

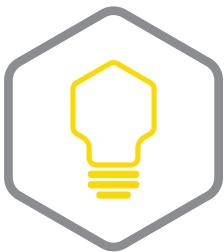
THE LION, THE UNICORN, AND THE CROWN

**Striking a Balance between Regulation
and Blockchain Innovation**

Joel Telpner
Sullivan & Worcester LLP

May 2018





Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, “the digital economy,” with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

In 2017, Don and Alex Tapscott launched the Blockchain Research Institute to help realize the new promise of the digital economy. We research the strategic implications of blockchain technology and produce practical insights to contribute global blockchain knowledge and help our members navigate this revolution.

Our findings, conclusions, and recommendations are initially proprietary to our members and ultimately released to the public in support of our mission. To find out more, please visit www.blockchainresearchinstitute.org.



Blockchain Research Institute, 2018

Except where otherwise noted, this work is copyrighted 2018 by the Blockchain Research Institute and licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License. To view a copy of this license, send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA, or visit creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

This document represents the views of its author(s), not necessarily those of Blockchain Research Institute or the Tapscott Group. This material is for informational purposes only; it is neither investment advice nor managerial consulting. Use of this material does not create or constitute any kind of business relationship with the Blockchain Research Institute or the Tapscott Group, and neither the Blockchain Research Institute nor the Tapscott Group is liable for the actions of persons or organizations relying on this material.

Users of this material may copy and distribute it as is under the terms of this Creative Commons license and cite it in their work. This document may contain material (photographs, figures, and tables) used with a third party's permission or under a different Creative Commons license; and users should cite those elements separately. Otherwise, we suggest the following citation:

Joel S. Telpner, “The Lion, the Unicorn, and the Crown: Striking a Balance between Regulation and Blockchain Innovation,” foreword by Don Tapscott, Blockchain Research Institute, 10 May 2018.

To request permission for remixing, transforming, building upon the material, or distributing any derivative of this material for any purpose, please contact the Blockchain Research Institute, [www.blockchainresearchinstitute.org/contact-us](http://blockchainresearchinstitute.org/contact-us), and put “Permission request” in subject line. Thank you for your interest!



Contents

Foreword 3

Idea in brief 5

Introduction 6

Is the blockchain beyond traditional concepts of law and regulation? 7

Does the nature of blockchain obviate traditional regulation? 9

Is self-governance the solution? 10

Law versus norms 12

Lessons from the Internet and financial markets 12

Regulating the Internet, a convergence of computing and communications 12

Regulating banks, exchanges, and financial institutions 17

Finding a better way 22

Understanding the core features of blockchain technology 22

The blockchain is jurisdictionally agnostic 22

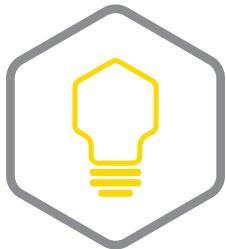
Start-ups can push existing players aside 25

Smart contracts fulfill the trustless component of the blockchain 26

Disintermediation and the blockchain are synonymous 30

Change is constant 31

A regulatory approach: Ask fundamental questions	33
Does the use of the technology raise truly novel legal issues?	33
What is the “it” that we are potentially regulating?	34
Do or should existing laws apply to blockchain technology?	40
Will existing laws have the same effect on new technology?	41
What are the costs and benefits of new or special regulation?	47
Whose law should apply?	48
A modest proposal: Follow these regulatory principles	49
Match as best as possible regulatory implementation to technology evolution	50
Focus on buy-in and identify new ways to achieve existing goals	52
Target the use and the user, not the blockchain itself	53
Use a flexible, yet strong (even threatening) approach	54
Play in the sandbox	56
Collaborate internationally and coordinate national agencies	57
Minimize unintended consequences	58
Pathway forward	59
About the author	62
About the Blockchain Research Institute	63
Notes	64



Foreword

Blockchain Research Institute members know the power of blockchain technology and the many groundbreaking ways in which it is being deployed. Together we show leadership in driving this innovation forward—but as leaders, we also have responsibility to steward the technology so that it becomes a driver of social good. When developing regulations, we need to balance protecting the public with encouraging inventors and fueling innovation.

Given how the business models and practices of firms such as Facebook on one hand and Wells Fargo on the other have eroded the trust of consumers as well as their government representatives, no one is buying the “just trust us” strategy. That so many organizations, jurisdictions, and industry groups are involved makes regulation even more challenging.

This project investigates the challenges—the key issues, trade-offs, and future scenarios related to blockchain and regulation. The research is thorough, and its presentation is accessible to those with a solid understanding of the space. It shows us a way forward while reminding us of the dangers of unintended consequences.

We knew that this project would require a very smart author with deep, diverse expertise. We were pleased to recruit Joel Telpner, who moderated a standing-room-only panel on the regulation of initial coin offerings at Blockchain Central, sponsored by the Global Blockchain Business Council in Davos, Switzerland, to coincide with the annual meeting of the World Economic Forum.¹ He is one of the top legal minds in the blockchain space and draws on his experience as a lawyer, strategist, venture capitalist, and thought leader.

As Joel put “fingers to keyboard” to describe the regulatory puzzlers dotting the blockchain landscape, the metaphors of a quite famous and fittingly pseudonymous mathematician—Lewis Carroll—came to mind. Carroll’s tale of “The Lion and the Unicorn,” for example, describes how these two creatures do battle over the kingdom on the other side of the looking glass. Carroll depicts the fearless felix of the forest as a drowsy doyen whom the cocky unicorn has just run through with his horn. Even in Carroll’s day, incumbent leaders had trouble recognizing the threat of unusual upstarts.

Both the lion and the unicorn look with wonder at the everyday Alice. The lion asks whether she’s “animal—vegetable—or mineral,” and the unicorn calls her a “fabulous monster.” As she struggles to cut a plum-cake with a knife—the knife isn’t “cutting it” as far as cake-cutting technology goes—both of the creatures complain about her use of the tool.

Most illuminating, however, is Carroll’s depiction of the king, over whose crown the lion and the unicorn are fighting. The king is feeble and his eyesight weak; he can’t see down the road. One of his messengers has strong “Anglo-Saxon attitudes,” which get “more extraordinary every moment, while [his] great eyes [roll] wildly from side to side”; and the other messenger has just been released from prison.



The king finds the battle over his kingdom highly amusing, whereas Alice is more bemused by the lion and the unicorn's fight. She ventures to clarify:

"Fighting for the crown?"

"Yes, to be sure," said the King: "and the best of the joke is, that it's my crown all the while!"

"Does—the one—that wins—get the crown?" she asked.

"Dear me, no!" said the King. "What an idea!"²

Even so, the king is aware of his predicament, "evidently very uncomfortable at having to sit down between the two great creatures; but there was no other place for him." In such a world, weak rulers are happy to watch strong rivals attack each other. In Joel's world, which is the world of the Blockchain Research Institute, all parties—the lion, the unicorn, and the crown as well as Alice—have seats at the table and voices in the conversation.

Joel's work really captures that down-the-rabbit-hole feeling of all stakeholders as they make sense of this nascent technology in business and society. He raises the questions that they should be exploring together. I hope everyone enjoys it as much as I did.



DON TAPSCOTT

*Co-Founder and Executive Chairman
Blockchain Research Institute*

The Lion and the Unicorn were fighting for the crown:
The Lion beat the Unicorn all round the town.
Some gave them white bread, some gave them brown;
Some gave them plum-cake and drummed them out of town.³



"The Lion and the Unicorn," Lewis Carroll, Through the Looking Glass: and What Alice Found There, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 152. No known copyright restrictions.



Idea in brief

Blockchain development and implementation are happening at a pace well beyond the capacity of regulators to respond, in many ways mirroring our experience with the Internet—but with one critical difference—speed.

- » The blockchain is disruptive innovation. On a daily basis, brilliant minds from all corners of the planet are announcing new ways to use blockchain technology to completely upend the old ways in which human beings interact and engage in commerce.
- » Disruptive innovation presents significant regulatory challenges. With its global footprint, blockchain technology does not recognize existing jurisdictional boundaries. Innovators pooh-pooh any notion that blockchain's distributed applications can be confined within or excluded from any individual country's borders.
- » Innovation occurs faster than applicable regulations. Blockchain development and implementation are happening at a pace well beyond the capacity of regulators to respond, in many ways mirroring our experience with the Internet—but with one critical difference—speed. The Internet developed and advanced at the speed of sound. By comparison, the blockchain is evolving at almost the speed of light.
- » The dominant feature of the blockchain is its ability to evolve unpredictably and to spawn new chains of technological development. Ignoring jurisdictional boundaries, the blockchain already spans every corner of the planet. It is capable of penetrating many aspects of our daily life and business, both visibly and imperceptibly. Regulating under such uncertainty is a serious challenge.
- » Those who think the blockchain is beyond regulatory reach are fool hearty, as are those who believe self-regulation is the only road forward. Reality is always both more complex and subtle. The bottom line is that some aspects of the blockchain and its applications should be regulated. Other aspects, less so, if at all.
- » To strike the right balance, global regulators, the private sector, and private industry groups must all work together with the common goal of striking an appropriate compromise between encouraging innovation and protecting consumers and markets where necessary. This research suggests how to achieve that balance.



Introduction

"But I don't want to go among mad people," Alice remarked.

"Oh, you can't help that," said the Cat: "we're all mad here. I'm mad. You're mad."

"How do you know I'm mad?" said Alice.

"You must be," said the Cat, "or you wouldn't have come here."⁴



"The cat grinned," Lewis Carroll, *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 54. Cropped for placement. No known copyright restrictions.

What a fitting description of those of us in the world of blockchain, written over 150 years ago by Charles Lutwidge Dodgson, a professor of mathematics at the University of Oxford publishing under his pseudonym Lewis Carroll.⁵ Like a rabbit hole, the exciting opportunities of blockchain pull us in headfirst; and, before we realize what has happened, we're converts, potentially getting ourselves into the Red Queen's race.⁶

Like a rabbit hole, the exciting opportunities of blockchain pull us in headfirst; and, before we realize what has happened, we're converts.

Don Tapscott and Alex Tapscott's book, *Blockchain Revolution* sets forth how blockchain technology could change the world.⁷ It's not hyperbole. Their book describes opportunities for rethinking, reinventing, transforming, and even upending business and society, of which there are many, but also highlights the promise and peril of blockchain. This research focuses on an aspect of the latter—regulatory risk.

This research paper does not argue that the blockchain or its uses should not or cannot be regulated. Some early blockchain adopters argue, just as their Internet forebears did, that regulating such a distributed technology is impossible and that, even if we could regulate it, we should not. Those arguments were wrong then and are wrong now.



Any regulatory overlay imposed on the blockchain and its applications must be implemented thoughtfully, carefully and with a light touch.

This research paper acknowledges the importance of appropriate regulation and suggests some approaches for achieving effective regulation. On the other hand, this paper should not be interpreted as a pro-regulatory mandate. Bad regulation can be worse than no regulation. The blockchain and *distributed applications* (Dapps) that run on it warrant appropriate regulation but only when and where necessary. Any regulatory overlay imposed on the blockchain and its applications must be implemented thoughtfully, carefully and with a light touch.

In this context, when this research paper refers to regulation, it means both the types of regulations—those created by governments through the issuance of laws and those shaped by community consensus and self-governance. There is room for both approaches. Part of the challenge created by this brave new world of blockchain is figuring out which approach is better for particular circumstances.

We will undoubtedly see more regulatory oversight of blockchain activities than presently exists. To assure that we strike the right balance between protection and free enterprise, between individual rights and collective interests, and between preventing harm and encouraging and facilitating innovation, our approach must be thoughtful and rigorous. As much as possible, it requires a deep understanding of blockchain technology, its applications, its potential, and its downside. We must apply the lessons of Internet regulation and from the regulatory response to the global financial crisis of 2008.

Below, this paper sets out a way to think about the blockchain and blockchain-based applications from the perspective of law and regulation. It looks at the extent to which the blockchain represents unprecedented regulatory challenges and suggests an approach to determining when regulation is necessary and, in such cases, the form that regulation should take.

Is the blockchain beyond traditional concepts of law and regulation?

Cyberanarchy—what a word! According to Webster’s *Hacker Dictionary*, it means the carving out of “activities outside the purview of nation states.”⁸ Is that how to think about the blockchain and regulation? Some argue that, by its very nature, blockchain cannot be regulated, at least not in the traditional way in which we think about regulation.⁹ Others argue that, even if regulating the world of blockchain is possible, regulators should nevertheless let the market and blockchain participants sort out the “rules of the road.”¹⁰ In other words, when it comes to blockchain, cyberanarchy is good. In the early days of the Internet, many made the same argument.¹¹ Where the cyberanarchists correct then? Are they now?

Let’s consider the hallmarks of blockchain technology. First is its distributed nature. The blockchain allows individuals to come together to achieve common goals and organize themselves in



The blockchain allows individuals to come together to achieve common goals and organize themselves in manners very different from traditional enterprises.

Blockchain protocols enforce norms of behavior supported by broad consensus.

manners very different from traditional enterprises. In theory, we can launch blockchain applications and businesses without any formal centralized body of owners or managers. The marriage of the blockchain and open-source software potentially obsoletes existing corporate and legal entities or at least sidelines such organizational structures.

This is a mindboggling concept for anyone from the traditional corporate world. Without a corporate or managerial structure, who makes decisions about the future? Who sets goals and objectives? Who imposes guidelines and discipline? Who models acceptable behavior? Who is accountable when plans go wrong or actions harm others? Corporations and governments deal with such basic questions daily.

Second, blockchain protocols enforce norms of behavior supported by broad consensus; and so there is a theoretical framework for how a larger legal system might defer to a self-governing community. Some argue that community institutions able to self-govern through consensus make the same decisions as traditional legal institutions. Therefore, whether internal self-governing bodies or traditional institutions identify, agree upon, and apply these norms makes no real difference; the law is the same either way.

This approach may be an appealing in a world in which bloated corporate structures and corrupt governments can be kicked to the trash heap of history. How realistic is this vision? The argument that blockchain communities should be able to govern themselves outside traditional organizational and governmental involvement becomes strained when we consider externalities, that is, conduct that causes or could cause harm outside these communities.

We cannot assume that no one outside a blockchain ecosystem will care when blockchain transactions cause harm outside that ecosystem. The global community at large, and certainly governments, will insist that ecosystem rules—those intended to address harm to its members—be enforced within blockchain applications as well as elsewhere.



"Drink me," Lewis Carroll, Alice's Adventures in Wonderland, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 13. No known copyright restrictions.



Does the nature of blockchain obviate traditional regulation?

[Alice] went on, "Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to," said the Cat.¹²



"'You'll see me there,' said the cat," Lewis Carroll, *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 55. No known copyright restrictions.

Should we change existing laws and regulations in response to the unique attributes of the blockchain? Or should we use existing laws and regulations to change the features of the blockchain, so that the blockchain and its applications conform to those existing laws and regulations?

Let's frame the debate with a threshold question: Is the blockchain universe so fundamentally different that it obsolesces and resists society's traditional organizational and governance structures?

First, blockchain applications enable users to disregard or operate across the geographic boundaries of traditional sovereigns. On that basis, blockchain ecosystems could potentially represent a new universe in which traditional regulation is impractical, if not impossible. Few would dispute that a blockchain transaction occurring in one geographically defined jurisdiction could harm someone or something in another jurisdiction. The more important question is whether this borderless impact is truly unique.

The types of issues and problems that rise above sovereign borders have existed since the time human beings began migrating, forming new societies, and engaging in commerce (or war) with each other.



Blockchain applications are based on open-source software that no one owns or controls.

Cross-border engagement has always raised such questions as the enforceability of export restrictions, the limitations on public access to public information, the protection of intellectual property, and liability for injurious content.

Second, blockchain applications are based on open-source software that no one owns or controls. Anyone is free to take this code, modify it, develop it, or build on top of it. Should we allow people to use the code to circumvent legal and regulatory constraints, thereby displacing the social values embedded within those laws and regulations? If not, then regulators must decide whether to introduce new laws and regulations to reinforce those existing values or allow the dissemination of new code through the blockchain potentially to change these existing values.

The traditional method of regulation would be to oversee the owners of the code. However, without clear ownership, regulators lose the ability to force coders to write their code differently to achieve regulatory or policy objectives. Rightly or wrongly, this reality could force a shift in focus. If regulators no longer have the ability to regulate code itself, they may instead assert increasing control over the users of services within their jurisdictional reach. They may also look to regulate indirectly within the blockchain space.

Is self-governance the solution?

If we accept, for the moment, the argument that we cannot apply traditional concepts of regulation to the blockchain but we reject the Mad-Tea-Party brand of anarchy, then can we agree on an alternative system? Perhaps that alternative is a system of self-governance. The feasibility of any self-governance system typically starts with and certainly depends on the traditional community's respect for, and deference to, community law.



"Your hair wants cutting," said the Hatter, Lewis Carroll, *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 56. No known copyright restrictions.



History is full of examples of self-governance. Much of the derivatives market voluntarily operates under policies and procedures developed over time by the International Swaps and Derivatives Association (ISDA). ISDA's membership is comprised of financial institutions, hedge funds and other significant participants involved in the derivatives industry. The ISDA has introduced most of the accepted documentation used to memorialize derivatives transactions to the market. ISDA even sponsors an adjudication process to determine when credit events have occurred that can trigger payouts of hundreds of millions of dollars under credit derivatives transactions. Participants in derivatives markets have voluntarily endorsed this form of self-governance.

Traditional communities generally respect party autonomy exercised through contractual agreements so long as such contractual agreements don't cross generally agreed upon lines of criminal or immoral activity. Theoretically, community law can earn this respect as a contractual framework for blockchain transactions begins to emerge, partially though the use of smart contracts for governing blockchain transactions.

Traditional communities generally respect party autonomy exercised through contractual agreements so long as such contractual agreements don't cross generally agreed upon lines of criminal or immoral activity.

Even with the adoption of solutions such as smart contracts, enforcement of contractual autonomy still depends on traditional institutions. We can mitigate this dependence by internalizing enforcement; that is, we can agree on the types of criminal and immoral activity that rise above the right of parties to contract among themselves. However, we have no such universal agreement by which we might deem some activities illegal and others immoral. This limitation already applies in our existing world. Adoption of blockchain technologies does not necessarily worsen the problem.

