-forking-blockchains-due-to-malicious-actors/, accessed 20 June 2017.
- 84 Vitalik Buterin. "Proof of Stake: How I Learned to Love Weak Subjectivity." Ethereum blog. 25 November 2014. <https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>, accessed 20 June 2017.
- 85 Herman Schoenfeld. "Fundamental problems with Casper." www.reddit.com. 15 April 2016. https://www.reddit.com/r/ethereum/comments/4euiut/fundamental_problems_with_casper/?st=j37y6mom&sh=5b2ef60e, accessed 27 May 2017; Jonesyjonesy. "Vlad Zamfir said it's a reasonable possibility Casper won't be implemented on Ethereum...is this cause for concern?" www.reddit.com. 25 May 2017. https://www.reddit.com/r/ethereum/comments/6dcs4x/vlad_zamfir_said_it_s_a_reasonable_possibility/?st=j380dpnr&sh=214cc1b6, accessed 27 May 2017.
- 86 Vlad Zamfir. "Introducing Casper 'the Friendly Ghost'". <https://blog.ethereum.org/>. 1 August 2015. <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>, accessed 27 May 2017.
- 87 Vlad Zamfir. @VladZamfir. www.Twitter.com. 25 May 2017. <https://twitter.com/VladZamfir/status/867768810278760449>, <https://twitter.com/VladZamfir/status/867769067838492677> and <https://twitter.com/vladzamfir/status/867769305303097345>, accessed 27 May 2017.
- 88 Vitalik Buterin, Verified account. @VitalikButerin. www.Twitter.com. 25 May 2017. <https://twitter.com/VitalikButerin/status/867870378974035968>, accessed 29 May 2017.
- 89 Vlad Zamfir. @VladZamfir. www.Twitter.com. 26 May 2017. <https://twitter.com/VladZamfir/status/867978070279430145>, accessed 29 May 2017.
- 90 MikeinSpace. @MikeinSpace. www.Twitter.com. 25 May 2017. <https://twitter.com/mikeinspace/status/867872553003601921>, accessed 27 May 2017.
- 91 Interview with Austin Hill, 22 July 2015.
- 92 Email from Ethan Buchman. 20 May 2017.
- 93 Email from Ethan Buchman. 20 May 2017.
- 94 Tendermint. "Tendermint vs. Other Software". <https://tendermint.com/intro/tendermint-vs-x>, accessed 24 May 2017.

- 95 Rebecca Campbell. "Tendermint Wins Innovation Award and Announces Cosmos at International Blockchain Week". *Bitcoin Magazine*. 23 September 2016. <https://bitcoinmagazine.com/articles/tendermint-wins-innovation-award-and-announces-cosmos-at-international-blockchain-week-1474657507/>, accessed 29 May 2017.
- 96 Email from Ethan Buchman. 20 May 2017.
- 97 Cosmos. "Fundraiser Was a Resounding Success". Announcement. Cosmos Network. 6 April 2017. <https://cosmos.network/blog/fundraiser-was-a-resounding-success>, accessed 27 May 2017.
- 98 Email from David B. Treat, 17 May 2017.
- 99 Interview with Brian Behlendorf, 2 May 2017.
- 100 Interview with Brian Behlendorf, 2 May 2017.
- 101 "Hyperledger Project Charter." The Linux Foundation. 22 January 2016. www.hyperledger.org/about/charter, accessed 17 May 2017.
- 102 Casey Kuhman. "Why We're Joining Hyperledger." *Monax. Monax Industries*, 28 February 2017. <https://monax.io/blog/2017/02/28/why-were-joining-hyperledger/>, accessed 17 May 2017.
- 103 Interview with Brian Behlendorf, 2 May 2017.
- 104 Interview with Jesse McWaters, 10 May 2017.
- 105 Ken Griffith and Ian Grigg. "Bitcoin Verification Latency: The Achilles Heel for Time Sensitive Transactions". White Paper, 3 February 2014. <http://iang.org/papers/BitcoinLatency.pdf>, accessed 20 July 2015.