Generally, we may justify self-governance or self-regulation where we can demonstrate its greater efficacy, where the activity regulated calls for specifically tailored adjudicatory procedural rules different from those of the surrounding community, or where those community rules are inapplicable. We would expect greater levels of member compliance with highly specialized procedural rules designed for a specific community, when self-enforced by that community.

For self-governance to work effectively, the community needs a number of critical elements including:

- » An ability or capacity to form and implement the types of functions central to a traditional legal system
- » An ability to enforce community decisions
- » A contractual or equivalent framework that clearly sets out the community's norms and related enforcement procedures
- » A sufficient level of institutionalization

For self-governance to work for the blockchain, the blockchain community must be able to police itself through either the



development of norms of conduct, private law enforced by contract, technological architecture, or some combination of the three.

Laws and norms represent opposite approaches to achieving the same outcome.

Law versus norms

Laws and norms represent opposite approaches to achieving the same outcome. If blockchains constitute social relationships formed by individuals and groups that operate outside the law, then norms become the default means of regulating activity. Are norms emerging for the blockchain? It is difficult to say. With the Internet, change has been constant and drastic, and so a strong set of norms never had a chance to develop beyond those core pioneers. That vacuum put law at a significant advantage. The same may become true of blockchain. We can learn a lot from the regulatory history of the Internet.

Lessons from the Internet and financial markets

Regulating the Internet, a convergence of computing and communications

Nearly twenty years ago, when Tim Wu was a law clerk for Judge Richard Posner, he published an article that described the debate over law and the Internet:

Table 1: Norms, contracts, and laws

	Norms of conduct	Private law	Public law
Defined as:	Recognized accepted forms of behavior and conduct	Agreements reached among specified parties for specific purposes and for a specified period	Statutes, regulations, and judicial decisions
Formed by:	Behaviors and practices over time by a self-defined community	Contract or technological architecture	Governments and regulators
Enforced by:	Community or representatives elected by the community	Adjudication, arbitration, or technological methods of self-enforcement	Centralized government
Effective only if:	Participants face negative consequences for ignoring norms enforced by ongoing actions of the community	Effective judicial system exists to impose and enforce penalties	Activity occurs within a jurisdiction, and the governmental body can assert control over parties involved through penal actions if necessary
Jurisdiction	Often unclear but based on self-defined parameters by a community	As defined by the parties involved	Single geography



One side asserts that the Internet is so new and different that it calls for new legal approaches, even its own sovereign law. The other side argues that, although it is a new technology, the Internet nonetheless presents familiar legal problems. It is a battle of analogies: One side refers to Cyberspace as a place, while the other essentially equates the Internet and the telephone.¹³

In the early life of the Internet, the Internet community resisted almost all forms of conventional government regulation.

In the early life of the Internet, the Internet community resisted almost all forms of conventional government regulation. Many embraced the mantra of “don’t regulate the Internet,” and others insisted that the Internet, by virtue of its openness and international nature, could not be regulated. Many blockchain enthusiasts are now repeating those arguments almost word for word.

(As it turns out, some of the same Internet pioneers who argued against anything but self-regulation of the Internet now see blockchain technology as a means of righting the wrongs inadvertently unleashed via the Internet, such as the concentration of power, state censorship, and monitoring of citizens.¹⁴)

Should we monitor the self-regulation of early adopters?

Much like early blockchain adapters, the early Internet world was “techno-libertarian.” Early Internet advocates viewed cyberspace as a unique place where regulation would not work and, hence, where people would be free. Freedom had two senses. A subset of Internet enthusiasts held that cyberspace was free from any regulation whatsoever. A second, somewhat more mainstream group maintained that the Internet was free from state regulation but acknowledged the possibility of self-regulation. The Internet’s libertarian community argued that cyberspace was unregulated and unregulatable and that cyber behavior was beyond the reach of governments.

Internet researchers regularly proclaimed, “The strongest argument for self-regulation is that it works,” pointing not just to the exponential growth of the Internet but also to its heterogeneity of language, culture, ethnicity, religion, and economic status, with constantly evolving infrastructures.¹⁵ In many respects, this was true. The US government did champion self-regulation, in part through industry, to address technical standards and public policy questions raised by Internet commerce.

As the Internet penetrated mainstream society, many argued that the Internet changed international law by eroding the dominance of sovereign states and facilitating new institutional mechanisms for making, applying, and enforcing law.

For the most part, those arguments didn’t hold—and they’re not holding now for blockchain. We must be cautious not to attribute God-like transformative powers to the blockchain that do not exist. Yes, the Internet certainly resulted in changes to the global order, threatening state hegemony. Consider the use of social media to



elect the first African American President of the United States or to effect regime change in Tunisia, Libya, Egypt, and Yemen.

However, incumbent powers have proven that they have many resources to fight back. They even exploit the Internet to surveil citizens, suppress speech, consolidate their control, and interfere with democratic elections elsewhere in the world.

We can learn from the Internet's development in such areas as technical standard setting, where industry participants likely have subject matter expertise superior to government agencies.

Should we take a light regulatory touch?

In reality, the Internet did not develop in a regulatory-free zone. For example, in 1996, in response to increasing incidences of copyright infringement that accompanied the growth of the Internet, the World Intellectual Property Organization (WIPO), a branch of the United Nations, decided to take action, following lobbying efforts from both film and music industries. WIPO's efforts resulted in two Internet treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

Fortunately, in many ways, the Internet did benefit tremendously from a light regulatory touch.

These treaties extended existing WIPO intellectual property agreements among the contracting nations. The two treaties required countries to establish laws preventing online copyright infringement. In response to these treaties, the United States enacted the Digital Millennium Copyright Act (DMCA). In reality, DMCA was not exactly a light touch.

According to one observer, the parties that "assembled to hammer out the details of the DMCA" were concerned that "it would discourage growth by forcing would-be web entrepreneurs to navigate a legal minefield that would cost more in fines and legal fees than was worth the effort."¹⁶ He concluded:

Without the fight put up by these Internet advocates, it's a fair bet that the online landscape we know and love today would be far more sparse. Google, YouTube, Twitter, Flickr, . . . and many other online service providers are protected by provisions in the DMCA that give them "safe harbor" from prosecution for copyright infringement so long as they adhere to certain guidelines.¹⁷

Fortunately, in many ways, the Internet did benefit tremendously from a light regulatory touch. The US government, for example, encouraged and protected the Internet's nonproprietary and layered architecture. The essence of this open architecture was a commitment to using a platform standard that both users and providers of content and services could access easily. In particular, this approach limited proprietary gatekeepers from restricting or charging for access to the standard.



Transmission control protocol and the Internet protocol (TCP/IP), both nonproprietary standards, enable the Internet to function as a network of networks.

Notably, this environment produced the *transmission control protocol* and the *Internet protocol* (TCP/IP), which together facilitate the routing of Internet communications. TCP/IP enables the Internet to function as a network of networks, just as the standard gauge of rail enabled the titans of locomotion to interconnect their railroads.¹⁸ To this date, this Internet standard remains nonproprietary. No one owns the intellectual property underlying the Internet, and so application developers can freely create—and users can easily access—new products and services.

Also significant to Internet development, formal and informal public and private partnerships such as the Internet Engineering Task Force have arisen and play ongoing governance roles in, for example, standards setting.¹⁹ Government experts may participate in but do not control proceedings; private sector engineers can develop the Internet's key software on a nonproprietary basis.²⁰ It also benefitted from the free software movement, launched in 1983 by Richard Stallman who created an open-source Unix-compatible software system and released it under a *general public license* (GPL) so that he and others could use, share, and improve it without violating anyone's intellectual property rights in perpetuity.²¹

In the 1990s, the US government eliminated restrictions on the use of the Internet for commerce and privatized key Internet infrastructure. Since then, and not surprisingly, the situation has grown somewhat more complicated. Early government support to an open architecture model for the Internet's development has given way to proprietary and closed standards for Internet applications.

"In particular, by calling on commerce to take the leading role in developing the Internet, the government created a gold rush for companies to introduce proprietary technologies to the developing Internet infrastructure," wrote Philip Weiser, the Hatfield Professor of Law and Telecommunications and Dean Emeritus of the University of Colorado Law School.²²

Should we apply an old framework to new technology?

Net neutrality promotes innovation through Darwinian competition where the fittest applications survive.

Here's a case in point: *net neutrality*, the principle that broadband Internet providers should allow access to all content and applications equally, irrespective of the content's source.²⁴

Proponents of net neutrality argue that an open-access regime will lead to better information, more innovation and investment in Internet infrastructure, and preservation of freedom of speech and freedom to access that speech. It promotes innovation through Darwinian competition where the fittest applications survive. Those that do not adapt quickly enough disappear. It also promotes investment in Internet infrastructure such as streaming video and high-speed Internet. Finally, they argue, net neutrality prevents price discrimination based on content. Opponents argue the opposite: a neutral network would actually decrease innovation and investment.²⁵



Before implementing its net neutrality policy under the Obama administration, the Federal Communications Commission (FCC) had classified broadband providers as information services under the Telecommunications Act of 1996. This Act divides the world into two categories: telecommunication carriers that transmit without altering information; and information service providers that enhance content received by Internet subscribers.²⁶

Congress incorporated the Telecommunications Act into the Communications Act of 1934, which regulates telecommunications. The Communications Act imposes so-called “common carrier duties” on certain telecommunication providers: telecommunication carriers that transmit telecommunication services are classed as common carriers. As technology evolved so that broadband service providers could discriminate based on the type and source of content delivered, the FCC decided to respond.

Whenever the horse stopped (which it did very often), [the Knight] fell off in front; and whenever it went on again (which it generally did rather suddenly), he fell off behind. Otherwise he kept on pretty well.²³



"Whenever the horse stopped he fell off," Lewis Carroll, Through the Looking Glass: and What Alice Found There, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 166. No known copyright restrictions.

In 2010, the US Federal Communications Commission issued three new rules that prevented broadband providers from discriminating when providing access to Internet traffic.

In September 2005, the FCC moved toward the regulation of broadband providers by releasing its Internet Policy Statement, announcing its goal to “preserve and promote the open and interconnected nature of the public Internet.”²⁷ Relying on this policy statement, the FCC brought a discrimination action against Comcast in 2007. However, a court struck down the Comcast order. In 2010, the FCC responded by issuing three new rules that, among other things, prevented broadband providers from discriminating when providing access to Internet traffic. Verizon challenged the FCC’s rules.

Although the court upheld a portion of the FCC’s new rules, it struck down the provisions relating to antidiscrimination. This ultimately led to the FCC’s decision in 2015 to reclassify broadband providers as common carriers to bring them under the Communications Act, thereby requiring them to provide indiscriminate, just, and reasonable access to all customers and content providers.



Over the next several years, regulators should watch what happens to Internet content and applications and distill lessons relevant to regulating blockchain technologies and applications.

In its attempt to regulate the new world of the Internet, the FCC first issued guidance to the public in the form of a policy statement. It then took selective enforcement action, issued new regulations, and reinterpreted existing statutes to broaden its authority.²⁸ That's how regulators adapt an existing regulatory framework to a new and potentially inchoate technology.

The FCC has since reversed its policy of net neutrality under the Trump administration. We will eventually find out which approach both protects the public and promotes innovation. Over the next several years, regulators should watch what happens to Internet content and applications and distill lessons relevant to regulating blockchain technologies and applications.

Regulating banks, exchanges, and financial institutions

In the 1970s, as the Internet pioneers were launching e-mail, TCP/IP, the first Internet address registry, and Telenet, the titans of finance were forming the Society for Worldwide Interbank Financial Telecommunication to communicate cross-border payments and hiring quantitative analysts ("quants") to combine advanced mathematical theory, large sets of historical data, and heavy duty computing in models that could predict market behavior.²⁹

Scott Patterson, author of *The Quants*, described how these models transformed the industry into what it is today: "Wall Street is essentially floating on a sea of mathematics and computer power."³⁰ We could say the same of such media as Facebook, Amazon, Netflix, and Google.

The titans also increased their use of securitization—the bundling of debt (loans, leases, trade receivables) into securities, the value of which derives from cash flows of the underlying assets—to create liquidity.³¹ "Securitization was one of the most brilliant financial innovations of the 20th century," said James Rokakis, a longtime Cuyahoga County treasurer in Ohio. "It freed up a lot of capital. . . . But then people realized they could scam it."³²

To regulate the financial system adequately, policymakers need to keep up with these complex financial innovations—not just to develop appropriate regulations but to recognize and respond to warning signs. According to the Financial Crisis Inquiry Commission, established by the Fraud Enforcement and Recovery Act of 2009 to identify the causes of the financial crisis:

Key policymakers—the Treasury Department, the Federal Reserve Board, and the Federal Reserve Bank of New York—who were best positioned to watch over our markets were ill prepared for the events of 2007 and 2008. . . . They thought risk had been diversified when, in fact, it had been concentrated.³³

To regulate the financial system adequately, policymakers need to keep up with these complex financial innovations.



Attracting key finance, math, and computer science talent to this kind of public service isn't easy, especially if the culture is one of defending bureaucracy rather than reinventing government for the common good.³⁴

How do we strike the right balance between public and private roles?

Consider what the FCIC said about the influence of the finance industry and the role that influence may have played in the 2008 financial crisis

From 1999 to 2008, the financial sector expended \$2.7 billion in reported federal lobbying expenses; individuals, and political action committees in the sector made more than \$1 billion in campaign contributions. What troubled us was the extent to which the nation was deprived of the necessary strength and independence of the oversight necessary to safeguard financial stability.³⁵

The FCIC concluded that lawmakers had become beholden to the financial services industry:

We ended up with a 21st century financial system with 19th century safeguards. More than 30 years of deregulation and reliance on self-regulation by financial institutions, championed by former Federal Reserve chairman Alan Greenspan and others, supported by successive administrations and Congresses, and actively pushed by the powerful financial industry at every turn, had stripped away key safeguards, which could have helped avoid catastrophe.³⁶

The FCIC concluded that lawmakers had become beholden to the financial services industry.



"Humpty Dumpty," Lewis Carroll, Through the Looking Glass: and What Alice Found There, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 118. Cropped for placement. No known copyright restrictions.



Should complex problems beget complex regulation?

Financial regulators have demonstrated a pattern of over-regulating, then deregulating, then re-regulating (with greater complexity).

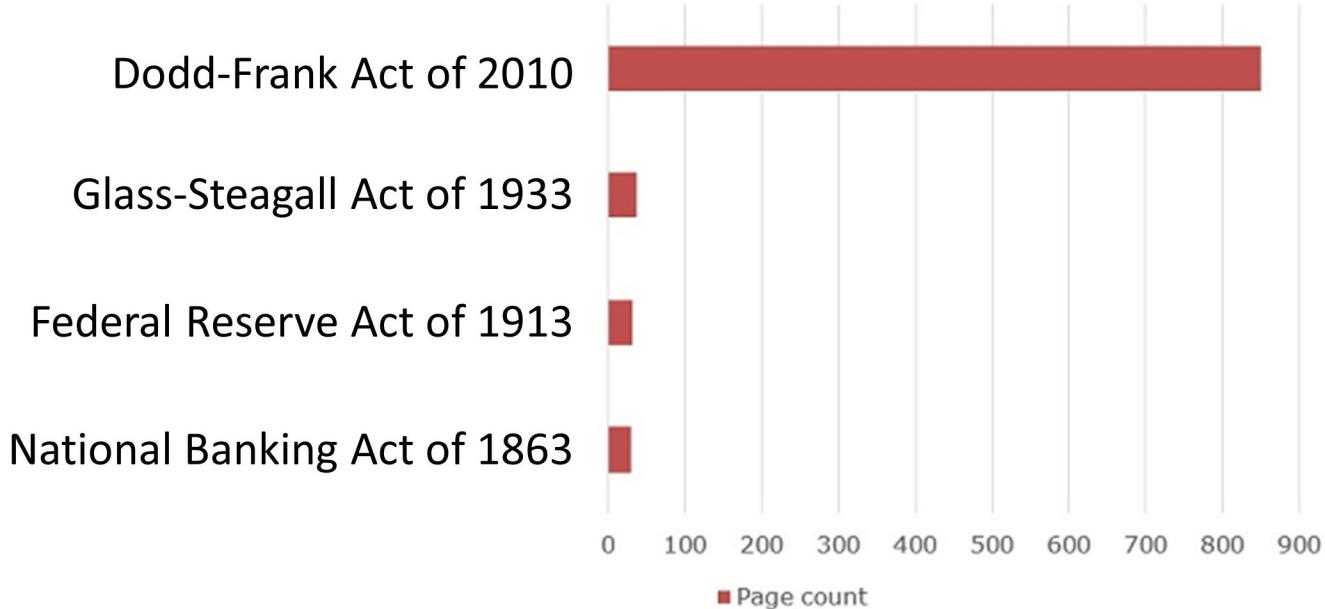
The Glass–Steagall Banking Act of 1933, enacted after the Great Depression of 1929 and which created the Federal Deposit Insurance Corporation, aimed to restore the public's trust in financial institutions, and separated commercial banking from insurance and investment banking to protect consumer deposits from speculators.³⁷ It was a mere 37 pages.³⁸

Fast forward to the Great Mortgage Meltdown of 2008, during which some 9.3 million families lost their homes.³⁹ Enacted amid concerns of a prolonged “Great Recession,” the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 weighed in at over 2,300 pages (or a mere 848 pages as published by the US Government Printing Office).⁴⁰

As Figure 1 shows, over the last 150 years, financial regulators have demonstrated a pattern of over-regulating to rebuild public trust in response to crisis, then deregulating after a period of stability and much industry lobbying, then re-regulating (with greater complexity) in response to another crisis and another breach of public trust.⁴¹

The legislative complexity of Dodd–Frank may be unprecedented. Equally unprecedented is the extent to which the US Congress effectively delegated the task of filling in the details of Dodd–Frank: between 240 and 530 of its substantive provisions and definitions required multiple US regulatory bodies to make, clarify, and

Figure 1: Complexity of financial regulation



Source of data: "Too Big Not to Fail," The Economist, 18 Feb. 2012.



implement new rules. The Act also mandated 60 to 70 regulatory studies and a comparable number of detailed reports. To date, almost a dozen regulators have issued thousands and thousands of pages of regulations to effect the requirements of Dodd–Frank.

That's not a good sign. The FCIC found that turf wars prevented timely intervention:

As irresponsible lending, including predatory and fraudulent practices, became more prevalent, the Federal Reserve and other regulators and authorities heard warnings from many quarters. Yet the Federal Reserve neglected its mission. . . . The Office of the Comptroller of the Currency and the Office of Thrift Supervision, caught up in turf wars, pre-empted state regulators from reining in abuses.⁴²

Consider the regulatory layers US-based financial institutions must deal with:

- » The Federal Reserve, the Federal Deposit Insurance Corporation, the Comptroller of the Currency, and the Consumer Financial Protection Bureau all regulate large financial institutions in the United States.
- » Another twenty or so federal bodies regulate various products and services offered by large US banks.
- » Each US state has its own set of regulatory agencies that, to various extents, also oversee financial institutions.
- » Additionally, large US financial institutions must deal with regulatory regimes in each non-US jurisdiction in which they operate.

The multitudes of regulators who have jurisdiction over large financial institutions have differing, complex mandates. To a various extent, all of them play roles in protecting consumers. Beyond that, some focus on systemic financial safety and soundness, others make sure the markets function smoothly, and still others focus on specific types of products. To stay in business, these financial institutions must have large, complex compliance operations and sophisticated risk management tools.

If the financial crisis of 2008 taught us anything, it is that regulators cannot be fighting over jurisdiction while the market in dispute is burning to the ground.

If the financial crisis of 2008 taught us anything, it is that regulators cannot be fighting over jurisdiction while the market in dispute is burning to the ground.

How should we account for the cost of complying with regulations?

Financial services institutions alone have spent billions of dollars to comply with Dodd–Frank. S&P Global Market Intelligence conducted a survey of the banking industry on the subject of compliance: nearly



It is no longer sufficient to simply throw more and more resources at risk and compliance—firms are now seeking targeted risk management outcomes by utilizing technology and specific value-add compliance skills.

half said compliance costs were up at least 20 percent, and nearly a fourth of respondents said their costs were up between 10 and 20 percent.⁴³

For some, compliance costs are unsustainable and may end up driving further industry consolidation: five percent of respondents said that they account for more than a third of the operating budget, and 14 percent reported that compliance costs comprise 20 to 30 percent of annual expenses.

Community banks and credits unions have been particularly hard-hit. Nearly 40 percent of respondents were either “very likely” or “somewhat likely” to consider a merger or acquisition offer over the next 12 months.⁴⁴

Others have had to pass on costs to their customers. One respondent from a credit union told S&P Global Market Intelligence:

*I can emphatically state if significant regulatory relief is not provided for small to mid-sized institutions soon, in 20 years, I doubt we will be left with anything else besides megabanks. . . . This will have a dramatic, chilling effect on small business creation and economic growth in the country.*⁴⁵

Thomson Reuters’ eighth annual “Cost of Compliance” survey of global risk and compliance practitioners found that they’re looking to automation to minimize compliance costs and maximize effectiveness: 33 percent of all firms and 48 percent of global systemically important financial institutions will involve compliance in assessing both fintech and regtech in the next 12 months.⁴⁶

According to the report’s authors, 2017 was a “pivot point for the cost of compliance. It is no longer sufficient to simply throw more and more resources at risk and compliance—firms are now seeking targeted risk management outcomes by utilizing technology and specific value-add compliance skills.”⁴⁷ Perhaps distributed ledger technology will be among the solutions.

Can we minimize unintended consequences from regulation?

In a recent survey on the efficacy of Dodd-Frank, more than half of the respondents agreed that financial services regulation either had little effect (35%) or actually worsened market stability (17%)—presumably reducing liquidity in some markets—against only 43 percent who said the new regulations had increased stability.⁴⁸ This is not surprising. Many in the United States believe that the Dodd-Frank regulations are overbroad, don’t accurately reflect the true causes of the financial meltdown, and have a number of unintended consequences.

For example, the so-called Volcker Rule under Dodd-Frank, subject to certain exceptions, severely restricts the ability of banks to engage in proprietary trading. One of the exceptions allows banks to engage in market-making activities so long as such activity is tied to reasonably expected near-term customer demand.



Unfortunately, customer demand decreases in times of market disruptions. As a result, banks can no longer step into the market through their market-making activities to stabilize markets exactly at the time most needed. Many economists have expressed concern that provisions like this will actually worsen the next financial crisis.

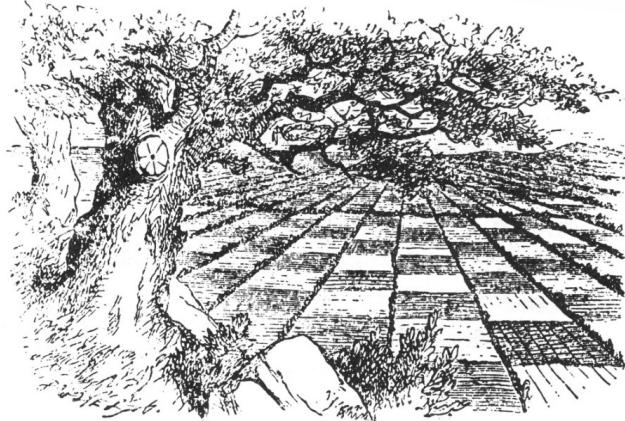
We will be well served if regulators first understand the technology before regulating it, and then ask the right questions.

Finding a better way

There are better ways to regulate. We hope that regulators take time to learn from the regulatory reaction (or overreaction) to the financial crisis. We will be well served if regulators first understand the technology before regulating it, and then ask the right questions, adopt appropriate regulatory principles suitably tailored to the blockchain and its applications, and follow a regulatory implementation approach that is open, clear, and consistent.

Understanding the core features of blockchain technology

Alice said at last, . . . "It's a great huge game of chess that's being played,—all over the world,—if this is the world at all, you know. Oh, what fun it is!"⁴⁹



"Just like a great chess-board!" Lewis Carroll, Through the Looking Glass: and What Alice Found There, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 38. No known copyright restrictions.

The blockchain is jurisdictionally agnostic

Does the borderless nature of blockchain transactions create problems that traditional legal systems cannot deal with? According to the European Parliament, the answer may be yes. A policy



Because of the decentralized, cross-boundary character of the blockchain, policymakers need a harmonized regulatory approach at the transnational level.

Blockchain users should urge governments to adopt a set of global blockchain rights that underlie their regulatory approach to the blockchain.

analysis by European Parliamentary Research Services warns that centralized legal systems may not be able to assert any control over decentralized activities on a distributed ledger for a number of reasons:

» No clear jurisdiction

"The decentralized, cross-boundary character of blockchain . . . raises jurisdictional issues as it seems to diffuse institutional accountability and legal responsibility in an unprecedented manner, rendering the need for a harmonized regulatory approach at the transnational level more pertinent compared with a local or regional one."⁵⁰

» Little control, few checkpoints

*"Centralized structures of law might lose their ability to control the ledger . . . or to shape the activities of disparate people or autonomous decentralized organizations, as no one (including the original creator) can control the ledger after it has been deployed. There will be fewer checkpoints to guide and assist the flow of data."*⁵¹

» No legal person

We also need to consider "the legal enforceability of smart contracts, and liability and accountability issues," exacerbated by their operating across borders and their potential inability to perform complex operations, because "distributed ledgers currently lack the legal personality that is necessary for them to be assigned with responsibilities and liabilities."⁵²

Even if a jurisdiction in which an injury arises from a blockchain transaction asserts its authority and chooses a plausible body of substantive law, it may lack the means of enforcing its decision, if the injuring party is beyond its reach. When conduct is criminal, authorities may lack the traditional jurisprudence means for addressing such transitory crimes, namely, trying a crime committed in one jurisdiction in the courts of another jurisdiction. Geographically defined legal systems do not usually prosecute crimes committed in other places, except by artificially redefining the place of commission to be the place of injury.

Where are players located, where does an activity occur, and which markets are affected all become debatable when transactions involve the blockchain. Resolving these questions could take years of jurisprudence development, a healthy dose of argument, and occasional chaos.

Unless blockchain ushers in a new utopian world, we will never see a single global approach to blockchain regulation. Blockchain's borderless nature will test the patience of governments as they try to assert their separate and potentially contradictory interests. Before



Before it is too late, the community of blockchain users may need to push governments to adopt a set of global blockchain rights that underlie their regulatory approach to the blockchain.

We have no single or shared definition of what constitutes inappropriate behavior or as to what the appropriate sanctions should be for that behavior.

it is too late, the community of blockchain users may need to push governments to adopt a set of global blockchain rights that underlie their regulatory approach to the blockchain. At a minimum, those rights could address:

- » *Access to applications.* Some governments may want to prevent their citizens from accessing certain encryption and blockchain applications. Nonetheless, the blockchain community should collectively press global regulators to adopt policies that assure individuals broad and open access to blockchain applications unless those applications violate universal norms of social behavior.
- » *Access to information.* Different societies place different values on the interaction between individuals and information. The United States puts a premium on giving individuals broad and open access to information. The European Union emphasizes the right of individuals to protect their personal data. Other countries prize their ability to restrict access to information. We will likely not soon reach global consensus on access to and use of information. At best, our approach should balance, as best as possible, the right to distribute and access information, the rights of individuals to privacy and data protection, and the legitimate needs of governments to access or restrict the flow of data occasionally.
- » *Ability to contract.* International commerce works only because players may contract with each other with relative assurances that they can enforce their contractual rights. Although blockchain applications may impede our ability to determine which rules of contract law to apply, any regulations should assure regulators' ability to adjudicate blockchain-related disputes. We cannot use the murkiness of location as an excuse for disregarding conflicts of law principles or the global organizations to which parties can presently turn in adjudicating contractual disputes.
- » *Civil society.* We will continue to hold widely divergent legal standards for the types of behaviors considered tortious, libelous, or defamatory. We have no single or shared definition of what constitutes inappropriate behavior or as to what the appropriate sanctions should be for that behavior. The Internet has forced us to rethink how we handle such concerns where different societies have legitimate and different ways of viewing behaviors that may be inappropriate in one culture and permitted and perhaps even desirable in another.

Blockchain applications will continue to push the limits as to how deal with such different views. We cannot use blockchain technology to disregard society's base behavioral norms nor should we pressure regulators to disregard such core societal values simply because of the seamless nature of the blockchain.



Start-ups can push existing players aside

Start-ups often lack the resources and expertise to understand, analyze, and create the policies and procedures necessary to comply with regulatory standards across jurisdictions.

As with the Internet, we are seeing two different approaches to blockchain development and growth. In the public spotlight, incumbent firms are developing blockchain applications to integrate into existing products. Large financial institutions such as those involved in the R3 consortium are creating apps to undertake all types of financial transactions more cheaply and securely.⁵³ Those with large global footprints can withstand the costs of regulatory compliance across multiple jurisdictions. They have the experience and resources to deal with competing and potentially contradictory regulatory demands.

Moreover, regulators charged with assuring ongoing compliance know that they can assert jurisdiction and authority over these global enterprises. They have the tools necessary to punish bad actors or to exclude them from accessing a local market. Regulators can achieve their objectives without relying on social pressure underlying social norms.

These dynamics fall apart for start-ups. Operating outside the public spotlight, start-ups often lack the resources and expertise to understand, analyze, and create the policies and procedures necessary to comply with regulatory standards across jurisdictions. This probably doesn't matter. Even if global regulators are aware of a start-up, that start-up may be operating beyond the regulator's reach.

To complicate matters, many entrepreneurs are working quickly and relentlessly to develop blockchain applications that will destroy our conventions of doing business and displace existing players in the process. For example, new businesses such as BitPesa, Veem, and WeTrust are aiming to onboard millions of people to the global



"Father William balances the eel," Lewis Carroll, *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 42. No known copyright restrictions.



Should these new small businesses be regulated as if they were large incumbents?

economy, starting with the instantaneous transfer of small amounts of money at little or no cost anywhere in the world, especially in developing markets where traditional banking services are too expensive or simply unavailable.⁵⁴ By operating outside traditional banking channels, these start-ups are operating outside existing regulatory channels.

Should these new small businesses be regulated as if they were large incumbents? We are seeing how this approach is killing the community bank. It makes no sense. Equally, it may also make no sense to ignore the potential for fraudulent practices in the absence of oversight. Of course, regulators could simply forbid start-ups from rolling out decentralized apps that purport to perform banking-like functions without regulatory scrutiny. But whose scrutiny? In whose jurisdiction? These are no simple questions.

Imposing the same regulatory spider web on blockchain start-ups—those offering products intended to displace typical banking products—would be nonsensical, as would leaving these start-ups completely and indefinitely alone. Such blockchain applications raise a myriad of appropriate regulatory structure questions: What types of blockchain businesses should be allowed to provide banking-like offerings? What types of banking-like products and services should they be allowed to offer?

At the same time, existing regulatory bodies must collaborate in policy-making and coordinate their responses to these questions. The patchwork of regulators with overlapping authority will simply not work to govern decentralized blockchain-based markets driven forward by small geographically dispersed players.

Smart contracts fulfill the trustless component of the blockchain

The *smart contract* has no widely accepted definition. Those who use the term are often referring to computer program code that, when run on a blockchain, facilitates entering into an agreement or arrangement between parties and automates (or automatically enforces) performance of that agreement.

A traditional contract sets out the understanding between contracting parties. In theory, smart contracts, sometimes called *self-executing contracts*, go a step further. They can implement or “enforce” that understanding. The critical point: performance of the agreement is automated because a programmer has translated relevant “legalese” into computer code that forms a set of instructions for self-executing activities. While parties needn’t run such a program on a blockchain, they may choose to do so because:

- » They don’t know or don’t necessarily trust each other and want the contract to execute exactly as coded without interference.

Smart contracts can implement or “enforce” the understanding between contracting parties.



- » They need assurance of continuity, which the distributed nature of the blockchain provides (during massive power outages, infrastructure sabotage, or government attempts to shut down communications).
- » They want to prevent any tampering with the code, which the blockchain's immutability and transparency provide; parties to the contract would see any attempts to alter it.
- » The smart contract contains conditions that refer to oracles, such as off-chain data events (e.g., price changes) or an on-chain threshold assurance (e.g., a majority of shareholder votes received); when these conditions are met, the code automatically triggers specific actions, also defined in the contract.
- » The smart contract controls other assets (both on-chain cryptoassets and titles to off-chain assets) or triggers or interacts with other smart contracts, such as initial coin offerings or self-sovereign identities.

To the extent that we can code regulatory requirements directly into smart contracts and make compliance with those requirements self-executing, then we may want to rethink existing regulatory paradigms in terms of the blockchain. Of course, because smart contracts are computer code, they can substitute only for traditional contractual arrangements where the terms are objective, not subject to interpretation, and are programmable, self-executing, and self-enforcing.

Smart contracts will need to become far more sophisticated if we want them to play such a regulatory role. For example, they will need to have "control" over the physical or digital assets to be transferred pursuant to the smart contract as well as fiat currency, if any, used for payment. Distributed ledgers must integrate with existing payment systems without requiring deposits of all funds necessary to perform the contract. Distributed ledgers must also be able to integrate with asset registries to create and release liens and even transfer assets as parties exchange payments through the ledger.

Smart contracts will need to become far more sophisticated if we want them to play such a regulatory role.

If smart contracts become sufficiently robust to begin taking on regulatory enforcement, forward-thinking policymakers will likely struggle for governmental buy. The extent to which regulators are willing to "delegate" aspects of regulatory enforcement to smart contracts may depend on who controls contract code and whether regulators have the ability to assert their authority.

If smart contracts rely on closed code owned or controlled by corporate or comparable legal entities, regulators would presumably be able to exercise regulatory oversight as they do over other means of global commerce. But if the code is open source outside the control of any particular, identifiable legal entity, then regulatory power is threatened. This does not mean that the use of open-source code to build blockchain applications isn't beneficial. Regulators may, however, need to rethink how they assert regulatory oversight.





Smart contracts may represent an efficient means of reflecting emergent consensus on acceptable blockchain practice.

"Alice picks up the White King," Lewis Carroll, Through the Looking Glass: and What Alice Found There, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 17. No known copyright restrictions.

A substantial number of blockchain start-ups rely entirely or to a significant extent on open-source code as the foundation of their blockchain applications. Part of blockchain's appeal, at least within the non-institutional side of blockchain, is its distributed nature in which everyone can contribute to the success of an application or idea that is owned by everyone and no one.

The beauty of allowing everyone to contribute to the code also has an unattractive side, at least from the perspective of a regulator who can only watch from the sidelines as a spectator. Of course, nothing would prevent regulators from becoming part of the community and contributing to its development.

Perhaps, then, smart contracts may represent an efficient means of reflecting emergent consensus on acceptable blockchain practice. Voluntary norms may likely wind their way into smart contracts so that the contracts themselves become a more effective means of codifying, if not institutionalizing, such norms than regulators' imposing smart contract standards.

However, *smart contracts are self-enforcing*. For smart contracts to work, or at least to work most effectively, we must operate under an assumption that, in an ideal world, all possible outcomes of the contract (including penalties for breach) haven been explicitly identified and addressed in advance, akin to liquidated damages clauses in traditional contracts.

What happens, however, if a contingency occurs that the parties have not anticipated and addressed in the smart contract's self-executing code? Smart contracts are necessarily deterministic and will not



work particularly well in circumstances where the contracting parties want to renegotiate terms and outcomes following the occurrence of unanticipated events.

Traditional contracts allow for the unpredictability of human behavior, including the potential of intentional nonperformance. Following a breach of a traditional contract, the aggrieved party has the option to seek specific enforcement, monetary damages, or restitution through third parties such as courts. In contrast, smart contracts are performed (and therefore enforced) automatically through the terms and mechanisms embedded in the code of the smart contract itself.

Instead of seeking damages for nonperformance, a party may be seeking redress for a contractual outcome that was actually performed (or is being performed) but does not reflect the true intent of the parties because of unanticipated factors outside the scope of the smart contract. The remedy must come after the fact to undo or alter an agreement that has fully and automatically been performed.

Here parties may want regulators to assert authority. Many laws recognize the occurrence of circumstances that allow for appropriate modifications or absolve a party from performing a contract. Given circumstances beyond their control or imagination, the contracting parties may voluntarily amend contract terms. Unless and until we have a widely accepted means by which we can amend or modify smart contracts to reflect changes in law, circumstances, or the desires of the parties, we may need to resort to external means of dispute resolution, as through the courts of various countries.