- 106 Interview with Brian Behlendorf, 2 May 2017.
- 107 Interview with Joichi Ito, 1 May 2017.
- 108 Interview with Brian Behlendorf, 2 May 2017.
- 109 Matthew Roszak. Written statement prepared for the Committee on Energy and Commerce of the United States House of Representatives. 16 March 2016. <http://docs.house.gov/meetings/if/if17/20160316/104677/hrg-114-if17-wstate-roszakm-20160316.pdf>, accessed 15 June 2017.
- 110 Andreas Antonopoulos. @aantonop. Verified account. [www.Twitter.com. 27 May 2017. https://twitter.com/aantonop/status/868400899340632066](https://twitter.com/aantonop/status/868400899340632066), accessed 29 May 2017.
- 111 Evily. @veryevilone. [www.Twitter.com. 27 May 2017. https://twitter.com/veryevilone/status/868409998036131840](https://twitter.com/veryevilone/status/868409998036131840), accessed 29 May 2017.
- 112 Andreas Antonopoulos. @aantonop. Verified account. [www.Twitter.com. 27 May 2017. https://twitter.com/aantonop/status/868455632650686464](https://twitter.com/aantonop/status/868455632650686464), accessed 29 May 2017.
- 113
- 114 Email from Primavera De Filippi, 24 May 2017.
- 115 Email from Karen Gifford, 19 June 2017.
- 116 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 117 Bilaji S. Srinivasan. "Thoughts on Tokens." [medium.com. 27 May 2017. https://medium.com/@balajis/thoughts-on-tokens-436109aabcbe](https://medium.com/@balajis/thoughts-on-tokens-436109aabcbe), accessed 1 June 2017.
- 118 Interview with Blythe Masters, 29 July 2015.
- 119 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 120 Email from Perianne Boring, 26 May 2017.
- 121 Bailey Reutzel. "Where is Gavin Andresen? The Quiet Exile of Bitcoin's Former Face." www.coindesk.com. 19 May 2017. <http://www.coindesk.com/where-is-gavin-andresen-the-quiet-exile-of-bitcoins-former-face/>, accessed 21 May 2017.
- 122 Interview with Brian Behlendorf, 2 May 2017.
- 123 Interview with Tyler Winklevoss, 9 June 2015. Edited by T. Winklevoss via email, 16 June 2017.
- 124 Email from Primavera De Filippi, 24 May 2017.
- 125 Email from Primavera De Filippi, 24 May 2017.
- 126 Primavera De Filippi and Aaron Wright, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," *Social Sciences Research Network*, 10 March 2015, 43.
- 127 Interview with Josh Fairfield, 1 June 2015.
- 128 Interview with John Fairfield, 1 June 2015.
- 129 Interview with Josh Fairfield, 1 June 2015.
- 130 Interview with Benjamin Lawsky, 2 July 2015.
- 131 Interview with Benjamin Lawsky, 2 July 2015.
- 132 Interview with Benjamin Lawsky, 2 July 2015.
- 133 Matthew Roszak. Written statement prepared for the Committee on Energy and Commerce of the United States House of Representatives. 16 March 2016. <http://docs.house.gov/meetings/if/if17/20160316/104677/hrg-114-if17-wstate-roszakm-20160316.pdf>, accessed 15 June 2017.
- 134 Interview with Jerry Brito, 29 June 2015.
- 135 Interview with Jerry Brito, 29 June 2015.
- 136
- 137 Anne Shields. "Which Microsoft Computers Were Affected Most by WannaCry?" *Market Realist*. 23 May 2017. <http://marketrealist.com/2017/05/which-microsoft-computers-were-affected-most-by-wannacry/>; Jonathan Berr. "'WannaCry' ransomware attack losses could reach \$4 billion." *MONEYWATCH*. CBS News. 16 May 2017. <http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>, both accessed 30 May 2017.