Is the smart contract intended to create a binding legal agreement or an effective substitute for a binding legal agreement? This is not just a technological question. As one commentator noted,

This answer depends on existing legal doctrine and how our legal, political, and commercial institutions decide to treat the technology and use of smart contracts. If businesspeople don't trust it, the legislature doesn't recognize it and the courts can't interpret it, then it won't be a very practically useful "contract."⁵⁵

Is the smart contract intended to create a binding legal agreement or an effective substitute for a binding legal agreement?

Ultimately, that smart contracts are written in open-source software that is not "owned" by a legal entity in the traditional sense may be irrelevant. So long as participants using smart contracts require assurance that they will have access to traditional adjudicatory bodies, regulators will have an ability to assert influence over blockchain behavior. This certainly does not mean that regulators won't rely on social and behavioral norms as enforcement tools. As the Internet has taught us, the regulatory web that overlays blockchain activity will likely be a combination of community-based consensus and norms where practical, and regulatory-mandated requirements when not.



Smart contracts could create new types of "choice of law" problems that international organizations can address more effectively than government regulators.

International commerce is replete with examples of international standards bodies that govern contracting terms and performance norms. For example, in the case of international trade, the commercial letter of credit is the primary mechanism for payment. Such letters of credit are subject to a special set of rules administered by the International Chamber of Commerce. These rules are not a body of law, but rather, a set of rules adhered to by banks worldwide.

Why should we believe that the blockchain environment would differ fundamentally? If the code used to write smart contracts is "law," then that law needs to distinguish between Dapps and basic standards developed by standards bodies regarding blockchains themselves. Smart contracts could create new types of "choice of law" problems that international organizations can address more effectively than government regulators.

Disintermediation and the blockchain are synonymous

Much of our existing regulatory scheme, particularly for financial services and markets, delegates regulatory oversight and enforcement responsibilities to intermediaries such as exchanges and clearing agents. Regulators use intermediaries to expand their regulatory reach and power but not their costs.

For example, although a routine securities trade can be executed within microseconds, the actual settlement, that is, the process of verification of transfer of ownership of the security, can take as long as a week. That's because the parties trading securities do not have direct access to each other's ledgers and there is no way to verify automatically that the securities are owned by one party and can be transferred to the other party.

Instead, a series of intermediaries, the clearinghouses, which serve as verifiers as to the ownership of the securities and which process and maintain the records for the securities trades, must reach out to other intermediaries such as broker dealers and share registrars, who all must update separately their respective ledgers. The existing securities regulatory system contemplates the roles played by all of these different intermediaries. Given the SEC's limited resources, the SEC uses these intermediaries to assure proper functioning of securities markets on the SEC's behalf.

Distributed ledger technology is already changing how we complete transactions and eliminating the use of intermediaries and related transaction costs. Consider Overstock.com, the first US public company to list and trade its securities on the blockchain. It demonstrated how the blockchain could revolutionize securities trading. For two years, Overstock.com worked closely with the SEC and Financial Industry Regulatory Authority (FINRA) to obtain their approval. Among its many challenges, Overstock.com needed to reconcile the blockchain trading process with existing US securities

Distributed ledger technology is already changing how we complete transactions and eliminating the use of intermediaries and related transaction costs.



laws and regulations because blockchain challenged the assumptions that policymakers made about the contexts in which securities regulations would operate.

Specifically, the SEC assumed a clearing and settlement process that involved a clearing agent subject to SEC regulatory oversight. However, whenever a security is “traded” on the blockchain, it is simultaneously traded and settled: there is no clearing and, thus, no clearing agent. Nor is there a custodian, since there is no physical thing to deliver.

The SEC sees the benefits of blockchain technology but also expresses concerns as to how bad actors might exploit the technology:

Although the design and maintenance of cryptocurrencies differ, proponents of cryptocurrencies highlight various potential benefits and features of them, including

- › *The ability to make transfers without an intermediary and without geographic limitation*
- › *Finality of settlement*
- › *Lower transaction costs compared to other forms of payment*
- › *The ability to [verify publicly] transactions. . . .*
- › *Personal anonymity*
- › *The absence of government regulation or oversight.*

Critics of cryptocurrencies note that these features may facilitate illicit trading and financial transactions, and that some of the purported beneficial features may not prove to be available in practice.⁵⁶

The blockchain and its applications will likely enable us to achieve our current goals in new ways that require policymakers to rethink how they regulate certain activities.

The blockchain and its applications will likely enable us to achieve our current goals in new ways that require policymakers to rethink how they regulate certain activities. New technologies and new methodologies arising from those technologies, even when unrelated to existing regulations, may have significant and unexpected effects on how those regulations operate and are enforced.

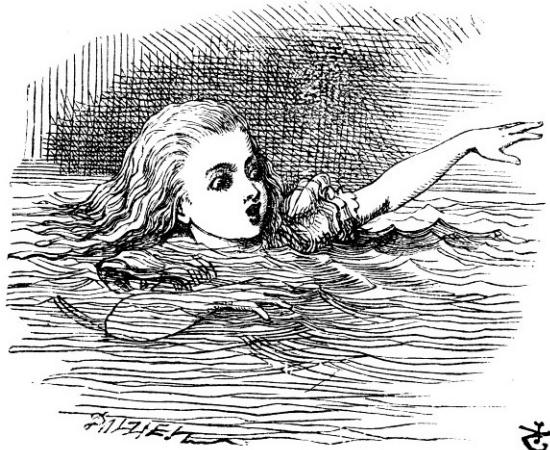
Change is constant

In a report, “Technology Will Keep Changing Everything—and Will Do It Faster,” Banning Garrett wrote,

Predicting how technology is developed and used—and the impact of that use—is inherently impossible and not a question of improved methods and information. Rather, it is dependent on the decisions of individuals—millions and billions of unpredictable, individual decisions.⁵⁸



"How puzzling all these changes are! I'm never sure what I'm going to be, from one minute to the other," [said Alice.]⁵⁷



"Alice swam about," Lewis Carroll, Alice's Adventures in Wonderland, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 20. No known copyright restrictions.

Garrett listed several ideas worth keeping in mind when attempting to forecast the effects of new technology, so as to determine whether, when, how, and why to regulate:

- » Technological disruption can result from a convergence of advances, as the Internet did from the technical leaps and plummeting costs of computing and communications. Now we have a confluence of blockchain, robotics, artificial intelligence, and the Internet of Things that is driving smart homes, autonomous vehicles, additive manufacturing, and cognitive supply chains.
- » The pace of technological change will continue to accelerate, and quantum computing is on the horizon. The arrival of a viable quantum computer—one that uses quantum bits (or “qubits”) rather than conventional bits—will usher in an unprecedented age of discovery. It will also undermine the cybersecurity of global finance and national defense.
- » Though behavioral economists have gotten better at anticipating the financial markets’ response to news, not all social systems behave according to laws as quantifiable and formulaic as those of physics.
- » With big data, social media, and prediction markets, we can leverage the wisdom of a large crowd of decision-makers and technology experts to identify emerging trends and imagine how society might adopt and adapt to these technologies.
- » Running scenarios can help regulators to consider worst cases, play out the effects of alternative regulations, and surface otherwise unintended consequences.

The pace of technological change will continue to accelerate, and quantum computing is on the horizon.



We agree. No one can say with certainty what impact the blockchain will have on society. Regulators can, however, develop scenarios and test assumptions as Garrett suggests. By identifying and understanding some basic and fundamental attributes of the blockchain, we can begin at least to identify the questions we should be asking in order to develop a potential blockchain regulatory framework. We can start by asking what we believe to be the most relevant question from a legal and regulatory point of view.

A regulatory approach: Ask fundamental questions

We will be better served if regulators ask some basic questions about blockchain and blockchain-based applications before enacting new regulations or applying existing regulations to unprecedented technologies and methods of doing business.

When regulators face an industry in a state of rapid evolution or revolution, that is, high uncertainty, regulators have three possible responses. They can make new laws through rulemaking and potentially through enforcement actions. They can refrain from taking any action and simply observe, study, and learn. Or they can watch developments and periodically issue reports, guidance, or threats. They may end up requiring some combination of the above. But determining which approach is optimal, we believe, must start with a process of informed questioning.

Some cases need regulatory intervention or immediate government response without the luxury of premeditative implementation process. Exigent circumstances such as the protection of human life must always take priority. In all other cases, we will be better served if regulators ask some basic questions about blockchain and blockchain-based applications before enacting new regulations or applying existing regulations to unprecedented technologies and methods of doing business.

The most basic is whether the blockchain should be self-regulated, government regulated, or unregulated. Historically, regulation often works best when it involves an appropriate balance, so we presume the answer will be to combine all three. Notwithstanding the views of blockchain anarchists, as the Internet has taught us, lack of physical boundaries does not put technology beyond the purview of regulators or above the need to regulate.

Does the use of the technology raise truly novel legal issues?

This is such a fundamental and critical question. If the answer is no, then we need to operate under an assumption that, instead, the blockchain gives rise to the same issues with which lawyers have grappled with for decades, only in a different medium. Whenever we are faced with radically new technology, there is a tendency to conclude that no one has ever before seen or addressed all of the regulatory issues it raises. This may be true at times.



Have policymakers based laws and regulations on a set of assumptions about the context in which they apply?

If blockchain technology enables us to pursue and achieve our existing objectives in new ways, then we may want to reconsider our understanding of those objectives. Further, we may need to reconsider how we regulate the pursuit and achievement of those objectives.

Have policymakers based laws and regulations on a set of assumptions about the context in which they apply? Significant technological advancements can alter how such laws and regulations function, even where the technological changes have nothing to do with the affected laws and regulations. Acknowledging this type of impact is a start. Whether that impact raises truly novel legal issues for which no existing precedent exists is a separate question. At the most general level of analysis, no legal questions are unique: they all involve human interaction, behaviors, and potential conflicts.

What is the “it” that we are potentially regulating?

"What do you know about this business?" the King said to Alice.

"Nothing," said Alice.

"Nothing whatever?" persisted the King.

"Nothing whatever," said Alice.

"That's very important," the King said, turning to the jury. They were just beginning to write this down . . . when the White Rabbit interrupted: "Unimportant your Majesty means, of course."⁵⁷



"'You're nothing but a pack of card,' cried Alice," Lewis Carroll, Alice's Adventures in Wonderland, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 98. No known copyright restrictions.

To regulate appropriately, we need to understand what we are seeking to regulate and why.

In the *Wall Street Journal*, James Mackintosh asked, "Is It Time to Regulate Bitcoin?"⁶⁰ It is a well-written article but it asks the wrong question. Again, this research paper is not intended to be an anti-regulation piece: the law plays an important role in the functioning of markets and in protecting, when necessary, individual market participants. Nevertheless, to regulate appropriately, we need to understand what we are seeking to regulate and why.

We cannot and should not talk about regulating bitcoin the cryptocurrency in isolation. Any discussion must encompass the whole blockchain ecosystem in which bitcoin and other



cryptocurrencies are components and distinguish between regulation of the ecosystem itself and regulation of applications utilizing distributed ledger technology. The former is akin to the regulation of the Internet, to the extent that it is a “thing” that can be regulated. The latter is akin to the regulation of email, an application that relies on the Internet backbone.

While some virtual or digital currencies are intended to serve a role similar to that of bitcoin, other types of coins or tokens perform or purport to perform functions (utilities) significantly different from bitcoin and its virtual currency cousins. Nor are the many distributed applications conceived to run on blockchain the same as cryptocurrencies or utility tokens.

From such differences arise different concerns, different constituencies, different markets, different industries, and different economic impacts. Regulatory efforts must incorporate such differences, if they are to succeed. For example, policymakers continue to debate whether cryptocurrencies are currencies, commodities, securities, computer code, or something else altogether. Perhaps they are a combination of the above.

In some cases, parties use bitcoin and other cryptocurrencies as an equivalent to money, to buy and sell goods.⁶¹ Consider these statistics:

Bitcoin is used by over 100,000 people, and hundreds of thousands of dollars' worth of bitcoin is traded every day. It even has greater volume transactions than Western Union and is becoming a real threat to PayPal, which explains the latter's decision to accept payments in bitcoin.⁶²

Economists define money as anything generally accepted in payment for goods or services or in the repayment of debts.⁶³ It falls within this broad definition to the extent that people use cryptocurrency to make payments for such goods and services as the following:

In certain countries, bitcoin is accepted for fee tuitions (Cyprus), in others for restaurants meals (restaurant Le Petit Jardin in Los Angeles), and since January 2013 the world's biggest retailer, Overstock.com, began accepting bitcoin, followed by Expedia, Wikipedia, and by Microsoft in December 2014.⁶⁴

Money has three functions—not just a means of exchange but a store of value and a unit of account—each of which is regulated. If cryptocurrencies have the same three characteristics, then regulating them as we regulate money might be appropriate.

However, just because bitcoin is accepted as payment in exchange for the delivery of goods or services does not mean that cryptocurrencies are money. It does mean that some parties will accept bitcoin instead of fiat currency as payment in exchange for goods or services.



From a legal perspective, cryptocurrencies do not presently qualify as a fiat currency, electronic money, or as a payment instrument.

Money is considered a store of value because it “retains its purchasing power over time with a good deal of certainty.”⁶⁵ Of course, we use other assets—stock, land, patents, art, gold—to store value. The same is potentially true of bitcoin and other cryptocurrencies, despite their recent price swings. After all, unsustainable fiscal and monetary policies can cause a fiat currency to experience such a high level of volatility and loss of value. Look at Venezuela. In August 2017, *Fortune Magazine* stated, “Venezuela’s real world currency—the bolivar—is worth less than fake gold in Azeroth, the mythical setting of World of Warcraft.”⁶⁶

Finally, money is considered a unit of account because we measure the value of goods and services in terms of money. As long as we can determine the relationship of the value of a cryptocurrency to the value of other goods and services for which it is exchanged, then the cryptocurrency can serve as a unit of account.

Is it money?

From a legal perspective, cryptocurrencies do not presently qualify as a fiat currency, electronic money, or as a payment instrument.⁶⁷ Bitcoin and other cryptocurrencies do not meet the strict definition of legal tender.⁶⁸ They are not backed by the full faith and credit of any government. But if cryptocurrencies function as money, should they nevertheless be regulated as such or at least in a comparable manner?

The Financial Action Task Force (FATF), an inter-governmental body established in 1989, defined *virtual currency* as “a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value.”⁶⁹

According to the FATF, virtual currency “does not have legal tender status . . . in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency.”⁷⁰

While FATF chose to use the term “virtual currency,” the definition effectively applies to cryptocurrencies as well. According to FATF, a cryptocurrency is simply a math-based, decentralized convertible virtual currency protected by cryptography. By “convertible,” FATF means that cryptocurrency has a value that can be determined in fiat currency and can be exchanged back and forth for fiat currency.

FATF further distinguished centralized from decentralized virtual currencies such as bitcoin, which are “distributed, open-source, math-based peer-to-peer virtual currencies that have no central administering authority and no central monitoring or oversight.”⁷¹ In contrast, under the FATF dichotomy, many of the recent initial coins offered would be examples of centralized ones:



Centralized virtual currencies have a single administrating authority (administrator)—[that is], a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation).⁷²

The FATF definition provides a convenient way to differentiate between fiat currencies and cryptocurrencies:

Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from emoney, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.⁷³

From a legal perspective, cryptocurrencies do not presently qualify as a fiat currency, electronic money, or a payment instrument.⁷⁴ They do not meet the strict definition of legal tender; they are not backed by the full faith and credit of any government.⁷⁵ Jay Clayton, Chairman of the SEC, stated:

Cryptocurrencies purport to be items of inherent value (similar, for instance, to cash or gold) that are designed to enable purchases, sales, and other financial transactions. They are intended to provide many of the same functions as long-established currencies such as the US dollar, euro, or Japanese yen but do not have the backing of a government or other body.⁷⁶

Does the distinction between centralized and decentralized virtual currencies warrant different regulatory approaches?

Is it a commodity?

But if cryptocurrencies function as money, should they be regulated in a comparable manner? Does the distinction between centralized and decentralized virtual currencies warrant different regulatory approaches? Or should regulators consider ICOs that fall within FATF's centralized category to be "something else" entirely?

In the United States, for example, the Commodity Futures Trading Commission (CFTC) considers bitcoin and other comparable virtual currencies to be commodities under the US Commodities Exchange Act and the related rules thereunder.⁷⁷ The CFTC treats bitcoin as an exempt commodity, putting it in the same category as a precious metal. To date, the CFTC has not provided any clear delineation as to which type of coin constitutes a virtual currency and which, a commodity.

The tokens issued in many ICOs have features very different from bitcoins and may not easily fall within the FATF definition of virtual currency. Some ICO-issued tokens give their holders rights to some



Purchasing an alternative blockchain token is less like an investment in a traditional currency and more like an equity investment in a company.

form of future profits and, accordingly, may be the digital equivalent of equity securities. Some tokens act as digital title to tangible assets such as real estate. Still others give their holders the right to participate in projects or businesses—so-called “access tokens” where the token holders expect to profit in some manner from such access or participation.

To some extent, many of these alternative blockchain tokens function less like traditional currencies and more like membership interests or frequent flyer miles because they only work within a closed network or business and can only be used for a particular service or product. However, membership interests and frequent flyer miles, if transferable at all, are typically subject to transfer restrictions.

In contrast, blockchain tokens are typically freely tradable; and numerous exchanges have formed for speculators to buy and sell various cryptocurrencies comparable to traditional foreign exchanges or securities markets.

Is it a security?

Just as we can see the value of an individual bitcoin tied to the value of the Bitcoin network, presumably, alternative blockchain tokens trade at prices based on the perceived value of the platforms and projects associated with them. In this context, purchasing an alternative blockchain token is less like an investment in a traditional currency and more like an equity investment in a company. Jay Clayton, Chairman of the SEC, stated:



"The White Rabbit as herald," Lewis Carroll, Alice's Adventures in Wonderland, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 89. No known copyright restrictions.



Coinciding with the substantial growth in cryptocurrencies, companies and individuals increasingly have been using initial coin offerings to raise capital for their businesses and projects. Typically, these offerings involve the opportunity for individual investors to exchange currency such as US dollars or cryptocurrencies in return for a digital asset labeled as a coin or token.⁷⁸

In contrast to bitcoin, which comes into circulation through mining, tokens or *alternative coins* (altcoins) may be sponsored by a developer and introduced to the market through a crowdfunding-type sale such as an ICO. These cryptocurrencies fall within the FATF's centralized virtual currency category. The purposes for conducting token sales vary, but the goals are typically to raise money by offering the new token to fairly a large group at a perceived discount from its potential future value in order to fund projects, pay developers, and incentivize early adopters. To date, the SEC has generally taken the view that most, if not all, tokens distributed in ICOs constitute securities under US law and should be regulated as such:

These offerings can take many different forms, and the rights and interests a coin is purported to provide the holder can vary widely. . . . By and large, the structures of initial coin offerings that [Chairman Clayton has] seen promoted involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws. Generally speaking, these laws provide that investors deserve to know what they are investing in and the relevant risks involved.⁷⁹

The SEC Chairman also clarified that, even though "[it] has been asserted that cryptocurrencies are not securities and that the offer and sale of cryptocurrencies are beyond the SEC's jurisdiction," the SEC still has a responsibility:

[J]ust as the SEC has a sharp focus on how US dollar, euro, and Japanese yen transactions affect our securities markets, we have the same interests and responsibilities with respect to cryptocurrencies. This extends, for example, to securities firms and other market participants that allow payments to be made in cryptocurrencies, set up structures to invest in or hold cryptocurrencies, or extend credit to customers to purchase or hold cryptocurrencies.⁸⁰

For the moment, the classification of cryptocurrencies remains a contentious subject.

For the moment, the classification of cryptocurrencies remains a contentious subject. Some cryptocurrencies can be used as a method of payment, some may function as commodities, and some may resemble securities-like investments. What is clear is that, when regulators cannot agree on what a cryptocurrency is, they will not likely develop a rational regulatory regime.



Do or should existing laws apply to blockchain technology?

By identifying instances in which a blockchain application represents a new medium for conducting business rather than an entirely new activity, regulators can logically determine the extent to which the existing regulatory environment is suitable. Every new medium raises complex legal questions, the most fundamental of which is whether regulators should apply existing laws designed for prior media to the new medium as well.

For example, in 2013, the Financial Crimes Enforcement Network (FinCEN) under the US Department of the Treasury issued interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act (BSA) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.⁸¹ FinCEN defines *fiat currency* as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."⁸²

Every new medium raises complex legal questions, the most fundamental of which is whether regulators should apply existing laws designed for prior media to the new medium as well.

FinCEN's definition of virtual currency as a medium of exchange, which operates like a currency in some environments but lacks all the attributes of real currency, resembles that of the FATF. FinCEN defines *money transmitter* as a person who provides money transmission services or engages in the transfer of funds and *money transmission services* as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."⁸³

FinCEN also defines convertible virtual currency using the FATF approach: a user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not a *money services business* (MSB), but an administrator or exchanger who (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter.

According to the FinCEN guidance, its "definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA."⁸⁴ As a result, an MSB must comply with US anti-money laundering and counter-terrorist financing regulatory requirements under the BSA. If an MSB is a US person, then the MSB must also comply with prohibitions of the Office of Foreign Assets Control regarding specially designated nationals or blocked persons.

While virtual currencies may constitute a new medium for paying for goods or services, FinCEN had no trouble applying the same money transmitter rules to convertible virtual currencies as to fiat



*When exactly is a cryptocurrency the equivalent of a fiat currency and not a commodity?
When is it a commodity?
When is it a security? When is it none of the above?*

currencies. To the extent that a virtual currency serves the same function as a fiat currency, and parties are using it in the same way for the same purpose, then why shouldn't some regulations that apply to fiat currency also apply to virtual currency?

That seems reasonable, but when exactly is a cryptocurrency the equivalent of a fiat currency and not a commodity? When is it a commodity? When is it a security? When is it none of the above? The problem created by the FinCEN guidance is not so much that it treats convertible virtual currencies as fiat currencies for purposes of the BSA. Rather, the problem is that, in a complex US regulatory environment, all the relevant regulators did not work together to provide clear and comprehensive guidance for answering those questions and determining when a cryptocurrency is subject to one set of regulatory requirements or another.

Will existing laws have the same effect on new technology?

Just because policymakers can make existing laws work for blockchain applications does not mean that they should. In the interim, applying existing laws may be expedient or even necessary, especially where regulators need more time to study these innovations. Because new blockchain technologies evolve rapidly, often in unexpected ways, policymakers may not be able to answer this question without observing the new technology in action over time.

Consider how the SEC has been grappling with the booming ICO market. According to the US Securities Act of 1933:

The term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security," or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.⁸⁵

Let's focus on the reference to *investment contract*, not defined separately in the Securities Act of 1933. Instruments that, because of their terms or unique features, do not fall within the straightforward elements of the security definition may be deemed



an investment contract, and so we must look at legal precedents and SEC pronouncements for guidance on what the SEC considers an investment contract.

The Howey test

The most common interpretation comes from a seminal US Supreme Court case, *SEC v. WJ Howey Co.*⁸⁶ In *Howey*, a promoter offered tracts in a citrus grove coupled with a ten-year service contract under which an affiliate of the promoter would cultivate the groves and harvest and market the fruit. Upon full payment, title to the land would be conveyed to the purchasers. The service company received a specified fee plus the cost of labor and materials as well as full discretion and authority over cultivation, harvesting, and marketing. The company was accountable for an allocation of net profits to the purchasers of grove tracts following harvest.

The Court concluded that the arrangement constituted an investment contract, defined as "a contract or scheme for 'the placing of capital or laying out of money in a way intended to secure income or profit from its employment.'"⁸⁷ In *Howey*, the Supreme Court identified four factors (often referred to as the *Howey* test) that, if present, would suggest the existence of an investment contract and, thus, a security: (i) an investment of money, (ii) in a common enterprise, (iii) with an expectation of profits, (iv) to be derived solely from the efforts of others.⁸⁸

Importantly, as stated by the Supreme Court, the *Howey* test "embodies a flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."⁸⁹ In a subsequent decision, the Supreme Court elaborated, stating, "In searching for the meaning and scope of the word 'security' . . . form should be disregarded for substance and the emphasis should be on economic reality."⁹⁰ In other words, just because something is called a cryptocurrency or described as a token does not automatically mean that it is not a security.

The *Howey* Court noted that, although the Securities Act does not provide a definition for the term "investment contract," other courts have construed the term broadly by favoring the substance of the transaction over its form and emphasizing its economic reality. Subsequent court decisions as well as the SEC have applied the *Howey* test to determine whether an arrangement, agreement, or understanding is an investment contract under the Securities Act.

The DAO

In July 2017, the SEC reported on its first investigation of an ICO involving "the DAO," a *decentralized autonomous organization* formed by German company Slock.it. The DAO's chief technology officer described it as a for-profit entity: buying its tokens was comparable to buying shares in a company and receiving dividends.⁹¹



To raise capital, the DAO conducted a public ICO in which it sold its tokens, called TheDAO. These tokens provided holders with both voting and ownership rights. A team referred to as *curators* would screen, select, and submit potential projects to TheDAO token holders who would vote whether to fund the proposed projects. Token holders would also be entitled to vote whether to reinvest any profits from funded projects in new projects or to distribute profits to token holders. They could also potentially receive a return by selling their tokens through various web-based secondary-trading platforms.⁹²

In its analysis, the SEC applied the *Howey* test to the DAO and determined that TheDAO tokens constituted an investment contract and, thus, a security under the Securities Act.⁹³ The DAO did not create its own blockchain. Instead, it was intended to run on top of Ethereum. The SEC also noted that, after the DAO was hacked in June 2016, its creators hardforked the Ethereum blockchain and enabled token holders to reclaim their funds.⁹⁴ The DAO contract was effectively unwound.⁹⁵

Munchee Inc.

SEC found that Munchee's token sale constituted a securities offering and that, because Munchee neither filed a registration statement nor qualified for an exemption from registration, it was in violation of US federal securities laws.

In December 2017, the SEC did more than report on a particular ICO: it took action, initiating a cease-and-desist proceeding against Munchee in connection with its sale of digital tokens to raise capital for its blockchain-based food review platform.⁹⁶ Munchee created a mobile app for users to review restaurants and post photos in exchange for digital MUN tokens. Again using the *Howey* test, the SEC found that Munchee's token sale constituted a securities offering and that, because Munchee neither filed a registration statement nor qualified for an exemption from registration, it was in violation of US federal securities laws.

In the Munchee order, the SEC repeated what it said in the DAO report: "Tokens, coins, or other digital assets issued on a blockchain may be securities . . . and if they are securities, issuers and others who offer or sell them in the United States must register the offering and sale with the Commission or qualify for an exemption from registration."⁹⁷

Munchee sought to raise about \$15 million in ether by selling 225 million tokens out of the 500 million total tokens created by Munchee. Munchee said it would use the tokens it kept to support its business, including by paying rewards in the Munchee app with its tokens, paying its employees and advisors with tokens, and facilitating advertising transactions in the future.

In its white paper describing its business and tokens, Munchee said that it would run its business in ways that would cause token value to appreciate.⁹⁸ It would use the proceeds from the ICO to build an "ecosystem" that would create demand for its tokens and make the tokens more valuable. Munchee intended to revise the Munchee app so that people could buy and sell services using tokens. Munchee



Munchee and its agents targeted the marketing of the token offering to people with an interest in cryptocurrencies and tokens that had in recent years created profits for early investors in ICOs.

also planned to recruit “partners” such as restaurants willing to sell meals in exchange for tokens.

In its white paper, Munchee also stated that it would work to ensure that the token holders would be able to sell their tokens on secondary markets, stating that it would ensure that its tokens available on a number of cryptocurrency exchanges in multiple jurisdictions. Munchee also stated that its tokens would be available for trading on at least one US-based exchange within 30 days of the conclusion of the ICO. Finally, Munchee stated that it would buy or sell tokens using its retained holdings in order to ensure there was a liquid secondary market in the tokens.

Like many token issuers, Munchee maintained that its token was a “utility token,” not a security. In its white paper, it referred to the SEC’s DAO report and stated that it had conducted its own “Howey analysis” and determined that, as currently designed, the sale of its utility tokens did “not pose a significant risk of implicating federal securities laws.”⁹⁹

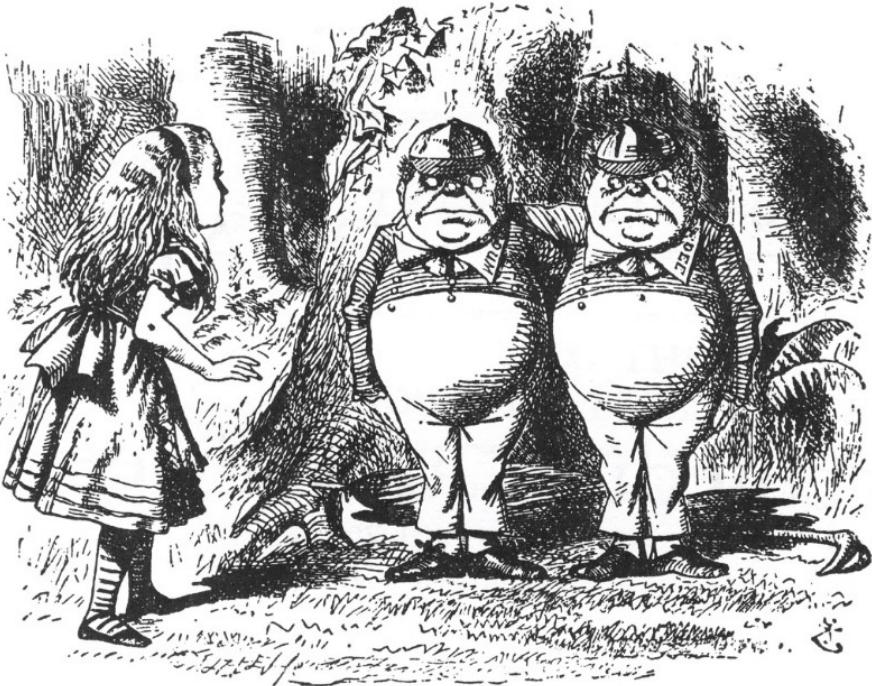
The SEC rejected this conclusion. It noted that Munchee made public statements or endorsed other people’s public statements that touted the opportunity to profit by acquiring tokens. Munchee and its agents targeted the marketing of the token offering to people with an interest in cryptocurrencies and tokens that had in recent years created profits for early investors in ICOs.

The SEC concluded that investors reasonably expected they would profit from any rise in the value of Munchee’s tokens created by the revised Munchee app and by Munchee’s ability to create an “ecosystem”—for example, the system described in the ICO where restaurants would want to use Munchee tokens to buy advertising from Munchee or to pay rewards to app users, and where app users would want to use tokens to pay for restaurant meals and would want to write reviews to obtain additional tokens.¹⁰⁰

In the eyes of the SEC, investors’ profits would be derived from the significant entrepreneurial and managerial efforts of others—specifically Munchee and its agents—who were to revise the Munchee app, create the ecosystem that would increase the value of Munchee tokens (through both an increased demand for tokens by users and Munchee’s specific efforts to cause appreciation in value, such as by burning tokens), and support secondary markets. Investors had little choice but to rely on Munchee and its expertise.

At the time of the ICO, purchasers could not actually use Munchee tokens. The Munchee platform was not yet operational. Buyers of tokens could either hold their tokens and wait for the platform to become operational or sell them to third parties. To the SEC, this looked like a pooled investment in which investors were taking on collective enterprise risk. Perhaps one of the most important statements in the Munchee order is the following:





"Tweedledum and Tweedledee," Lewis Carroll, *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 137. No known copyright restrictions.

Even if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labeling—such as characterizing an ICO as involving a "utility token"—but instead requires an assessment of "the economic realities underlying a transaction."¹⁰¹

For all of the above reasons, the SEC determined, "Purchasers reasonably would have viewed the MUN token offering as an opportunity to profit," whether they used the Munchee app or otherwise contributed to the Munchee platform.¹⁰² Investors' expectations were primed by Munchee's marketing of the ICO. The SEC believed that Munchee primed purchasers' reasonable expectations of profit through statements on blogs, podcasts, and Facebook that talked about profits.

Had Munchee's marketing not focused so explicitly on prospective investors and the future profit and investment potential of the tokens rather than on app users, advertisers, and the token's utility in Munchee's ecosystem, the outcome might have been different.

We are sympathetic to the SEC's position. Unlike the DAO, Munchee was US-based—no one questioned the SEC's assertion of jurisdiction over Munchee—and the SEC could not ignore how Munchee marketed its tokens. However, to reach this outcome, the SEC glossed over another aspect of the *Howey test*.

The SEC believed that Munchee primed purchasers' reasonable expectations of profit through statements on blogs, podcasts, and Facebook that talked about profits.



The exception to the *Howey* test

In *United Housing Found, Inc. v. Forman*, a Supreme Court case that came after the *Howey* decision, the Court defined *profit* of the *Howey* test as either

[C]apital appreciation resulting from the development of the initial investment . . . (sale of oil leases conditioned on promoters' agreement to drill exploratory well), or a participation in earnings resulting from the use of investors' funds . . . (dividends on the investment based on savings and loan association's profits).¹⁰³

In that case, the Court distinguished other scenarios noting, "By contrast, when a purchaser is motivated by a desire to use or consume the item purchased—to occupy the land or to develop it themselves,' as the *Howey* Court put it, . . . the securities laws do not apply."¹⁰⁴

Investors purchase securities "not with an eye toward personal use or consumption of the underlying interest . . . but rather for the purpose of acquiring an interest in a profit-making venture."

So if a token purchaser's primary motivation in acquiring a token is to spend it on goods and services that can only be acquired with the token, then does it matter whether that purchaser also expects the token to appreciate in value? Many tokens sold in ICOs are ultimately intended to be consumed, that is, spent like bitcoin and fiat currency. As indicated in *United Housing Found v. Forman*, the mere existence of a profit motive does not automatically make the proposed transaction a security. Rather, a purchaser's profit expectation must be the predominate motivation for the purchase.¹⁰⁵ As the Supreme Court stated,

What distinguishes a security transaction—and what is absent here—is an investment where one parts with his money in the hope of receiving profits from the efforts of others, and not where he purchases a commodity for personal consumption or living quarters for personal use.¹⁰⁶

In other words, investors purchase securities "not with an eye toward personal use or consumption of the underlying interest . . . but rather for the purpose of acquiring an interest in a profit-making venture."¹⁰⁷ In the Munchee order, the SEC did not address the consumption purpose of MUN tokens.

The SEC was likely more concerned with protecting individual investors and preserving the integrity of U.S. securities markets. Had neither the DAO nor Munchee sold tokens as a means to raise capital, the SEC would not have had a potential role to play.

Where a cryptocurrency is the sole means by which users can access a blockchain platform and obtain (purchase) goods and services, that cryptocurrency has features similar to bitcoin and other virtual currencies. However, when the creator of that cryptocurrency initially sells it to fund development or completion of that platform, any early purchaser of that cryptocurrency takes on enterprise risk that the



A cryptocurrency or token is unique and can act like a currency, a commodity, a security, or some combination of the three.

platform will never be completed and the cryptocurrency will never be useable and, as a result, have no future value.

If we had examples of instruments used simultaneously as a currency and as a security, then we would have regulatory precedents to apply. But we don't. Not yet. We do have many examples of pooled vehicles created for investing in one or more currencies. But those vehicles ultimately involve the issuance of securities held as a speculative investment based on the value of the underlying currencies.

Will the SEC's determinations help or harm us?

Notwithstanding the valid public policy and regulatory concerns of the SEC, have the SEC's determinations to date with respect to ICOS been helpful or harmful? A cryptocurrency or token is unique. Depending on its characteristics, how it is being used, and who is using it, it acts like a currency, a commodity, a security, or some combination of the three.

If the SEC insists on pushing most token offerings into a securities law bucket, this will represent a failure to recognize all the ways cryptocurrencies are being and will be used. It also fails to recognize that cryptocurrencies may present a completely new way of raising capital that, although subject to some form of regulation, should not be treated as traditional securities offerings.