- 138 Interview with Izabella Kaminska, 5 August 2015.
- 139 Interview with Izabella Kaminska, 5 August 2015.
- 140 OpenMIC. *Breaking the Mold: Investing in Racial Diversity in Tech. A Report for Investors*. February 2017. <http://breakingthemold.openmic.org/>, accessed 17 June 2017.
- 141 Alberto Felice De Toni and Giovanni De Zan. "The complexity dilemma: Three tips for dealing with complexity in organizations". *Emergence: Complexity and Organization No. 3-4 (2016): H1, December 2016*.
- 142
- 143 Alessia Camera. @alessia_camera. [www.twitter.com. 25 May 2017. https://twitter.com/alessia_camera/status/867679046443945984](https://twitter.com/alessia_camera/status/867679046443945984), accessed 29 May 2017.
- 144 Julia B. Bear and Anita Williams Woolley. "The Role of Gender in Team Collaboration and Performance". *Interdisciplinary Science Reviews*, Vol. 36, No. 2: 146–153, June 2011.; Sally Helgesen. *The Female Advantage: Women's Ways of Leadership*. New York, NY. Doubleday, 1990; Sylvia Ann Hewlett, Melinda Marshall and Laura Sherbin. "How Diversity Can Drive Innovation". *Harvard Business Review* 91, No. 12: 30, December 2013.
- 145 Andrew Vegetabile. "An objective look into the impacts of forking blockchains due to malicious actors". Digital Currency Council, 9 July 2015. www.digitalcurrencycouncil.com/professional/an-objective-look-into-the-impacts-of-forking-blockchains-due-to-malicious-actors/, accessed 20 June 2017.

- 146 Interview with Keonne Rodriguez, 11 May 2015.
- 147 Telephone interview with Steve Omohundro, 28 May 2015.
- 148
- 149 Email from Perianne Boring, 26 May 2017.
- 150 Interview with Jim Orlando, 28 September 2015.
- 151 PricewaterhouseCoopers. *Global FinTech Report 2017*. <https://www.pwc.com/jg/en/publications/pwc-global-fintech-report-17.3.17-final.pdf>, accessed 30 May 2017.
- 152 Email correspondence with Tim Draper, 3 August 2015.
- 153 PricewaterhouseCoopers. *Global FinTech Report 2017*. <https://www.pwc.com/jg/en/publications/pwc-global-fintech-report-17.3.17-final.pdf>, accessed 30 May 2017.
- 154 Bailey Reutzel. "Where is Gavin Andresen? The Quiet Exile of Bitcoin's Former Face." www.coindesk.com. 19 May 2017. <http://www.coindesk.com/where-is-gavin-andresen-the-quiet-exile-of-bitcoins-former-face/>, accessed 21 May 2017.
- 155 Interview with Gavin Andresen, 8 June 2015.
- 156 Interview with Gavin Andresen, 8 June 2015.
- 157 Bailey Reutzel. "Where is Gavin Andresen? The Quiet Exile of Bitcoin's Former Face". www.coindesk.com. 19 May 2017. <http://www.coindesk.com/where-is-gavin-andresen-the-quiet-exile-of-bitcoins-former-face/>, accessed 21 May 2017.
- 158 Interview with Joichi Ito, 24 August 2015.
- 159 Justin OConnell. "More US Colleges & Universities Offering Bitcoin Courses In The Fall". 27 August 2015. www.cryptocoinsnews.com/us-colleges-universities-offering-bitcoin-courses-fall/, accessed 20 June 2017.
- 160 Interview with Jerry Brito, 29 June 2015.
- 161 Interview with Benjamin Lawsky, 2 July 2015.
- 162 Stan Higgins. "Bank of England Economist Proposes National Digital Currency". 18 September 2015. www.coindesk.com/bank-of-england-economist-digital-currency/, accessed 20 June 2017.