When regulators simply apply existing regulatory regimes to what could be new paradigms, we are likely to have unintended outcomes, particularly that negatively skew how new technology rolls out. How we develop and use cryptocurrencies should tell us that we cannot and should not force them into an existing regulatory regime if that regime is not sufficiently flexible and robust to address the new and unique attributes of cryptocurrencies.

Equally, the regulatory responsibility is often bifurcated among multiple regulatory bodies, as it is in the United States; individual regulatory bodies ought not step headfirst into new technologies such as blockchain without carefully coordinating with the other regulators who may legitimately have an interest and be more appropriately suited to play a role.

What are the costs and benefits of new or special regulation?

Any time officials propose new laws and regulations, they ought to conduct a rigorous cost/benefit analysis to understand the object of potential new regulation. More often, however, little is known about the new, rapidly evolving technology or industry. Issuing specific or new rules based on hypotheses about their future increases the risk of creating a bad law or rules much worse than those issued after such analysis.



Global consensus and coordination among regulators are critical.

Instead of providing clarity, premature rulemaking can actually create a significant lack of clarity for emerging industries, particularly where poorly thought out or unimaginative rules result in multiple judicial challenges. When the market must spend resources attempting to predict which rules will likely survive and which will be overturned, the regulatory outcome will be more uncertainty, not less. At the very least, informal processes may be the best approach, giving regulators time to conduct helpful cost/benefit analyses prior to implementing new, formal rules.

Whose law should apply?

Regardless of whether policymakers decide to apply existing regulations, or modify them, or implement new ones, the only way to avoid failure and unintended consequences is to understand the seamless nature of blockchain applications and their ability to transcend traditional boundaries. Global consensus and coordination among regulators are critical.

Where human activity is global, history shows us that effective global regulatory approaches typically require governmental and institutional cooperation and supranational implementation. Coordinating bodies, either formed or endorsed by multiple governments, may be more appropriate and effective in regulating borderless technologies.

Blockchain communities have no geographic boundaries, and the location of participants may be unavailable. Criteria for defining membership and the boundaries of governance are unavailable for many blockchain applications. The power to control activity in cyberspace—particularly with the anonymity supported by blockchains—has a tenuous connection to the physical location of participants.

Questions such as the extent of disclosure required to offer goods or services, the types of behaviors that constitute actionable “fraud,” or the conditions under which parties can rescind a transaction are examples of the issues that arise daily in global commerce. The world has a rich jurisprudence for dealing with these types of conflicts of law. But regulators will need to determine whether the existing approaches for resolving legal conflicts will continue to work in the world of blockchain. In any case involving cyber activity, complex fundamental questions arise as to how to determine both the location of the participants and the various jurisdictions “touched” by the cyber activity.

The power to control activity in cyberspace has a tenuous connection to the physical location of participants.

Some have expressed concern that blockchain ecosystems will give rise to legal uncertainty due to the inability to enforce contractual relationships. Some argue there may be no central administering authority to decide a dispute, no obvious defendant, or no ability to enforce a court judgment or arbitration award in a transaction on the blockchain.



Parties can include dispute resolution arrangements in smart contracts as they would in traditional contractual relationships.

Are these concerns valid? No, we have a rich and robust history under conflicts of laws principles that provide guidance as to which jurisdictions laws apply to a particular activity or circumstances and how such determination is made. In many cases, the starting point as a matter of contract law is the agreement between transacting parties, specifically which jurisdiction's laws they want to apply to their relationship. Moving to a blockchain ecosystem that relies on smart contracts does not change this matter. Parties agreeing to use smart contracts will continue to have the ability to elect a governing law and to submit voluntarily to the jurisdiction of the courts of a particular country.

Parties can include dispute resolution arrangements in smart contracts as they would in traditional contractual relationships. We recognize that the automated execution of smart contracts is intended to ensure performance without resorting to courts. However, as much as some believe that properly designed smart contracts will eliminate unanticipated contingencies, we remain skeptical of the code's or the coder's ability to obviate contractual disputes.

A modest proposal: Follow these regulatory principles

We must always clearly identify the primary rationale for regulation. We can use our experience with regulation of the Internet and financial innovation to understand what has worked and what has not. To a significant extent, the same rationale is relevant for the blockchain:

- » Improve data gathering and sharing
- » Fill newly exposed or created regulatory gaps
- » Incentivize strong corporate stewardship beyond regulatory requirements
- » Enhance agency expertise and coordination
- » Provide for regulatory adaptability and flexibility
- » Achieve substantial, diverse stakeholder involvement
- » Maximize international collaboration among regulators
- » Minimize interagency turf wars among regulators.

We must always clearly identify the primary rationale for regulation.

At times, regulation may be a critical component for creating the right kind of environment for technology to advance. For example, there is no sure answer to, "Is this cryptocurrency a security, a commodity, a currency, or something else?" Without regulatory certainty, we cannot easily identify whether and how a particular



cryptocurrency is regulated, how it may be used, distributed, or traded, who is entitled to buy it, how it is taxed, which legal rights it gives its holders, or who may be accountable when problems arise. Such unknowns, when combined with the potential to unknowingly cross-regulatory lines, can impede the deployment and adoption of new technologies.

Circumstances where a market needs regulatory clarity and certainty to grow and survive serve as a strong rationale for regulatory action, as long as it is done in the right way.

Match as best as possible regulatory implementation to technology evolution

When an economy or a society is undergoing rapid change, traditional regulatory approaches do not work.

According to MIT professors Erik Brynjolfsson and Andrew McAfee, we are fast approaching “an inflection point in the history of our economies and societies because of digitization. It’s an inflection point in the right direction—bounty instead of scarcity, freedom instead of constraint—but one that will bring with it difficult challenges and choices.”¹⁰⁹ Among them will be regulatory implementation.

When an economy or a society is undergoing rapid change, resulting in conditions of high uncertainty, traditional regulatory approaches do not work. Environments in which facts are unclear and evolving

“Who are you?” said the Caterpillar.” Alice replied, rather shyly, “I—I hardly know, sir, just at present—at least I know who I was when I got up this morning, but I think I must have been changed several times since then.”¹⁰⁸



“The caterpillar addressing Alice,” Lewis Carroll, Alice’s Adventures in Wonderland, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 38. No known copyright restrictions.



At times, a wait-and-see approach may make sense and may be the only feasible approach.

create a constantly moving target that can remain beyond the ability of regulators to understand and manage. Technology that evolves as quickly and as unpredictably as the blockchain renders rigid regulations obsolete as soon as they have been issued. Timing is thus a crucial element because it is axiomatic that technological change happens faster than social change and regulatory responses.

As we enter what Brynjolfsson and McAfee call “a second machine age,” they “hope that regulation . . . will not be stifling.”¹¹⁰ They foresee “a continued patchwork of regulations in many areas” but believe that policymakers should “try to reduce the regulatory burden” on entrepreneurs.¹¹¹

At times, a wait-and-see approach may make sense and may be the only feasible approach. Where we simply cannot anticipate the direction of a new industry or technology, we may want or even need to allow the new industry or technology to develop organically. Of course, such an approach, if followed too long, can have negative consequences ranging from lack of adequate public protection to environmental externalities. The SEC, for example, has acted in the interest of small investors in the overheated ICO space.

On the flip side, a garden intended for too long allows for undesirable norms and business practices to take root. At this point, rulemaking may not easily eradicate or reverse norms and practices. A watchful, incremental approach can potentially strike the right balance between premature action and acting too late to avert harm.

Harvard Business School professors Marco Iansiti and Karim R. Lakhani argue that blockchain is a foundational technology, rather than a disruptive technology. By that, they mean that the blockchain has the potential to provide a new foundation for our economic and social systems; and, although the impact will be enormous, it will take decades for blockchain to underpin our economic and social infrastructure.¹¹² In contrast, they borrow from their colleague Clayton Christensen’s definition of a disruptive technology as one that can attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly.¹¹³

Iansiti and Lakhani assert that the adoption of foundational technologies typically happens in four phases and that each phase is defined by the novelty of the applications and the complexity of the coordination efforts needed to make them workable:

- » Users initially adopt single-purpose applications that are low in novelty and complexity such as Overstock.com’s acceptance of bitcoin payments. Iansiti and Lakhani draw parallels between blockchain and TCP/IP development:

Just as email enabled bilateral messaging, bitcoin enables bilateral financial transactions. The development and maintenance of blockchain is open, distributed, and shared—just like TCP/IP’s. A team of volunteers around the world maintains the core software. And just like email, bitcoin



first caught on with an enthusiastic but relatively small community.¹¹⁴

- » Substitute applications are the next to gain traction. These are not particularly novel but require coordination such as the use of Ripple to execute cross-border payments.
- » Then localized applications develop, where whole industries adopt such practices as Walmart's permissioned blockchain for food provenance (though such an effort will require much coordination).
- » Applications high in novelty and complexity such as self-executing smart contracts take decades to evolve, as will the knowledge required to use them and the expertise required to create and audit them. TCP/IP took 30 years to move through these phases to reshape the economy and society. Iansiti and Lakhani note:

Today more than half the world's most valuable public companies have Internet-driven, platform-based business models. . . . Physical scale and unique intellectual property no longer confer unbeatable advantages; increasingly, the economic leaders are enterprises that act as "keystones," proactively organizing, influencing, and coordinating widespread networks of communities, users, and organizations.¹¹⁵

Blockchain technology may follow a developmental path similar to that of the Internet, but it may do so at a much faster pace than many predict.

Iansiti and Lakhani's four phases can help regulators to anticipate how blockchain technologies will develop. Regardless of whether we characterize blockchain as disruptive or foundational—and that may be a false dichotomy—the development of regulation should track with the development of the technology, neither getting too far ahead nor lagging too far behind. Blockchain technology may follow a developmental path similar to that of the Internet, but it may do so at a much faster pace than many predict. Regulators cannot afford to underestimate the speed, the force, or the breadth of this development.

Focus on buy-in and identify new ways to achieve existing goals

The blockchain and its applications are likely to allow us to achieve preexisting goals in new ways that require us to rethink the way certain activities are regulated. Regulations are typically premised on preexisting assumptions as to the context in which those regulations will operate. New technologies and new methodologies arising from those technologies, even when unrelated to existing regulations, may have significant and unexpected impacts on how those regulations operate and are enforced. The Internet unlocked new economic value by dramatically lowering the cost of connections.



As the blockchain becomes the new system of record for transactions, blockchain-based solutions will grow in influence and control and result in an economy-wide radical shift.

Similarly, the blockchain will change ways transactions are completed and will result in a reallocation of transaction costs. As the blockchain becomes the new system of record for transactions, blockchain-based solutions will grow in influence and control and result in an economy-wide radical shift. Regulations that are premised on certain approaches and embedded costs will need to be redesigned.

Regulatory responses, particularly those to promote marketplace buy-in, must identify the actors and aspects of the preexisting commerce, data management, financial systems, and so forth that blockchain technology could disintermediate. Regulations premised on the ongoing participation of such actors must be reexamined. Either those actors would need to be incentivized to continue to perform regulatory significant activities or alternative forms of regulation would need to be explored.

Market supervisors would be wise to determine whether new microstructures or new institutions could fill the vacuum created by new ways of engaging in activities on the blockchain that make certain actors or methods of interaction obsolete. The European Parliament suggested using permissioned blockchains for existing systems and structures, effectively maintaining the role and power of existing intermediaries by providing the basic functionality of blockchains without full decentralization and transparency.¹¹⁶

Target the use and the user, not the blockchain itself

When thinking about blockchain regulation, we need to distinguish upfront between regulation of the blockchain itself and regulation of applications (such as cryptocurrencies) that utilize blockchain technology. The blockchain pushes the ability to develop and use applications to the ultimate user. Because applications will drive blockchain usage, they should also drive legal analysis, and so policymakers should always begin with the application, how it is used, and who will use it.

From a legal standpoint, it may be a function of a particular blockchain application that is at issue, not necessarily the blockchain protocols themselves. Policymakers should focus on users and how they are harmed or helped by blockchain applications. Such an approach should help regulators to identify and analyze the social costs and benefits derived from blockchain applications.

Bitcoin is a perfect example. It has many different uses that, in turn, touch many types of users. Fundamentally, depending on who is using bitcoin and why, it may function as a form of payment comparable to fiat currency, it may act as a type of speculative investment, or it may fuel the core functioning of an application. The chameleon-like characteristics of many cryptocurrencies should tell us that a one-sizefitsall regulatory approach simply cannot work.

For example, US securities laws apply different regulatory approaches depending on who is buying and selling a security. As a policy matter, regulations provide a greater level of protection for

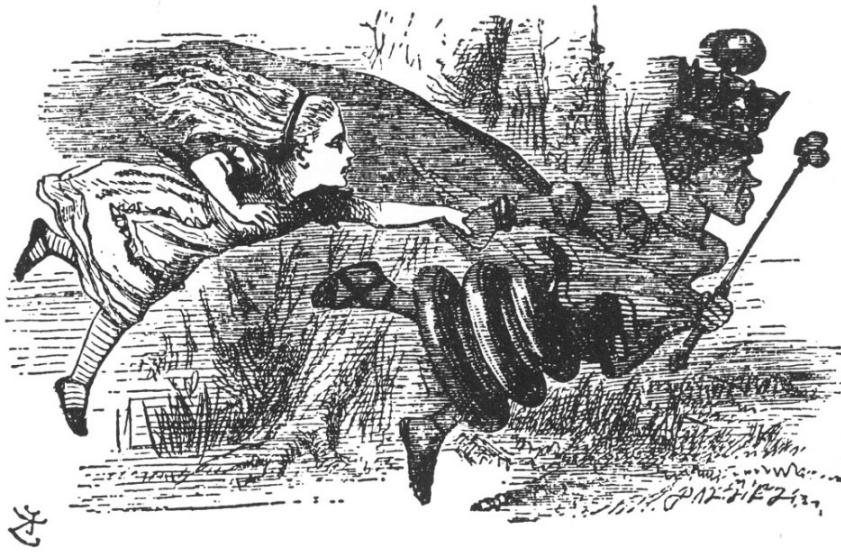


individual investors, since large institutional investors presumably can undertake more sophisticated investment analyses and absorb greater economic risk.

On the other hand, regulators apply more scrutiny to institutional investors with respect to market manipulation. Individuals are unlikely to have sufficient economic clout to raise the same levels of concern. As a policy matter, brokers and exchanges have special regulatory responsibilities to help assure the safety and soundness of securities markets.

Use a flexible, yet strong (even threatening) approach

They were running hand in hand, [Alice and the Queen,] and the Queen went so fast it was all [Alice] could do to keep up with her; and still the Queen kept crying, "Faster! Faster!" Alice felt she could not go faster. . . . However fast they went, they never seemed to pass anything.¹¹⁷



"'Faster! Faster!' cried the Queen," Lewis Carroll, *Through the Looking Glass: and What Alice Found There*, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 41. No known copyright restrictions.

Just as Alice and her fellow players could never get ahead, so too will the world's regulators remain just behind the advance of blockchain and related technologies.

Figuring out how to regulate a rapidly evolving technology is like the Red Queen's race. Just as policymakers think they have figured out the right approach to regulating the complex interplay among innovations, industries, players, products, business models, and market practices, everything morphs again and the newly implemented regulations are again out of alignment. Just as Alice and her fellow players could never get ahead, so too will the world's regulators remain just behind the advance of blockchain and related technologies. In that sense, regulatory reach is always beyond the regulator's grasp of a technology.



Combining a wait-and-see approach with the occasional regulatory threat may give regulators time to learn about new technologies while selectively intervening to protect the public.

Some have argued that the best regulatory approach in this type of environment may be the use of regulatory threat, that is, the threat to enact new laws or impose new regulations. Regulatory threats take the form of warning letters, interpretations, reports such as the SEC's investigation of the DAO, speeches by the heads of regulatory bodies, private meetings with potentially regulated parties, and enforcement actions such as the SEC's against Munchee.¹¹⁸

Tim Wu divides industries into two states, stable and dynamic, and argues that regulatory threat works better in the latter case: "In a stable industry, business models are relatively settled, and the facts relevant to regulation are therefore likely clearer. Conversely, in a dynamic industry, the agency confronts what economists call conditions of 'high uncertainty,'" where identifying alternative future states with a quantifiable level of probability is difficult.¹¹⁹ Wu notes,

What creates a dynamic industry is some kind of external shock to an existing industry. . . . Given such a shock, the industry's business models begin to change, and the future shape or function of the industry may be difficult to predict. It is under such conditions that threat regimes are more justified and, indeed, attractive.¹²⁰

Combining a wait-and-see approach with the occasional regulatory threat may give regulators time to gather facts and feedback, undertake necessary cost/benefit analyses, and learn about new technologies while selectively intervening to protect the public. It may also allow regulators to overlay a level of public policy on the development of norms and practices without implementing rules that may not make sense or be sufficiently flexible for a new and rapidly evolving technology.

Selective regulatory threats can serve as pilot programs for eventual rulemaking. They may initiate beneficial public debate not possible through formal rulemaking processes dominated by lawyers and lobbyists. At times, regulatory threats may result in the establishment of industry norms and practices and eliminate

Table 2: Examples of external shocks

Type	Example	Disrupted
Disruptive innovation	Commercialization of the Internet	Government postal service, telephone service, traditional media sources
Unexpected market entry	Amazon.com in retail	Bricks-and-mortar retail
Unprecedented business model	Uber's ridesharing, Airbnb's room sharing	Taxi service, hotel industry



Generally, the role of regulatory threat is likely to be limited.

the need for permanent rulemaking. More likely, however, such norms and practices will most likely represent interim rather than permanent solutions.

Generally, the role of regulatory threat is likely to be limited. It cannot serve to allow regulators to do informally what they lack formal regulatory authority to undertake. Threats without appropriate statutory or delegated authority are nothing more than abuses of power.¹²¹

Play in the sandbox

A regulatory sandbox is a testing ground for new business models not governed by current regulation or supervised by regulatory institutions. The purpose of the sandbox is to adapt compliance with strict appropriate regulations to the growth and pace of the most innovative new technological developments without smothering them prematurely.

The UK Financial Regulatory Authority launched a regulatory sandbox in 2015 so that firms could

- » Test products and services in a controlled environment
- » Reduce time to market at lower costs
- » Identify appropriate consumer protection safeguards
- » Gain better access to finance.¹²²

Thus far, several firms have used this sandbox to test distributed ledger technology. It "was the most popular technology employed across the first two cohorts with 17 firms utilizing the technology in some way."¹²³ The majority of these sandbox firms were electronic money or payments institutions, a number of which tried to "facilitate cross-border payments, with models differing significantly from traditional and peer-to-peer money remittance companies."

Regulatory sandboxes can be an extremely helpful tool for observing how innovators might use highly disruptive and unpredictable technologies.

One firm experimented with an intermediary cryptocurrency to transfer funds from British sterling to South African rand and was able to reduce transaction time to as little as two minutes.¹²⁴ Another firm tested whether private limited companies could represent and manage their shares and corporate governance digitally, thereby minimizing associated legal costs. Still another emulated "the normal issuance process for a short-term debt instrument" without the typical registrars and nominees.¹²⁵

Regulatory sandboxes are not always appropriate and should be used judiciously. However, they can be an extremely helpful tool for observing how innovators might use highly disruptive and unpredictable technologies.



Collaborate internationally and coordinate national agencies

"I don't think they play at all fairly," Alice began, in rather a complaining tone; "and they all quarrel so dreadfully one can't hear one's self speak—and they don't seem to have any rules in particular; at least, if there are, nobody attends to them."¹²⁶



"'Off with her head!' screamed the Queen," Lewis Carroll, *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 68. No known copyright restrictions.

Following the 2008 financial crisis, global regulators collaborated to reform derivatives markets on a global basis.

Following the 2008 financial crisis, global regulators collaborated to reform derivatives markets on a global basis. In 2009, the members of the G20 agreed to a set of common regulatory principles for derivatives that addressed the reporting, use and means of trading derivatives. Core to the G20 agreement was a requirement that governments work to harmonize derivatives regulations.

The Dodd-Frank requirements relating to swaps regulated by the CFTC apply to activities outside the United States that either: (a) have a direct and significant connection with activities in, or effect on, commerce in the United States; or (b) contravene CFTC rules intended to prevent evasion of US requirements.¹²⁷ EU swap regulations are similar, thus setting the stage for potential conflicts.

Given the global nature of derivatives markets, the United States, the European Union, and other G20 countries recognized the notion



The G20 initiative demonstrated that a level of global regulatory harmonization is indeed possible.

of substitute compliance. To a certain extent in their respective derivatives regulations, they have enabled a financial institution operating in multiple markets to comply with the derivatives regulatory requirements of one country rather than multiple ones, where the appropriate regulator has determined that the regulations of the different jurisdictions are substantially comparable.

This system is not perfect and has by no means resolved all existing or potential future regulatory conflicts. Nevertheless, the G20 initiative demonstrated that a level of global regulatory harmonization is indeed possible. There is no reason for not taking a global approach to many blockchain applications.

Dodd-Frank also included a number of Congressional requirements that the multitude of US financial regulators work together to jointly develop and issue regulations covering derivatives markets and participants. For example, the Volcker Rule (part of Dodd-Frank) was jointly developed and issued by the SEC, CFTC, and various US federal banking agencies. However, the Volcker Rule itself is exceedingly complex, and these regulators sometimes have differing interpretations of various provisions of the rule.

If regulators with potentially overlapping jurisdictions don't attempt to coordinate and harmonize their efforts, then markets can significantly suffer. We are already seeing the effects of the lack of coordination among the SEC, CFTC, and FinCEN on the regulatory treatment of tokens issued in ICOs.

Minimize unintended consequences

This is a great aspirational goal, but easier said than done. Daniel Gervais, professor of law at Vanderbilt University, argues that the likelihood of regulatory efforts leading to unintended consequences is greater with inchoate technologies such as blockchain because they "evolve in unpredictable ways and . . . spawn new chains of technological developments" independently of both regulation and market forces that, in turn, can result in unintended consequences that serve to defeat the objectives of regulatory intervention.¹²⁸

The ability of the blockchain to democratize determinations of its future uses and development may empower behaviors encouraged by social norms rather than regulation.

Gervais argues that inchoate technologies require a different type of regulatory intervention and that the level of difficulty in regulating an inchoate technology is proportional to its level of inchoateness. A characteristic of inchoate technologies essentially is their ability to develop and evolve independently of both regulation and market forces that, in turn, can result in unintended consequences that serve to defeat the objectives of regulatory intervention. The ability of the blockchain to democratize determinations of its future uses and development may empower behaviors encouraged by social norms rather than regulation.

Early in the life of inchoate technologies, social norms often arise with the intended purpose of trying to circumvent regulations or at least with the intent of demonstrating that "old world" regulations do not apply to the new technology world. Consider the anarchist attitudes of early blockchain enthusiasts: they maintain that the consensus of blockchain users, not regulators, should determine how



the blockchain is used and developed. This attitude tends to give way to a more mature, realistic view of the legitimate role of regulation as the technology begins to mature.

As this process unfolds, regulatory attempts, if too heavy handed, can push the technology and its users in unanticipated ways, potentially driving aspects of development and usage underground or beyond regulatory reach. That is, developers and users will concertedly hide from regulators or seek more favorable jurisdictions. Gervais reminds us that the path to perdition is paved with good intentions:

The law of unintended consequences, when applied to an inchoate technology, supports the claim that because of the high degree of unpredictability of the evolution of the technology, the impact of future chains of events is almost impossible to predict, and whether more harm than good will be prevented by even well-intended regulation is educated guesswork at best.¹²⁹

Flexibility is key. As the technology stabilizes, the social norms that have developed alongside the technology become easier to identify.

At the very least, inchoate technologies likely have a life of their own, and regulators must take this into account. Does this mean that regulators should refrain from regulating a new and unpredictable technology such as the blockchain? Of course not. But regulators should remember that inchoate technologies like the blockchain are unpredictable. Accordingly, regulators must acknowledge that they simply do not know whether blockchain applications will ultimately lead to net positive or negative consequences. But should regulators evaluate these applications ex ante and ban or limit those deemed mostly negative?

Flexibility is key. As the technology stabilizes, the social norms that have developed alongside the technology become easier to identify. Over time, regulatory intervention becomes easier as future evolution of the technology becomes less susceptible to unforeseen forces. The greater predictability of the technology makes it easier to mesh regulations with the social norms that have arisen.

Pathway forward

Regulators, blockchain users, and society at large needs to understand where the blockchain may be taking us and how we might use it. The following action items will allow us to strike the right balance between regulating where appropriate and fostering an environment in which blockchain technologies and applications can flourish.



Educate and help all stakeholders deal with “regulatory disruption.”



- › The faster a new technology moves or evolves, or the greater the amount of disruption to existing technology or ways of socializing or doing business, the more challenging it is for regulators to understand what needs to be regulated (if at all) and how.
- › Disruptive innovations really challenge regulators. New products, services, and business practices arising from blockchain technology may fall within an agency's jurisdiction, yet not square well with the agency's existing regulatory framework.
- › Massive information asymmetries may yield commensurate regulatory uncertainty or misregulation.



Determine whether these are unprecedented activities or merely a new medium.

- › Ask whether we really need new regulation or whether existing regulation will suffice.
- › If existing regulations mostly work, then determine what the minimal required modifications are. Legacy regulation is not in itself a reason to intervene or not to refrain from doing so. It is, however, part of the extant framework that policymakers must take into account, in part because changes to one policy lever impact others.
- › Avoid premature regulation. Adopt interim measures—interpretive guidance and statements of best practices—especially to learn and monitor.



Experiment and test potential regulations.

- › Consider continuing education, data collection, feedback loops, peer review, pilot programs, sandboxes, and other means of gathering stakeholder input.
- › Encourage and work with market-based and private initiatives.
- › Measure regulatory initiatives. By examining the extent to which a proposed regulation strikes a balance between maximizing the benefits of the new innovations and minimizing the risks or harm that could be caused by the new innovation.
- › Don't adopt new regulations if feedback from experimentation does not support the regulation.



Pursue national and global coordination and consensus.

- › Use existing precedents in cross-border commerce, international financial markets and property protection as models for cross-border collaboration.



Embrace the multi-faceted personality of the blockchain as an invitation for regulatory bodies to collaborate instead of engaging in turf battles.

- › Explore public-private partnerships that take advantage of existing or newly formed international trade groups and other multi-national organizations.
- › Embrace the multi-faceted personality of the blockchain as an invitation for regulatory bodies to collaborate instead of engaging in turf battles.



- If new regulations are required, then ask these questions.
- › *Timing:* When should the agency intervene, if at all? Does waiting necessarily generate a better informational basis on which to regulate? What are the drawbacks of waiting?
 - › *Form:* Should the agency regulate via rule, adjudication, guidance, or some alternate form? Given the costs and benefits of each, which best accommodates the uncertainties of the innovation? Does form even matter?
 - › *Durability:* Should the agency's intervention be permanent, or temporary, or conditional? How long should it endure? Are there ways to better calibrate regulatory interventions to the innovation?
 - › *Enforcement:* How rigorously should the agency monitor and sanction noncompliance? How much should agencies temper enforcement against the novel products and new ways of doing business arising from the blockchain?
 - › *Unintended consequences:* Regulators should try to determine the unintended consequences the proposed regulation (or lack thereof) could cause. To a large degree, this is impossible to do with any precision for disruptive technologies like the blockchain both because by their very nature they are unpredictable and because they can react to defeat regulatory efforts. One possible way to consider the consequences of a regulatory intervention is to ask what would happen if all actors did as prompted by the regulation; that is, regulators should consider the global impact.





About the author

Joel Telpner is a corporate and finance partner in the New York office of Sullivan & Worcester LLP and heads the firm's fintech and blockchain practice group. He is a seasoned advisor, strategist, and problem solver. Mr. Telpner brings more than 30 years of legal experience in a career. He has served as an Am Law 100 partner, the US general counsel of a global financial institution, and a venture capitalist. He is a highly sought after legal advisor in the blockchain space.

He led a panel discussion about ICOs and best practices in Davos during the World Economic Forum in January. He is working on policy initiatives on global regulatory issues for blockchain on behalf of the Global Blockchain Business Council and Wharton Reg@Tech. He is a member of the Wall Street Blockchain Alliance's Legal Working Group, which is developing guidance on best practices for ICOs, and of the Digital Currency and Ledger Defense Coalition, a coalition of lawyers and academics who focus on the legal issues surrounding digital currency and distributed ledger technology.

Mr. Telpner is also recognized for his ability to deftly manage complex financial transactions, especially those involving sophisticated structured finance and derivatives matters, and has an extensive and unique combination of transactional and regulatory experience.

Education

M.B.A., University of Pennsylvania, Wharton School, 1999
J.D., with distinction, The University of Iowa, 1983
B.B.A., The University of Iowa, 1978

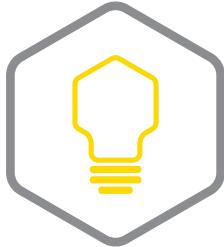
Awards and honors

"Deal Maker of the Year," Finance Monthly, 2014 (\$1.5 billion issuance by SanDisk)
"Lawyer of the Year," Corporate LiveWire, 2014
New York Super Lawyers (2006-2007; 2013-2018)
The Legal 500 US (2009-2017)

Disclosures

Mr. Telpner is a legal advisor to some of the biggest cryptocurrencies. He structured some of the first ICOs and blockchain-based applications. He also structured the first issuance of digital securities utilizing blockchain technology for Overstock.com and helped in launching Overstock's distributed ledger platform, tZero.





About the Blockchain Research Institute

Co-founded in 2017 by Don and Alex Tapscott, the Blockchain Research Institute is a knowledge network organized to help realize the new promise of the digital economy. It builds on their yearlong investigation of distributed ledger technology, which culminated in the publication of their critically acclaimed book, *Blockchain Revolution* (Portfolio|Penguin).

Our syndicated research program, which is funded by major corporations and government agencies, aims to fill a large gap in the global understanding of blockchain technology and its strategic implications for business, government, and society.

Our global team of blockchain experts is dedicated to exploring, understanding, documenting, and informing leaders of the market opportunities and implementation challenges of this nascent technology.

Research areas include financial services, manufacturing, retail, energy and resources, technology, media, telecommunications, healthcare, and government as well as the management of organizations, the transformation of the corporation, and the regulation of innovation. We also explore blockchain's potential role in the Internet of Things, robotics and autonomous machines, artificial intelligence, and other emerging technologies.

Our findings are initially proprietary to our members and are ultimately released under a Creative Commons license to help achieve our mission. To find out more, please visit www.blockchainresearchinstitute.org.

Leadership team

Don Tapscott – Co-Founder and Executive Chairman

Alex Tapscott – Co-Founder

Joan Bigham - Managing Director, International

Hilary Carter - Managing Director, Canada

Kirsten Sandberg - Editor-in-Chief

Jane Ricciardelli - Director of Marketing

Wayne Chen - Director of Business Development

Maryantonett Flumian - Director of Client Experience

Luke Bradley – Director of Communications



Notes

1. Jim Newsome, Daniel Gasteiger, Meltem Demirors, Heinrich Zetlmeyer, and Catrina Luchsinger Gaehwiler. "Lessons Learned: ICOs and Regulation Best Practices," panel, moderated by Joel Telpner, *Blockchain Central during WEF*, Global Blockchain Business Council, Davos, Switzerland, 24 Jan. 2018. www.gbbccouncil.org/event/blockchain-for-business-during-berkshire-hathaway-week, accessed 6 May 2018.
2. Lewis Carroll, "The Lion and the Unicorn," *Through the Looking-Glass*, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 145-155. archive.org/stream/throughlookinggl01carr.
3. Lewis Carroll, *Through the Looking Glass*, p. 145. archive.org/details/throughlookinggl01carr, accessed 7 May 2018.
4. Lewis Carroll, "Pig and Pepper," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 53. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
5. Originally published in 1865.
6. Lewis Carroll, "The Garden of Live Flowers," *Through the Looking-Glass*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 124-125. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
7. Don and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (New York: Penguin Portfolio, 2016).
8. Bernadette Schell and Clemens Martin, "Cyberanarchy, Cryptoanarchy," *Webster's New World Hacker Dictionary* (Hoboken, NJ: John Wiley & Sons, 2006): 77. books.google.com/books?isbn=0470047526, accessed 7 March 2018.
9. David G. Post, "Against 'Against Cyberanarchy,'" *BerkeleyTech Law Journal*, Vol. 17, Iss. 4, Berkeley Electronic Press, Elsevier Ltd. (2002): 1365. doi.org/10.15779/Z384T2B, accessed 7 March 2018.
10. For example, see Philip J. Weiser, "Internet Governance, Standard Setting, and Self-Regulation," *Northern Kentucky Law Review* 28 (2001): 822. scholar.law.colorado.edu/articles/588, accessed 7 March 2018.
11. Jack L. Goldsmith, "Against Cyberanarchy," *University of Chicago Law Occasional Paper*, Chicago Unbound, No. 40 (1999). chicagounbound.uchicago.edu/occasional_papers/2, accessed 7 March 2018.
12. Lewis Carroll, "Pig and Pepper," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 53. archive.org/stream/throughlookinggl01carrgoog#page/n58, accessed 5 March 2018.
13. Tim Wu, "Application Centered Internet Analysis," *Virginia Law Review* 85 (1999): 1163-1202. papers.ssrn.com/sol3/papers.cfm?abstract_id=157928, accessed 7 March 2018.
14. Joseph M. Reagle Jr., "Why the Internet Is Good: Community Governance That Works Well," *Berkman Center for Internet and Society*, Harvard Law School, 26 Mar. 1999. cyber.harvard.edu/archived_content/people/reagle/regulation-19990326.html; and Sir Tim Berners-Lee, "The Web Is under Threat. Join Us and Fight for It," *Webfoundation.org*, World Wide Web Foundation, 12 March 2018. webfoundation.org/2018/03/web-birthday-29, both accessed 6 May 2018.
15. Llewellyn Joseph Gibbons, "No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace," *Cornell Journal of Law and Public Policy*, Vol. 6, Iss. 3 (1997): 475-501. scholarship.law.cornell.edu/cjllpp/vol6/iss3/1, accessed 7 March 2018.
16. Joseph Gildred, "What Is DMCA? A Guide to Copyright Law," *Cloudwards.net*, Alohomora Ltd., 7 Nov. 2017. www.cloudwards.net/what-is-dmca, accessed 6 May 2018.
17. Joseph Gildred, "What Is DMCA? A Guide to Copyright Law," *Cloudwards.net*, Alohomora Ltd., 7 Nov. 2017. www.cloudwards.net/what-is-dmca, accessed 6 May 2018.
18. Philip J. Weiser, "The Internet, Innovation, and Intellectual Property Policy," *Columbia Law Review* 103 (April 2003): 534-613. lawweb.colorado.edu/profiles/pubpdfs/weiser/InternetInnovation.pdf, accessed 7 March 2018.
19. Wolfgang Kleinwachter, "From Self-Governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources," *Loyola of Los Angeles Law Review* 36: 3 (2003): 1103. digitalcommons.lmu.edu/llr/vol36/iss3/2, accessed 7 March 2018.
20. Amb. Daniel Sepulveda, "The Role for Governments in Internet Governance," mod. by Denise E. Zheng, Center for Strategic and International Studies, Washington DC, 15 Oct. 2014, uploaded 6 June 2016. www.csis.org/events/role-governments-internet-governance, accessed 7 March 2018.