- 163 Alexandra Perry. "Is Russia the Reason Ethereum Is Climbing?" 5 June 2017. *Wealth Daily*. <https://www.wealthdaily.com/articles/is-russia-the-reason-ethereum-is-climbing-why-is-ethereum-rising/8708>, accessed 12 June 2017.
- 164 Interview with Adam Draper, 31 May 2015.
- 165 Email correspondence with Vint Cerf, 12 June 2015.
- 166 W3C. "Web Payments at W3C". www.w3.org/Payments/, accessed 21 June 2017.
- 167 "No. 238 Bitcoin, Blockchain and Beyond: FLASH HELP!" www.intgovforum.org/cms/wks2015/index.php/proposal/view_public/239, accessed 20 June 2017.
- 168 Interview with Izabella Kaminska, 5 August 2015.
- 169 Interview with Pindar Wong, 7 April 2017.
- 170 "Online governance. Lost in the splinternet". *The Economist*. 5 November 2016.
- 171 Interview with Roger Ver, 30 April 2015.
- 172 Interview with Gavin Andresen, 8 June 2015.
- 173
- 174 Email from Primavera De Filippi, 24 May 2017.
- 175 Email from Iliana Oris Valiente, 16 June 2017.
- 176 Email from Perianne Boring, 26 May 2017.
- 177 Interview with Joseph Lubin, 3 May 2017.
- 178 Interview with Jesse McWaters, 10 May 2017.
- 179 Email from George Small, 31 May 2017.
- 180 Email from George Small, 31 May 2017.
- 181 World Economic Forum. *Deep Shift: Technology Tipping Points and Societal Impact*. September 2015. http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf, 7, accessed 20 June 2017.
- 182 Interview with Perianne Boring at Money 2020, 26 October 2015.
- 183 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 184 Interview with Elizabeth Rossiello, 15 May 2017.
- 185 Interview with Jerry Brito, 29 June 2015.
- 186 Interview with Jerry Brito, 29 June 2015.
- 187 Email from Jerry Brito, 14 June 2017.
- 188 Chamber of Digital Chamber. "Dear G7, Bitcoin is Already Highly Regulated". Press release. 19 November 2015. <http://digitalchamber.org/assets/press-release---g7---for-website.pdf>, accessed 20 June 2017.
- 189 Interview with Carolyn Wilkins, 27 August 2015.
- 190 Interview with Elizabeth Rossiello, 15 May 2017.
- 191 Email from Primavera De Filippi, 24 May 2017.
- 192 Email from Primavera De Filippi, 24 May 2017.
- 193 Chamber of Digital Commerce. www.digitalchamber.org/, accessed 21 June 2017.
- 194 Email from Perianne Boring, 26 May 2017.
- 195 Email from source who wrote on condition of anonymity, 30 May 2017.
- 196 Email from Jamie Elizabeth Smith, 1 June 2017.
- 197 Email from Primavera De Filippi, 24 May 2017.
- 198 Interview with Tyler Winklevoss, 9 June 2015.
- 199 Email from Primavera De Filippi, 24 May 2017.
- 200 Interview with Joichi Ito, 1 May 2017.
- 201 Interview with Joichi Ito, 1 May 2017.
- 202 Interview with Joichi Ito, 1 May 2017.
- 203 Email from Karen Gifford on behalf of Chris Larsen, 19 June 2017.
- 204 Interview with Joichi Ito, 24 August 2015.
- 205 Coalition of Automated Legal Applications. http://coala.global/?page_id=13396, accessed 21 May 2017.
- 206 Interview with Joseph Lubin, 3 May 2017. Edited by Lubin via email, 16 June 2017.
- 207 Anna Irrera, "Bosch, Cisco, BNY Mellon, others launch new blockchain consortium," [www.Reuters.com](http://www.reuters.com). 27 January 2017. <http://www.reuters.com/article/us-blockchain-iot-idUSKBN15B2D7>, accessed 16 June 2017.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org