21. Ira V. Heffner, "Note, Copyleft: Licensing Collaborative Works in the Digital Age," *Stanford Law Review* 49, no. 6 (July 1997): 1487-1521. See also Richard Stallman, "Initial Announcement: The GNU Project," *GNU Operating System*, Free Software Foundation, Inc., 27 Sept. 1983. www.gnu.org/gnu/initial-announcement.html, accessed 7 March 2018.
22. Philip J. Weiser, "The Internet, Innovation, and Intellectual Property Policy," 544.
23. Lewis Carroll, "It's My Own Invention," *Through the Looking-Glass*, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 166. archive.org/stream/throughlookinggl01carr#page/166.
24. Public Knowledge, "Net Neutrality," n.d. www.publicknowledge.org/issues/net-neutrality, accessed 25 Dec. 2017.
25. Emma N. Cano, "Saving the Internet: Why Regulating Broadband Providers Can Keep the Internet Open," *BYU Law Review*, no. 2 (March 2016). digitalcommons.law.byu.edu/lawreview/vol2016/iss2/10, accessed 6 May 2018.
26. *Verizon v. FCC*, 740 F. 3d 623, 630 (DC Cir. 2014).
27. 25 FCC Record 17937 (2009): para. 54.
28. The article by Emma N. Cano provides a detailed discussion of the origins and evolution of the net neutrality rule and the various court challenges. See Cano, "Saving the Internet."
29. Financial Crisis Inquiry Commission, chaired by Phil Angelides, *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*, official government ed. pursuant to Public Law 111-21, Jan. 2011, updated 25 Feb. 2011, p. 44. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf, accessed 11 March 2018.
30. Scott Patterson, interview by Financial Crisis Inquiry Commission, 12 Aug. 2010, for *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*, official government ed. pursuant to Public Law 111-21, Jan. 2011, updated 25 Feb. 2011, p. 44. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf, accessed 11 March 2018.
31. Cameron L. Cowan, on behalf of the American Securitization Forum, "Hearing on Protecting Homeowners: Preventing Abusive Lending While Preserving Access to Credit," Written Testimony, Subcommittee on Housing and Community Opportunity, Subcommittee on Financial Institutions and Consumer Credit, United States House of Representatives, 5 Nov. 2003. financialservices.house.gov/media/pdf/110503cc.pdf.
32. James Rokakis, interview by Financial Crisis Inquiry Commission, 8 Nov. 2010, for *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*, official government ed. pursuant to Public Law 111-21, Jan. 2011, updated 25 Feb. 2011, p. 10. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf, accessed 11 March 2018.
33. Financial Crisis Inquiry Commission, chaired by Phil Angelides, *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*, official government ed. pursuant to Public Law 111-21, Jan. 2011, updated 25 Feb. 2011, p. xxi. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf, accessed 12 Feb. 2018.
34. Charles Chieppo, "What Government Can Do to Attract Top IT Talent," *Governing: The State and Localities*, E. Republic, 18 Apr. 2014. www.governing.com/blogs/bfc/col-government-challenge-attracting-top-information-technology-talent.html, accessed 15 March 2018.
35. Financial Crisis Inquiry Commission, *The Financial Crisis Inquiry Report*, p. xviii. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf.
36. Financial Crisis Inquiry Commission, *The Financial Crisis Inquiry Report*, p. xx. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf.
37. Julia Maues, "Banking Act of 1933 (Glass-Steagall)," *Federal Reserve History*, Federal Reserve Bank of St. Louis, 22 Nov. 2013. www.federalreservehistory.org/essays/glass_steargall_act, accessed 11 March 2018.
38. Carter Glass, Henry Bascom Steagall, 73rd Congress, *Banking Act of 1933 (Glass-Steagall Act)*, Public Law No. 66, H. R. 5661, 16 June 1933. fraser.stlouisfed.org/scribd/?title_id=991&filepath=/files/docs/historical/congressional/1933_bankingact_publiclaw66.pdf, accessed 11 March 2018.
39. Laura Kusisto, "Many Who Lost Homes to Foreclosure in Last Decade Won't Return—NAR," *The Wall Street Journal*, Dow Jones & Company, 20 April 2015. www.wsj.com/articles/many-who-lost-homes-to-foreclosure-in-last-decade-wont-return-nar-1429548640, accessed 16 Feb. 2018.
40. 111th Congress, *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010*, Public Law 111-203, § 929-Z, 124 Stat. 1376, 1871, 21 July 2010. fraser.stlouisfed.org/scribd/?title_id=1031&filepath=/files/docs/historical/congressional/dodd-frank.pdf, accessed 11 March 2018.



41. See "The Dodd-Frank Act: Too Big Not to Fail," *The Economist*, The Economist Newspaper Ltd., 18 Feb. 2012. www.economist.com/node/21547784, accessed 28 April 2018.
42. Financial Crisis Inquiry Commission, chaired by Phil Angelides, *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*, official government ed. pursuant to Public Law 111-21, Jan. 2011, updated 25 Feb. 2011, p. xxiii. www.gpo.gov/fdsys/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf, accessed 12 Feb. 2018.
43. Kevin Dobbs, "Since Dodd-Frank, Compliance Costs Up At Least 20% for Many US Banks," S&P Global Market Intelligence, S&P Global Inc., 27 Oct. 2017. www.snl.com/Cache/snlpdf_886e26a7-d03a-4947-ac46-af4af8dca809.pdf, accessed 6 May 2018.
44. Kevin Dobbs, "Since Dodd-Frank, Compliance Costs Up At Least 20% for Many US Banks."
45. Kevin Dobbs, "Since Dodd-Frank, Compliance Costs Up At Least 20% for Many US Banks."
46. Stacey English and Susannah Hammond, "Cost of Compliance Report 2017: Is There a New Risk Approach?" *Inside Financial and Risk Blog*, Thomson Reuters, 6 Dec. 2017. blogs.thomsonreuters.com/financial-risk/risk-management-compliance/cost-of-compliance-report-2017-is-there-a-new-risk-approach, accessed 15 March 2018.
47. Stacey English and Susannah Hammond, "Cost of Compliance Report 2017."
48. Julian Korek et al., "Global Regulatory Outlook 2017," Duff & Phelps, 28 Feb. 2017. www.duffandphelps.com/-/media/assets/pdfs/publications/compliance-and-regulatory-consulting/2017-global-regulatory-outlook-viewpoint.ashx, accessed 9 March 2018.
49. Lewis Carroll, "The Garden of Live Flowers," *Through the Looking-Glass*, with illustrations by John Tenniel (London: Macmillan & Co., 1872): 39. www.gutenberg.org/files/12/12-h/12-h.htm, accessed 5 March 2018.
50. Philip Boucher, "How Blockchain Technology Could Change our Lives," *European Parliamentary Research Services*, Feb. 2017. [www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRI_IDA\(2017\)581948_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRI_IDA(2017)581948_EN.pdf), accessed 31 Dec. 2017.
51. Philip Boucher, "How Blockchain Technology Could Change our Lives."
52. Philip Boucher, "How Blockchain Technology Could Change our Lives."
53. R3 is an enterprise software firm working with a network of over 200 banks, financial institutions, regulators, trade associations, professional services firms and technology companies to develop on Corda, its blockchain platform designed specifically for businesses. See www.r3.com/about, accessed 28 April 2018.
54. Rachel W. Robinson, "Distributed and Collaborative Marketplaces: Blockchain Serving the Unbanked," Blockchain Research Institute, 22 Jan. 2018.
55. John Stark, "Making Sense of Blockchain Smart Contracts," *CoinDesk*, 4 June 2016. www.coindesk.com/making-sense-smart-contracts, accessed 1 Jan. 2018.
56. SEC Chairman Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings," Securities and Exchange Commission, 11 Dec. 2017. www.sec.gov/news/public-statement/statement-clayton-2017-12-11, accessed 25 Dec. 2017.
57. Lewis Carroll, "Advice from a Caterpillar," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 46. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
58. Banning Garrett, "Technology Will Keep Changing Everything—and Will Do it Faster," *Atlantic Council: Brent Scowcroft Center on International Security*, Atlantic Council of the United States, July 2015. www.atlanticcouncil.org/images/publications/Technology.pdf, accessed 23 Dec. 2017.
59. Lewis Carroll, "Alice's Evidence," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 95-96. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
60. James Mackintosh, "Is It Time to Regulate Bitcoin?" *Wall Street Journal*, Dow Jones & Company, 4 Dec 2017. www.wsj.com/articles/is-it-time-to-regulate-bitcoin-1512409004, accessed 12 Dec. 2017.
61. In a literal sense, a bitcoin is a unique answer to a math problem and proof that you solved that problem or else had the unique record of the solution transferred to your control. See Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.bitcoin.org/bitcoin.pdf, accessed Sept. 15, 2017.
62. Tara Mandjee, "Bitcoin, its Legal Classification and its Regulatory Framework," *Journal of Business & Securities Law* 15, no. 2 (2015): 158-218. Footnotes within this passage were omitted for readability.
63. Bill Z. Yang, "What is (Not) Money? Medium of Exchange ≠ Means of Payment," *American Economist* 51, no. 2 (Fall 2007): 101-104.



64. Tara Mandjee, "Bitcoin, its Legal Classification and its Regulatory Framework." Footnotes within this passage were omitted for readability.
65. John Butler, "Is Money a Store of Value?" *Financial Sense*, 3 Nov. 2010. www.financialsense.com/contributors/john-butler-john-boylan/is-money-a-store-of-value, accessed 2 Jan. 2018.
66. Chris Morris, "Venezuela's Cash Is Now Worth Less Than Currency in 'World of Warcraft,'" *Fortune*, 1 Aug. 2017. fortune.com/2017/08/01/venezuela-bolivar-world-of-warcraft-currency, accessed 21 Jan. 2018.
67. However, in Germany, Bitcoin has been recognized as a "unit of account" and, therefore, referred to as private money. See Tyler Durden, "Bitcoin Is Recognized As 'Legal Tender' in Germany," *Zero Hedge*, 19 Aug. 2013. www.zerohedge.com/node/47778, accessed 17 Feb. 2018.
68. California Bankers Association v. Shultz, 416 U.S. 25, 39 n.14 (1974). "Currency is defined in the Secretary's regulations as the 'coin and currency of the United States or of any other country, which circulate in and are customarily used and accepted as money in the country in which issued."
69. Financial Action Task Force, "FATF Report, Virtual Currencies, Key Definitions and Potential AML/CFT Risks," June 2014, p. 4. www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, accessed 21 Oct. 2017. Endnotes within this definition were omitted for readability.
70. Financial Action Task Force, "FATF Report, Virtual Currencies, Key Definitions and Potential AML/CFT Risks," June 2014, p. 4. www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, accessed 21 Oct. 2017. Endnotes within this definition were omitted for readability.
71. Financial Action Task Force, "FATF Report," p. 5.
72. Financial Action Task Force, "FATF Report," p. 5.
73. Financial Action Task Force, "FATF Report," p. 4. Endnotes within this definition were omitted for readability.
74. However, in Germany, Bitcoin has been recognized as a "unit of account" and, therefore, referred to as private money. See Tyler Durden, "Bitcoin Is Recognized As 'Legal Tender' in Germany," *Zero Hedge*, 19 Aug. 2013. www.zerohedge.com/node/47778, accessed 17 Feb. 2018.
75. *California Bankers Association v. Shultz*, 416 U. S. 25, 39 n. 14 (1974). supreme.justia.com/cases/federal/us/416/21/case.html, accessed 6 May 2018. "Currency is defined in the Secretary's regulations as the 'coin and currency of the United States or of any other country, which circulate and are customarily used and accepted as money in the country in which issued."
76. SEC Chairman Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings," 11 Dec. 2017. www.sec.gov/news/public-statement/statement-clayton-2017-12-11, accessed 25 Dec. 2017.
77. See *In re Coinflip, Inc. , d/b/a Derivabit, and Francisco Riordan*, CFTC Docket No. 15-29, 2015 WL 5535736, [Current Transfer Binder] (CCH) if 33,538 (CFTC Sept. 17, 2015); *In re TeraExchange LLC*, CFTC Docket No. 15-33, 2015 WL 5658082, [Current Transfer Binder] (CCH) if 33,546, (CFTC 24 Sept. 2015).
78. SEC Chairman Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings."
79. SEC Chairman Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings."
80. SEC Chairman Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings."
81. Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," 18 March 2013. www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering, accessed 25 Dec. 2017.
82. 31 CFR § 1010. 100(m).
83. 31 CFR § 1010. 100(ff)(5)(i)(A).
84. 31 CFR § 1010. 100(ff)(5)(i)(A).
85. Section 2(a)(1) of the US Securities Act of 1933, as amended through P.L. 114-94 and enacted 4 Dec. 2015, 23 June 2016. legcounsel.house.gov/Comps/Securities%20Act%20of%201933.pdf, accessed 30 Dec. 2017.
86. *SEC v. W. J. Howey Co.*, 328 U. S. 293 (1946), Legal Information Institute, Cornell Law School, n.d. www.law.cornell.edu/supremecourt/text/328/293.
87. *Howey*, 298, citing *State v. Gopher Tire & Rubber Co.*, 146 Minn. 52, 56, 177 N.W. 937, 938.
88. *Howey*, 302.



89. Howey, 299.
90. *Tcherepnin v. Knight*, 389 U. S. 332, 336 (1967).
91. Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The Dao," Exchange Act Release No. 81206, 25 July 2017. www.sec.gov/litigation/investreport/34-81207.pdf, accessed 30 Dec. 2017.
92. Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The Dao."
93. Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The Dao."
94. SEC, Report on the Dao, 25 July 2017, pp 9-10.
95. Andrew Quentson, "Ethereum to Hardfork, DAO to Be Dismantled," *CryptoCoinsNews*, PF Wetting, 17 June 2016. www.ccn.com/ethereum-to-hardfork-dao-to-be-dismantled, accessed 28 Feb. 2018.
96. "Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933: In the Matter of Munchee Inc.," Securities Act Release No. 10445, 11 Dec. 2017. www.sec.gov/litigation/admin/2017/33-10445.pdf, accessed 30 Dec. 2017.
97. "In the Matter of Munchee," para. 29, p 8.
98. Sanjeev Verma, Nghi Bui, and Chelsea Lam, "Munchee Token: A Decentralized Blockchain Based Food Review/Rating Social Media Platform," White Paper, Munchee Inc., 16 Oct. 2017, pp. 11, 17. www.theventurealley.com/wp-content/uploads/sites/5/2017/12/Munchee-White-Paper.pdf, accessed 3 Feb. 2018.
99. Sanjeev Verma et al., "Munchee Token," White Paper, p. 3.
100. "In the Matter of Munchee," para. 18, p. 6.
101. "In the Matter of Munchee," para. 35, p. 9.
102. "In the Matter of Munchee," para. 14, p. 5.
103. *United Housing Found, Inc. v. Forman*, 421 US 837, 852 (1975).
104. *United Housing Found, Inc. v. Forman*, 421 US 837, 852 (1975).
105. *United Housing*, 858.
106. *United Housing. Id. See also, Landreth Timber Co. v. Landreth*, 471 US 681, 689 (1985).
107. *Bronstein v. Bronstein*, 407 F. Supp. 925, 930 (ED Pa. 1976).
108. Lewis Carroll, "Advice from a Caterpillar," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 38. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
109. Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (W. W. Norton & Company, 20 Jan. 2014): 11. www.amazon.com/Second-Machine-Age-Prosperity-Technologies/dp/0393350649.
110. Brynjolfsson and McAfee, p. 245.
111. Brynjolfsson and McAfee, p. 217.
112. Marco Iansiti and Karim R. Lakhani, "The Truth about Blockchain," *Harvard Business Review*, Jan.-Feb. 2017. hbr.org/2017/01/the-truth-about-blockchain, accessed Jan. 29, 2018.
113. Clayton Christensen, "Disruptive Innovations," *Christensen Institute*, Clayton Christensen Institute, n.d. www.christenseninstitute.org/disruptive-innovations, accessed 28 Feb. 2018.
114. Iansiti and Lakhani, "The Truth about Blockchain."
115. Iansiti and Lakhani, "The Truth about Blockchain."
116. Philip Boucher, Susana Nascimento, and Mihalis Kritikos, "How Blockchain Technology Could Change our Lives," *Scientific Foresight Unit*, European Parliamentary Research Services, PE 581.948, Feb. 2017. [www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf), accessed 31 Dec. 2017.
117. Lewis Carroll, *Through the Looking Glass: and What Alice Found There*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 124. archive.org/details/throughlookingl01carr, accessed 6 May 2018.
118. See Tim Wu, "Essay Agency Threats," *Duke Law Review* 60 (2011): 1841-1857.
119. Tim Wu, "Essay Agency Treats," 1848.
120. Tim Wu, "Essay Agency Treats," 1848.
121. See Jerry Brito, "'Agency Threats' and the Rule of Law: An Offer You Can't Refuse," *Harvard Journal of Law & Public Policy* 37, no. 2 (2012): 553-577. www.mercatus.org/publication/agency-threats-and-rule-law-offer-you-can-t-refuse, accessed 6 May 2018. Brito opposes the use of agency threats in virtually all scenarios and issues a strong rebuttal to Tim Wu.



122. "Regulatory Sandbox," *Financial Conduct Authority*, accountable to UK Parliament's Treasury Select Committee, 11 May 2015, updated, 14 Feb. 2018. www.fca.org.uk/firms/regulatory-sandbox, accessed 28 Feb. 2018.
 123. "Regulatory Sandbox Lessons Learned Report," *Financial Conduct Authority*, Parliament's Treasury Select Committee, Oct. 2017, p. 9. www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf, accessed 28 Feb. 2018.
 124. "Regulatory Sandbox Lessons Learned Report," p. 11.
 125. "Regulatory Sandbox Lessons Learned Report," p. 10.
 126. Lewis Carroll, "The Queen's Croquet-Ground," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 69. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
 127. Dodd-Frank, section 722(d); Commodity Exchange Act Section 2(i).
 128. Daniel Gervais, "The Regulation of Inchoate Technologies," *Houston Law Review* 47, no. 3 (2010): 666-705. discoverarchive.vanderbilt.edu/bitstream/handle/1803/7328/Regulation_of_Inchoate_Technologies.pdf, accessed 6 March 2018.
 129. Daniel Gervais, "The Regulation of Inchoate Technologies."
 130. Lewis Carroll, "The Rabbit Sends in a Little Bill," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 30. ia801408.us.archive.org/35/items/alicesadventure01carrgoog/alicesadventure01carrgoog_djvu.txt, accessed 5 March 2018.
-

"It was much pleasanter at home," thought poor Alice, "when one wasn't always growing larger and smaller, and being ordered about by mice and rabbits. I almost wish I hadn't gone down that rabbit-hole—and yet—and yet—it's rather curious, you know, this sort of life! I do wonder what can have happened to me!"¹³⁰



"What happened to Alice," Lewis Carroll, "The Rabbit Sends in a Little Bill," *Alice's Adventures in Wonderland*, with illustrations by John Tenniel (New York: Macmillan & Co., 1898): 30. No known copyright restrictions.







blockchainresearchinstitute.org